Space Lower Bounds for Approximating Maximum Matching in the Edge Arrival Model

Michael Kapralov
EPFL

January 11, 2021

Abstract

The bipartite matching problem in the online and streaming settings has received a lot of attention recently. The classical vertex arrival setting, for which the celebrated Karp, Vazirani and Vazirani (KVV) algorithm achieves a $1-1/e$ approximation, is rather well understood: the $1-1/e$ approximation is optimal in both the online and semi-streaming setting, where the algorithm is constrained to use $n \cdot \log^{O(1)} n$ space. The more challenging the edge arrival model has seen significant progress recently in the online algorithms literature. For the strictly online model (no preemption) approximations better than trivial factor $1/2$ have been ruled out [Gamlath et al'FOCS'19]. For the less restrictive online preemptive model a better than $\frac{1}{1+\ln 2}$-approximation [Epstein et al'STACS'12] and even a better than $(2-\sqrt{2})$-approximation[Huang et al'SODA'19] have been ruled out.

The recent hardness results for online preemptive matching in the edge arrival model are based on the idea of stringing together multiple copies of a KVV hard instance using edge arrivals. In this paper, we show how to implement such constructions using ideas developed in the literature on Ruzsa-Szemerédi graphs. As a result, we show that any single pass streaming algorithm that approximates the maximum matching in a bipartite graph with n vertices to a factor better than $\frac{1}{1+\ln 2} \approx 0.59$ requires $n^{1+\Omega(1/\log\log n)} \gg n \log^{O(1)} n$ space. This gives the first separation between the classical one sided vertex arrival setting and the edge arrival setting in the semi-streaming model.

Contents

1 Introduction

Large datasets are common in modern data analysis, and processing them requires algorithms with space complexity sublinear in the size of the input. The streaming model of computation, originally introduced in the seminar work of [AMS96], captures this setting, has received a lot of attention in the literature recently. In this paper we study the space complexity of the bipartite matching problem in the streaming model: the edges of a bipartite graph $G = (P, Q, E)$ are presented in an adversarial order as a stream, and the algorithm must output a matching $M_{ALG} \subseteq E$ at the end of the stream such that $|M_{ALG}| \geq \gamma|M_{OPT}|$ with high constant probability, for some approximation ratio $\gamma \in (0, 1]$. The algorithm is constrained to use $n \log^{O(1)} n$ space, where n is the number of vertices in the input graph. This is a common assumption, and the streaming model with this space restriction is often referred to as the *semi-streaming* model of computation [FKM$^+$05]. In this model the simple greedy algorithm, which maintains a maximal matching in the graph received so far, achieves a $\gamma = \frac{1}{2}$ approximation by storing $O(n)$ edges (and therefore using only $O(n \log n)$ bits of space). Despite a considerable amount of research over the past decade, it is still not known whether it is possible to achieve a better than $\frac{1}{2}$ approximation in this model using a single pass over the stream. The best hardness result so far is due to [Kap13], ruling out a $(1 - 1/e + \eta)$-approximation for any constant $\eta > 0$ in less than $n^{1+\Omega(1/\log\log n)}$ space, and thereby showing that no semi-streaming algorithm can do significantly better than $1 - 1/e$. The lower bound of [Kap13] applies (and is tight for) a more restricted model, where vertices on one side of the input graph $G = (P, Q, E)$ arrive in the stream in an arbitrary order and reveal their edges upon arrival. This model is inspired by the classical online matching problem studied in the seminal work of Karp, Vazirani and Vazirani [KVV90], where vertices on one side of a bipartite graph $G = (P, Q, E)$ arrive online, and the algorithm must match an arriving vertex irrevocably to one of its neighbors upon arrival or discard it. The competitive ratio of $1 - 1/e$ is achievable and tight for the online model with one sided vertex arrivals as well. The online version of the matching problem in the edge arrival setting has recently been resolved, the work of [GKM$^+$19] showing that no strictly online (i.e., without preemption) algorithm can do better than greedy in the edge arrival model. The same question remains open for the online model with preemption, which is close to the semi-streaming model that we are interested in. Several new hardness results for this model have been shown recently [ELSW13, WW15, HPT$^+$19], ruling out the possibility of a $1 - 1/e$ approximation in the online model with preemption. In this work we extend one of these results, due to Epstein et al [ELSW13], to the streaming setting. Specifically, our main result is

Theorem 1 *Any single-pass streaming algorithm that finds a* $(\frac{1}{1+\ln 2} + \eta)$*-approximate matching in an* n*-vertex bipartite graph for a constant* $\eta > 0$ *with probability at least* $1/2$ *must use* $n^{1+\Omega(1/\log\log n)} \gg n \log^{O(1)} n$ *bits of space.*

This gives the first separation between the classical one sided vertex arrival setting and the edge arrival setting in the semi-streaming model. We note that the best hardness result for online preemptive matching at the moment is a $2 - \sqrt{2}$-hardness, due to [HPT$^+$19]. Our techniques in this paper can probably be extended to their instance, but we prefer to use the earlier instance of [ELSW13] to simplify exposition.

1.1 Related Work

Over the past decade, matchings have been extensively studied in the context of streaming and related settings. The prior work closest to ours is the aforementioned $1-1/e$ lower bound of [Kap13] (see also [GKK12] and [FLN$^+$02]). Strong lower bounds for approximating matchings in the sketching model have been proposed in [AKLY16, AK17]. Multipass lower bounds for exact matching computation are given in [GO16].

Good approximations using a small number of passes have been presented in [KT17], and algorithmic results on the weighted version of the problem are given in [CS14, PS17]. Besides the most stringent adversarial edge arrival model, the relaxed random order streaming model has seen a lot of attention, where small space approximations to matching size have been given [KKS14, CJMM17, MMPS17, KMNT20]. The problem of approximating the size of the maximum matching in adversarially ordered streams has also received significant attention in the literature:[EHL$^+$15, BS15, AKL17, MV18, BGM$^+$19, MV16, CCE$^+$16, EHM16].

2 Technical overview

We start by defining $\frac{1}{1+\ln 2}$-hard instance from [ELSW13]. We first define an α-KVV gadget $G = (S, T, E)$.

Definition 2 (α-KVV gadget) *We define a α-KVV gadget as a bipartite graph $G = (S, T, E)$ with $|T| = N$ vertices on the T side of the bipartition and $|S| = \alpha \cdot N$ vertices on the S side of the biparitition as follows. We think of vertices in T as being numbered with integers in $[N] = \{0, 1, \ldots, N-1\}$ and vertices in S as being numbered with integers in $[\alpha \cdot N] = \{0, 1, \ldots, \alpha \cdot N - 1\}$. The graph G is parameterized by a permutation $\pi : [N] \to [N]$ of vertices in T: every vertex $j \in S$ is connected to all vertices $i \in T$ such that $\pi(i) \geq j$.*

Note that the original $(1 - 1/e)$-hard instance of Karp, Vazirani and Vazirani [KVV90] is a 1-KVV instance as above with the permutation π chosen uniformly at random. A version of this construction was implemented using techniques from the literature on Ruzsa-Szemerédi graphs in [Kap13], showing that any algorithm that finds a better than $(1 - 1/e)$-approximation using a single pass over the input stream with high constant probability must use $n^{1+\Omega(1/\log\log n)}$ bits of space. In this work we show how to combine such implementations of a KVV-gadget to achieve the stronger hardness result of $\frac{1}{1+\ln 2}$ for single pass streaming algorithms in the more general edge arrival model. To achieve our result, we implement the construction of [ELSW13], which we now describe.

Combining $1/2$-KVV gadgets: the hard instance of [ELSW13] . The hard instance of [ELSW13] uses a combination of L independent copies of the $1/2$-KVV gadget for a large constant L as follows. For $\ell \in [L] = \{0, 1, \ldots, L-1\}$[1] let $G^\ell = (S^\ell, T^\ell, E^\ell)$ be an independent $1/2$-KVV gadget. Let π^ℓ denote the ℓ-th permutation, selected independently and uniformly at random. For every $\ell \in [L]$ define the *terminal subset* of T^ℓ as the set of vertices that are assigned the largest values by π^ℓ. Namely, let

$$T^\ell_* = \{i \in T^\ell : \pi(i) \geq N/2\}.$$

Note that $|T^\ell_*| = N/2$ for every ℓ (we assume that N is even). The actual input graph $\widehat{G} = (P, Q, \widehat{E})$ of [ELSW13] is defined as follows. First, one lets

$$P = \bigcup_{\text{even } \ell \in [L]} T^\ell$$

and

$$Q = S^0 \cup \bigcup_{\text{odd } \ell \in [L]} T^\ell.$$

For every $\ell \in [L], \ell > 1$ one lets

$$\tau^\ell : S^\ell \to T^{\ell-1}_*$$

denote an arbitrary bijective mapping between the S^ℓ side of the biparition of G^ℓ and the terminal subset $T^{\ell-1}_*$ of $G^{\ell-1}$ – we refer to such maps as *glueing maps*. See Fig. 1 for an illustration. Let τ^0 denote the identity

[1] We use the notation $[a] = \{0, 1, \ldots, a-1\}$ throughout the paper.

map for convenience. The mapping $\tau^\ell, \ell \in [L], \ell > 0$, is naturally extended to edges $e = (u, v) \in E^\ell$, where $u \in S^\ell$ and $v \in T^\ell$ by letting

$$\tau^\ell(e) = (\tau^\ell(u), v).$$

In other words, one simply applies the map τ^ℓ to the S^ℓ endpoint of e. The edge set $\widehat{E}$ of $\widehat{G}$ is now defined as follows: for every $\ell \in [L]$ one adds, for every edge $e \in E^\ell$, the edge $\tau^\ell(e)$ to $\widehat{E}$. In other words, for every $\ell \in [L], \ell > 0$, one simply grows the $1/2$-KVV instance G^ℓ with the S^ℓ side of the bipartition identified with the terminal subset T^ℓ_* of the previous instance $G^{\ell-1}$ – see Fig. 2 for an illustration. In [ELSW13] the authors show that no online preemptive algorithm can find a better than $(\frac{1}{1+\ln 2} + o(1))$-competitive matching on this instance in expectation (and with nontrivial probability).

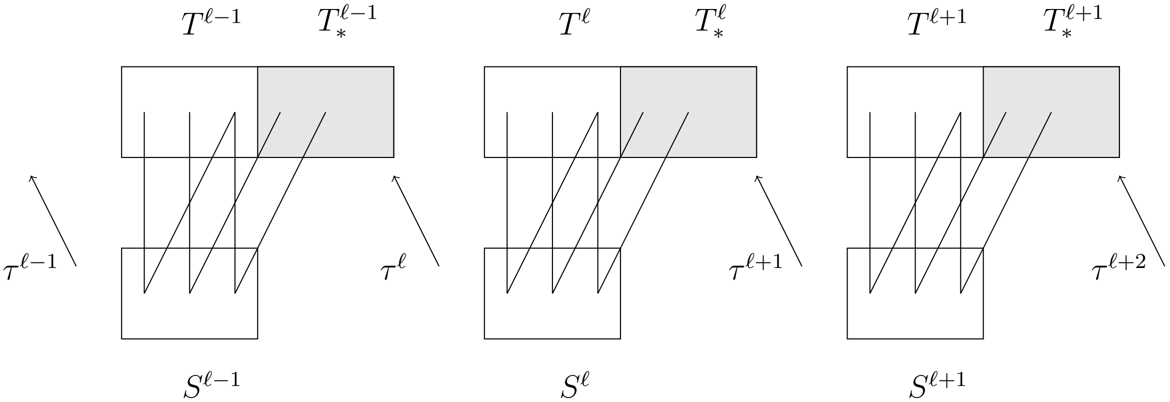
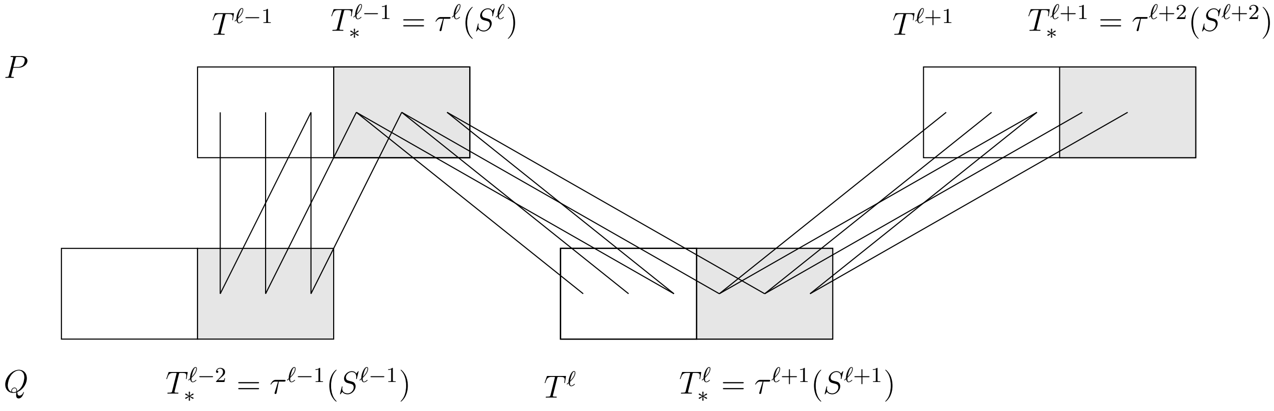


Figure 1: Illustration of the basic gadgets $G^\ell = (S^\ell, T^\ell, E^\ell)$ and the glueing maps $\tau^\ell : S^\ell \to T^{\ell-1}_*$. The terminal sets in each gadget are shaded.



$T^{\ell-1}$
$T^{\ell-1}_* = \tau^\ell(S^\ell)$
$T^{\ell+1}$
$T^{\ell+1}_* = \tau^{\ell+2}(S^{\ell+2})$
P
Q
$T^{\ell-2}_* = \tau^{\ell-1}(S^{\ell-1})$
T^ℓ
$T^\ell_* = \tau^{\ell+1}(S^{\ell+1})$

Figure 2: Illustration of the final graph $\widehat{G} = (P, Q, \widehat{E})$ obtained by gluing together basic gadgets $G^\ell = (S^\ell, T^\ell, E^\ell)$ from Fig. 1 using maps τ^ℓ.

Our construction: a geometric implementation of the instance of [ELSW13]. We present our lower bound construction in two steps. First, two illustrate our construction, we consider a simpler model than streaming, namely the *generalized online* model that we define below. The intuition behind the model is simple. In this model the edges of the graph are presented to the algorithm as a stream, and the algorithm must output a large matching at the end of the stream. Upon receiving an edge in the stream the algorithm can arbitrarily choose to either remember the edge or discard it (in this case the algorithm may not use the edge as part of the final output matching), and is constrained to remember at most s edges overall, i.e. the algorithm can only use edges that it remember when they arrived. The algorithm is not allowed to forget edges, i.e. the budget of s bounds the total number of edges remembered upon their arrival. The formal definition of the model is given in

Definition 3 (Generalized online algorithms) *In the* generalized online *setting the algorithm is presented with edges of a graph $G = (P, Q, E)$ as a stream of edges, and at every point must either commit to remembering the edge that has been presented to it, or discard the edge irrevocably. The total number of edges that the algorithm can remember is bounded by a parameter s. At the end of the stream the algorithm must output a matching M_{ALG} in the subset of edges that it remembered upon their arrival.*

This setting is easier than streaming, where the algorithm may maintain any small state. On the other hand, this setting is quite a bit more general than the online model, as the the algorithm may maintain significantly more edges than are needed to find a matching. It is not hard to see that this power renders standard hard instances for online algorithms very easy. In particular,

Lemma 4 *For every constant $\epsilon \in (0, 1)$ there exists a generalized online algorithm that remembers $s = O(n/\epsilon^2)$ edges and achieves a $(1 - \epsilon)$-approximation on the instance above.*

The algorithm is simple – one simply maintains a random sample of $O(n/\epsilon^2)$ edges of the input graph and outputs a maximum matching in the sample at the end. We include the proof of Lemma 4 in Appendix A for completeness. A similar claim is true for the 1-KVV instance – simply maintaining a uniform sample of $O(n/\epsilon^2)$ edges of the input graph will result in a $(1 - \epsilon)$-approximation.

To illustrate the techniques that lead to a proof of our main result (Theorem 1) in an easier setting, in Section 3 we prove the following:

Theorem 5 *There exists a distribution $\mathcal{D}$ on input graphs $G = (V, E)$ with n vertices such that any generalized algorithm that finds a $(\frac{1}{1+\ln 2} + \eta)$-approximation to the maximum matching in a graph G sampled from $\mathcal{D}$ with probability at least 0.9 must remember $\Omega(n \log n)$ edges.*

Note that even though the lower bound of $\Omega(n \log n)$ edges is not very strong from the standpoint of streaming algorithms, the result is interesting in light of Lemma 4. A major advantage of this setting is that it **(a)** allows for a rather clean construction and **(b)** illustrates all the central ideas of our main construction that leads to a proof of Theorem 1.

In what follows we give an outline of the proof of Theorem 5. The construction consists of two pieces. First, we define a construction of a basic gadget $G^\ell = (S^\ell, T^\ell, E^\ell)$, which is a geometric version of the α-KVV gadgets defined above. Second, we define maps τ^ℓ that glue together these gadgets to obtain the final input instance. Finally, we prove the $\frac{1}{1+\ln 2}$-hardness result in the generalized online model we defined above. The main ideas behind the first step are implicit in [Kap13], but we are able to present the construction in a different and arguably cleaner way (in particular, all bounds on the sizes of various sets are exact in our construction, which significantly simplifies presentation). The main contribution of the present paper lies in the second and third steps.

A geometric version of the α-KVV gadget $G = (S, T, E)$. Let $K, m \geq 1$ be large constant integers. Let

$$T = [m]^n$$

i.e. vertices in T are vectors of dimension n, with each co-ordinate taking values in $[m] = \{0, 1, 2, \ldots, m-1\}$. This way we have $N := |T| = m^n$, so $n = \Omega(\log N)$ for every constant m. The vertices on the S side of the bipartition will also be associated with points on the hypercube $[m]^n$, as we define below. We often treat vertices in T or S and points in $[m]^n$ interchangeably where this does not create confusion. The set S will consist of αK disjoint sets (we will use $\alpha = 1/2$ for our main result here, since we are implementing an instance that uses $1/2$-KVV gadgets). We will have

$$S = S_0 \uplus S_1 \uplus \ldots \uplus S_{\alpha K-1}.$$

Remark 6 (Use of $\uplus$ instead of $\cup$) *Note that we use the $\uplus$ as opposed to $\cup$ above. The reason for this is as follows. It is convenient to view vertices in G as points in the hypercube $[m]^n$. Formally, this means that our vertices are labeled by points in the hypercube. For example, the set T contains all of the hypercube $[m]^n$, and there is no confusion in using points in $[m]^n$ and vertices in T interchangeably. Vertices in S are also labeled by points in the hypercube, as we define below, but the labels are not distinct – there can be two vertices, say one in S_i and one in S_j for $i \neq j$, whose labels are the same (but labels are distinct within one set $S_i, i \in [\alpha \cdot K]$). Thus, we use the $\uplus$ sign to stress the fact that the union above is disjoint, even if different sets S_i may contain vertices with the same labels, to avoid confusion. Also, for two vertices $x, y \in S \cup T$ we write $x \asymp y$ to denote the relation 'the label of x equals the label of y' – see definition of S_k in* (4).

Before we define S, however, recall that an α-KVV gadget is parameterized by a permutation $\pi : [N] \to [N]$, and then every vertex $j \in S = \{0, 1, \ldots, N-1\}$ has an edge to vertices $i \in T$ such that $\pi(i) \geq j$. In our basic gadget the role of this permutation π is played by a nested sequence of subsets of T that we denote by

$$T = T_0 \supset T_1 \supset \ldots \supset T_{\alpha K} = T_*,$$

where the outermost set in the nested sequence is the entire T side of the bipartition, and the innermost set is the *terminal subset* T_*, which we refer to as the *terminal subcube* for reasons that will become clear shortly. These $\alpha K + 1$ nested sets will correspond to αK phases over which the gadget will be revealed to the algorithm (nothing is revealed in the last phase for certain technical reasons). In every phase $k \in [\alpha K]$ the algorithm will receive a carefully crafted subset of edges in $S_k \times T_k$, i.e. a subgraph induced by the k-th set S_k and the k-th set T_k in the nested sequence above. Once αK rounds are done, the next gadget will be presented, with vertices in the terminal subcube $T_* = T_{\alpha K}$ serving as the S side of the new gadget, as in the [ELSW13] construction outlined above.

We now define the nested sequence $T_0 \supset T_1 \supset \ldots \supset T_{\alpha K} = T_*$. Choose a subset $\mathbf{B} \subseteq [n]$ of coordinates to be used by our basic α-KVV gadget $G = (S, T, E)$ (we need to reserve other coordinate blocks for the other $L - 1$ gadgets – see below). Partition $\mathbf{B}$ into $\alpha K + 1$ disjoint roughly equal size subsets as

$$\mathbf{B} = \mathbf{B}_0 \cup \ldots \cup \mathbf{B}_{\alpha K},$$

where $|\mathbf{B}_k| = \frac{|\mathbf{B}|}{(\alpha K+1)}$. The nested sequence in T is parameterized by a vector

$$J \in \mathbf{B}_0 \times \ldots \times \mathbf{B}_{\alpha K}.$$

In other words, for every $k \in [\alpha K + 1]$ we have $J_k \in \mathbf{B}_k$. We use the notation $J_{<k} := (J_0, \ldots, J_{k-1})$ and $J_{\geq k} := (J_k, \ldots, J_{K/2})$. Let $T_0 = T$, and for every $k \in [\alpha K]$ let

$$T_{k+1} = \left\{ y \in T_k : y_{J_k}/m \in \left[0, 1 - \frac{1}{K-k}\right) \right\}, \tag{1}$$

so that

$$T_k = \left\{ y \in [m]^n : y_{J_s}/m \in \left[0, 1 - \frac{1}{K-s}\right) \text{ for all } s \in \{0, 1, \ldots, k-1\} \right\}. \tag{2}$$

One can show that $|T_k| = (1 - \frac{k}{K}) \cdot |T_0|$ for every $k \in [\alpha K + 1]$, i.e. the sizes of T_k decrease linearly in k – see Lemma 32[2]. The set S of vertices is naturally partitioned into disjoint subsets

$$S = S_0 \uplus S_1 \uplus \ldots \uplus S_{\alpha K - 1} \tag{3}$$

as follows. For every $k \in [\alpha K]$ we let

$$S_k \asymp \{x \in T_k : \text{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W}\} \tag{4}$$

In the definition above W is an integer parameter that we choose so that W divides m and $\text{wt}(x) = \sum_{j \in [n]} x_j$. Recall that for a pair of vertices $x, y \in P \cup Q$ we write $x \asymp y$ if their labels (vertices of the hypercube $[m]^n$ assigned to them) are the same. The notation in (4) above stands for S_k being a copy of the set of vertices on the rhs. Intuitively, the set S_k is a *subsample* of the set T_k that contains a $\frac{1}{K-k}$ fraction of points in T_k. A similar effect was achieved in [Kap13] by sampling vertices in T_k independently, but we find this deterministic construction cleaner to present. The key reason why we include vertices in S_k depending on the residue class of their weight modulo W is that we need this 'sampling mechanism' to 'accept' exactly a $\frac{1}{K-k}$ fraction of vertices along every coordinate aligned line as defined in (6) below; this property is crucial for establishing the existence of a large matching in our gadget – see Lemma 37. Using the weight of a point ensures that this property is satisfied. Another important observation is that $|S_k| = \frac{1}{K} \cdot |T_0|$ for every $k \in [\alpha K]$ (see Lemma 32 in Section 3). Intuitively, this means that in every round $k \in [\alpha K]$ the number of vertices arriving on the S side of the bipartition and revealing their edges to vertices in T_k is the same. We also define, for every $k \in [K/2]$ and $j \in \mathbf{B}_k$

$$\begin{aligned} T_k^j &= \left\{ y \in T_k : y_j/m \in \left[0, 1 - \frac{1}{K-k}\right) \right\} \\ S_k^j &= \left\{ x \in S_k : x_j/m \in \left[0, 1 - \frac{1}{K-k}\right) \right\}. \end{aligned} \tag{5}$$

Note that $T_k^{J_k} = T_{k+1}$ as per (1). The intuition behind these sets is that during phase k, i.e. when the edge set induced by S_k and T_k is revealed to the algorithm, the algorithm is presented with several possible options for the next set T_{k+1} in the nested sequence defined above. In other words, given the edge set presented in round k and before (we define the edge set below), any of the sets T_k^j for all $j \in \mathbf{B}_k$ (rather, any j in a subset $\mathring{\mathbf{B}}_j$ of $\mathbf{B}_j$ of comparale size) look like perfectly valid continuations for the nested sequence. The algorithm does not know which of them is important and hence most likely misses important edges in phase k – see below for more details.

Edges of G. Fix $k \in [\alpha K]$. For each coordinate $j \in \mathbf{B}_k$ for each $x \in [m]^n$ we denote the line in direction j going through x by

$$\text{line}_j(x) = \{x' \in [m]^n : x'_{-j} = x_{-j}\}, \tag{6}$$

where we write x_{-j} to denote the restriction of x on coordinates $[n] \setminus \{j\}$. Note that for every y, y' and every j one has either $\text{line}_j(y) = \text{line}_j(y')$ or $\text{line}_j(y) \cap \text{line}_j(y') = \emptyset$, i.e. lines in direction j partition T_k, and consequently also partition S_k. We now define the edges of G incident on S_k for every $k \in [\alpha K]$. For that we first need

[2] We note that lemma proved in Section 3 are presented for the setting of $\alpha = 1/2$. However, all of these bounds extend to other settings of α that are bounded away from 1.

Definition 7 (Line cover in direction j) *For every $j \in \mathbf{B}_k$ a collection $C_k^j \subseteq T_k$ of representative points is called a* line cover of T_k in direction j *if $T_k = \bigcup_{y \in C_k^j} \text{line}_j(y)$ and $\text{line}_j(y) \cap \text{line}_j(y') = \emptyset$ for every $y, y' \in C_k^j$, $y \neq y'$.*

Note that a line cover of T_k in direction j can be constructed by picking points $y \in T_k$ greedily until the union of lines in direction j through these points covers T_k.

The edge set induced by $S_k \cup T_k$ is defined as follows. First, we leave out a few coordinates from the current coordinate block $\mathbf{B}_k$, letting

$$\mathring{\mathbf{B}}_k \subset \mathbf{B}_k.$$

The reason for this will be clear once we define the glueing maps τ^ℓ below. For now it is only important that $|\mathring{\mathbf{B}}_k| \approx |\mathbf{B}_k|$, i.e. we did not lose too many coordinates by passing to $\mathring{\mathbf{B}}_k$. Now for every $j \in \mathring{\mathbf{B}}_k$ fix a line cover C_k^j of T_k in direction j (as per Definition 7).

For every $y \in C_k^j$ we include a complete bipartite graph between $\text{line}_j(y) \cap S_k^j$ and $\text{line}_j(y) \cap (T_k \setminus T_k^j)$.

In other words, let

$$E_k = \bigcup_{j \in \mathring{\mathbf{B}}_k} E_{k,j}, \tag{7}$$

where

$$E_{k,j} = \bigcup_{y \in C_k^j} (\text{line}_j(y) \cap S_k^j) \times (\text{line}_j(y) \cap (T_k \setminus T_k^j)). \tag{8}$$

One can show that the edge sets $E_{k,j}$ are disjoint (see Lemma 36). Note that E_k is fully determined by the first $k-1$ values of J, namely by the prefix $J_{<k}$. At this point we note that for our hard input distribution we choose

$$J \sim UNIF(\mathring{\mathbf{B}}_0 \times \ldots \times \mathring{\mathbf{B}}_{\alpha K}).$$

Crucially, conditioned on all edges received up to phase k, i.e. on $\bigcup_{s=0}^k E_s$, one has $J_k \sim UNIF(\mathring{\mathbf{B}}_k)$. This property is important for a key structural lemma, Lemma 10 below.

For every choice of $J \in \mathring{\mathbf{B}}_0 \times \ldots \times \mathring{\mathbf{B}}_{\alpha K}$ the edge set of G that we defined satisfies

Lemma 8 (Matching of S to $T \setminus T_*$; see Lemma 37 in Section 3) *There exists a matching of a $(1-O(1/K))$ fraction of S to $T \setminus T_*$ in E.*

This is a very natural property since the instance that we are defining is a version of the α-KVV gadget defined at the beginning of this section: those gadgets admitted a perfect matching of S to $T \setminus T_*$ (the optimal matching in that instance).

We now define the key property that underlies our lower bound (and, similarly, that of [Kap13]). For that we need the definition of a downset of a subset U of T:

Definition 9 (Down-set of a set in T) *For every $U \subseteq T$, $k \in [\alpha K]$, we define the* downset of U in S_k *by*

$$\textsc{DownSet}_k(U) = \{x \in S_k : \exists y \in U : y \asymp x\}$$

and define

$$\textsc{DownSet}(U) = \bigcup_{k \in [\alpha K]} \textsc{DownSet}_k(U).$$

Note that a given point in U has anywhere between 0 and αK images under the DOWNSET map: indeed, the downset of a point $x \in U$ is simply the set of points in the vertex sets $S_0, S_1, \ldots, S_{\alpha K-1}$ whose labels match the label of x. There can be up to αK such points, since labels are distinct within every single $S_i, i \in [\alpha K]$. It is also good to note that $S_k = \text{DOWNSET}_k(T_k)$ for every $k \in [\alpha K]$. Finally, it is important to note that for appropriately 'nice' subsets $U \subseteq T$ (see Lemma 39 in Section 3) one has

$$|\text{DOWNSET}_k(U)| = \frac{1}{K-k}|U|,$$

which is consistent with the idea that our weight condition in the definition of S_k (see (4)) essentially 'samples' points at rate $\frac{1}{K-k}$. The more important property of the DOWNSET map and the terminal subcube T_* is

Lemma 10 (Key structural property) *For $G = (S, T, E)$ defined as above, for every $E' \subset E$ one has*

$$E' \cap (\text{DOWNSET}(T_*) \times (T \setminus T_*)) \subseteq \bigcup_{k \in [\alpha K]} E' \cap E_{k,J_k}.$$

Note that intuitively the lemma above shows that only very special edges in E, namely the ones in E_{k,J_k}, cross from $\text{DOWNSET}(T_*)$ to the complement of T_* in T. This is intuitively useful since, as we verify below, for the right setting of parameters the cardinality of $\text{DOWNSET}(T_*)$ is quite a bit higher than that of T_*, meaning that if $E' \cap E_{k,J_k}$ is small, one gets a Hall's theorem witness set certifying that E' does not contain a large matching (as without these special edges all neighbors of $\text{DOWNSET}(T_*)$ are in T_*, a set of size significantly smaller than $\text{DOWNSET}(T_*)$).

Proof of Lemma 10: Consider an edge $(a, b) \in E' \cap E_k$ with $a \in \text{DOWNSET}_k(T_*)$ for some $k \in [\alpha K]$ and $b \in T \setminus T_*$. Recalling that $T_* = T_{\alpha K+1}$ and using (2), we get

$$T_* = \left\{ y \in [m]^n : y_{J_s}/m \in \left[0, 1 - \frac{1}{K-s}\right) \text{ for all } s \in \{0, 1, \ldots, \alpha K\} \right\}.$$

Further, since by Definition 9 the set $\text{DOWNSET}_k(T_*)$ is the set of vertices in S_k whose label matches the label of some vertex in T_*, the assumption that $a \in \text{DOWNSET}_k(T_*)$ implies

$$a_{J_s}/m \in \left[0, 1 - \frac{1}{K-s}\right) \text{ for all } s \in \{0, 1, \ldots, \alpha K\}.$$

On the other hand, since $b \in T \setminus T_*$ by assumption, there exists an index $r \in [\alpha K + 1]$ such that

$$b_{J_r}/m \in \left[1 - \frac{1}{K-r}, 1\right).$$

Thus, a and b differ on coordinate J_r. At the same time, we have $(a, b) \in E_k$ by assumption, which means by (7) that there exists a point $y \in C_k^j$ (a line cover of T_k in direction j) such that $a \in \text{line}_j(y)$ and $b \in \text{line}_j(y)$, which by definition of a line in direction j (see (6)) implies that $a_{-j} = y_{-j} = b_{-j}$. Since a and b differ on coordinate J_r, we now get that $j = J_r$. It remains to note that edges in E_k are all generated by lines in directions $j \in \mathbf{B}_k$. Since the blocks $\mathbf{B}_i$ are disjoint for different i by construction, we get that $J_r \in \mathbf{B}_k$. Thus, $r = k$ and $(a, b) \in E_{k,J_k}$, as required. ■

We now explain the significance of the key structural property above. Suppose that E' is the set of edges maintained by a generalized online algorithm that remembers at most $s = o(N \log N)$ edges. Taking the expectation of the rhs in Lemma 10 above with respect to J_k and conditioning $J_{<k}$, we get

$$\begin{aligned}\mathbf{E}_{J_k \sim UNIF(\mathring{\mathbf{B}}_k)}\left[|E' \cap E_{k,J_k}|\right] &= \sum_{j \in \mathring{\mathbf{B}}_k} |E' \cap E_{k,j}| \cdot \mathbf{Pr}[J_k = j] \\ &= \frac{1}{|\mathring{\mathbf{B}}_k|} \sum_{j \in \mathring{\mathbf{B}}_k} |E' \cap E_{k,j}| \\ &\leq \frac{s}{|\mathring{\mathbf{B}}_k|},\end{aligned} \tag{9}$$

where we used the fact that $\sum_{j \in \mathring{\mathbf{B}}_k} |E' \cap E_{k,j}| \leq |E'| \leq s$ for an algorithm that remembers at most s edges (since $E_{k,j}$ are disjoint), as well as the fact that J_k is independent of $J_{<k}$. At the same time we have $|\mathring{\mathbf{B}}_k| \geq n/2K$ or so, since we have n coordinates altogether, and $\alpha K \leq K$ phases to present the gadget to the algorithm over. If the parameter m is a constant (which it is by our parameter setting), we get $|\mathring{\mathbf{B}}_k| \geq n/2K = \Omega_K(\log N)$. Substituting into (9), we thus get

$$\mathbf{E}_{J_k \sim UNIF(\mathring{\mathbf{B}}_k)}\left[|E' \cap E_{k,J_k}|\right] = O_K(s/\log N).$$

Summing over all $\alpha K \leq K$ phases, we get that any generalized algorithm that remembers at most s edges can remember at most

$$O_K(s/\log N) = o(N)$$

edges from $E' \cap (\textsc{DownSet}(T_*) \times (T \setminus T_*))$ (the lhs in Lemma 10) since $s = o(N \log N)$ by assumption. Now we can upper bound the size of the matching that the set E' contains by exhibiting a vertex cover as follows:

Lemma 11 (Small vertex cover) *The size of the maximum matching in $E' \subseteq E$ is upper bounded by*

$$|E' \cap (\textsc{DownSet}(T_*) \times (T \setminus T_*))| + |S \setminus \textsc{DownSet}(T_*)| + |T_*|.$$

Proof: We construct a vertex cover by first adding one endpoint of every edge $e \in (\textsc{DownSet}(T_*) \times (T \setminus T_*))$. Then add T_* and $S \setminus \textsc{DownSet}(T_*)$. This is indeed a vertex cover: every edge $(u, v) \in E'$ either belongs to the first edge set, or has one endpoint in at least one of the other two. The lemma now follows. ■

Since, as we established above,

$$\mathbf{E}_J[|E' \cap (\textsc{DownSet}(T_*) \times (T \setminus T_*))|] = o(N), \tag{10}$$

it suffices to upper bound $|S \setminus \textsc{DownSet}(T_*)|$ and $|T_*|$. Since $T_* = T_{\alpha K}$, and we have $|T_k| = (1 - \frac{k}{K})|T_0|$ (see Lemma 32 in Section 3), we get that $|T_*| = (1 - \alpha)|T_0|$. We also have

$$\begin{aligned}|S \setminus \textsc{DownSet}(T_*)| &= |S| - |\textsc{DownSet}(T_*)| \\ &= \sum_{k \in [\alpha K]} |S_k| - \sum_{k \in [\alpha K]} |\textsc{DownSet}_k(T_*)| \\ &= \alpha K \cdot \frac{1}{K}|T_0| - \sum_{k \in [\alpha K]} \frac{1}{K - k}|T_*| \\ &\approx \left(\alpha - \int_0^\alpha \frac{1}{1-x} dx \cdot (1 - \alpha)\right)|T_0|.\end{aligned}$$

We used the fact that $|S_k| = \frac{1}{K}|T_0|$ (see Lemma 32) and $|\textsc{DownSet}_k(T_*)| = \frac{1}{K-k}|T_*|$ (see Lemma 39). Letting $\alpha = 1 - e^{-1}$ and using the fact that $\int_0^\alpha \frac{1}{1-x}dx = \ln \frac{1}{1-\alpha} = 1$, we get

$$|S \setminus \textsc{DownSet}(T_*)| \approx 2\alpha - 1,$$

and our upper bound on the size of the matching constructed by the algorithm becomes

$$\begin{aligned} |E' \cap (\textsc{DownSet}(T_*) \times (T \setminus T_*))| + |S \setminus \textsc{DownSet}(T_*)| + |T_*| &\approx ((2\alpha - 1) + (1 - \alpha))\,|T_0| \\ &= \alpha|T_0| \\ &= (1 - e^{-1})|T_0|. \end{aligned}$$

Thus, by Markov's inequality applied to $|E' \cap (\textsc{DownSet}(T_*) \times (T \setminus T_*))|$ no generalized online online algorithm that remembers $s = o(N \log N)$ edges can construct a matching of size larger than $(1 - e^{-1})|T_0|$ with any nontrivial probability. At the same time, if the terminal set T_* is perfectly matched to a separate set of vertices by an extra matching that arrives last in the stream, the size of the maximum matching in the graph is $\approx |T_0|$. This is exactly what happens in the $1 - e^{-1}$ hardness result of [Kap13], and brings us to our main challenge: how does one ensure that the terminal subset T_* is not merely matched to an unstructured set of vertices by a perfect matching, like in [Kap13], but rather that we are able to attach another α-KVV instance (in this case, for $\alpha = 1/2$) and continue?

Our contribution: glueing maps τ^ℓ and vertex cover construction in the $\frac{1}{1+\ln 2}$-hard instance. First, it is useful to observe that the construction of gluing maps τ^ℓ that associate different instances is nontrivial. For example, simply choosing τ^ℓ to be a random bijection from S^ℓ to T_*^ℓ will not work, as it will certainly destroy the delicate coordinate structure of the good vertex cover that we defined above. From now on we let $\alpha = 1/2$, as this discussion directly corresponds to our construction in Section 3.

We use L basic gadgets $G^\ell = (S^\ell, T^\ell, E^\ell)$, $\ell \in [L]$, and assume that L is even throughout the paper. We now define maps τ^ℓ identifying vertices in S^ℓ in $G^\ell = (S^\ell, T^\ell, E^\ell)$ with vertices in the terminal subcube $T_*^{\ell-1}$ of $G^{\ell-1} = (S^{\ell-1}, T^{\ell-1}, E^{\ell-1})$. For simplicity of notation we let $G' = (S', T', E')$ denote $G^\ell = (S^\ell, T^\ell, E^\ell)$, let $G = (S, T, E)$ denote $G^{\ell-1} = (S^{\ell-1}, T^{\ell-1}, E^{\ell-1})$, and adopt similar notation for all other relevant quantities. Specifically, let the disjoint coordinate blocks dedicated to these two gadgets be denoted by $\mathbf{B}' := \mathbf{B}^\ell, \mathbf{B} := \mathbf{B}^{\ell-1}$, and let the coordinate vectors be denoted by $J \in \mathbf{B}_0 \times \mathbf{B}_1 \times \ldots \times \mathbf{B}_{K/2}$, and $J' = \mathbf{B}'_0 \times \mathbf{B}'_1 \times \ldots \times \mathbf{B}'_{K/2}$ respectively. Thus, we define a bijection τ from S' to T_*:

$$\tau : S' \to T_*.$$

We start by defining τ on the sets S'_k for $k \in [K/2]$ (recall that $S' = S'_0 \uplus \ldots \uplus S'_{K/2-1}$ as per (3)). The restriction of τ to S'_k is denoted by τ_k:

$$\tau_k : S'_k \to T_*.$$

The images of τ_k that we define will be disjoint for different $k \in [K/2]$, i.e. these maps extend naturally to an injective map from the union of S'_k over all $k \in [K/2]$ to T_*. At this point our task is to map *subsampled* cubes S'_k (as per (4)) to a *non-sampled* terminal subcube T_* (as per (1)). Our first step is to design an intermediate mapping ρ that maps S'_k to a *non-sampled* subcube. We ensure that such a map uses only one special coordinate direction – for every $k \in [K/2]$ we denote this coordinate by $q_k \in \mathbf{B}_k$ and refer to it as the *compression index*. We refer to the corresponding map as the *densifying map* ρ, defined below. Note that in order to 'densify' S'_k we need to set the densification parameter to $\lambda = K - k$ (i.e., the inverse of the subsampling rate).

Definition 12 (**(λ, r)-densifying map**) *For $r \in [n]$ and integer $\lambda > 0$ the (λ, r)-densifying map $\rho : [m]^n \to [m]^n$ is defined as follows. We let $x \in [m]^n$, and write $x = (x', x''), x' \in [m]^{[n]\setminus\{r\}}, x'' \in [m]$. Write $x'' = aW + bW/\lambda + c$, where $a \in \{0, 1, \ldots, m/W - 1\}, b \in \{0, 1, \ldots, \lambda - 1\}$ and $c \in \{0, 1, \ldots, W/\lambda - 1\}$. We define $\rho(x)$ by letting, for $j \in [n]$:*

$$(\rho(x))_j := \begin{cases} aW/\lambda + c & \textit{if } j = r \\ x_j & \textit{o.w.} \end{cases}$$

The following lemma formalizes the densification property:

Lemma 13 (Densification of a subsampled set; see Lemma 39 in Section 3) *For every integer $\lambda \geq 2$, every $r \in [n]$, every $U \subseteq [m]^n$ that does not depend on coordinate r the (λ, r)-densifying map ρ (see Definition 12) maps*

$$\{x \in U : \mathit{wt}(x) \in [0, 1/\lambda) \cdot W \pmod{W}\}$$

bijectively to $\{x \in U : x_r/m \in [0, 1/\lambda)\}$.

Letting ρ_k be a $(K - k, q_k)$-densifying map, we get by Lemma 13 that

$$\rho_k(S'_k) = \left\{ x \in T'_k : x_{q_k}/m \in \left[0, \frac{1}{K-k}\right) \right\}. \tag{11}$$

This is progress, since now we need to design a map that maps the subcube $\rho_k(S'_k)$ above to T_*, which is also a subcube. We would like to design a mapping from S'_k to T_* that **(a)** 'uses' as few coordinates as possible and **(b)** maps entire subcubes of $\rho_k(S'_k)$ to subcubes of T_*. This second property **(b)** ensures that the structure of the good vertex cover we defined in Lemma 19 above can be translated from one instance of a basic gadget to another. A basic issue that we are facing now is that $\rho_k(S'_k)$ and T_* are subcubes, but have a different number of 'active dimensions': the former constrains variables in $J'_{<k}$ and q_k, while the latter constrains variables in J. To equalize this number let $\mathrm{Ext}_k \subseteq \mathbf{B}'_k$ is a subset of size $K/2 + 1 - k$ referred to as the *extension indices* in phase k – we will artificially add them to the index set $J'_{<k}$ and q_k to equalize the number of 'active' coordinates. $q_k \in \mathbf{B}'_k \setminus \mathrm{Ext}_k$ referred to as the *compression index* for the k-th phase of round ℓ. Now we can define the set $\mathring{\mathbf{B}}_k$ that we already used formally: $\mathring{\mathbf{B}}'_k = \mathbf{B}'_k \setminus (\mathrm{Ext}_k \cup \{q_k\})$. We also need an index $r \in \mathbf{B}_{K/2}$ that we refer to as the compression index for the terminal subcube T_*. Define index sets

$$I = J \cup \{r\} \subset [n] \tag{12}$$

and

$$I' = \{J'_0, \ldots, J'_{k-1}\} \cup \mathrm{Ext}_k \cup \{q_k\}. \tag{13}$$

Note that $|I| = |I'|$ – this is exactly why we defined the relevant compression and extension indices. This allows us to write

$$T_* \asymp A \times [m]^{[n]\setminus I}, \tag{14}$$

where

$$A = \left\{ x \in [m]^I : x_{J_s}/m \in \left[0, \frac{1}{K-i}\right) \text{ for all } s \in [K/2] \right\}.$$

Similarly, we write

$$\rho_k(S'_k) \asymp D_k \times [m]^{[n]\setminus I'}, \tag{15}$$

where as per (11)

$$D_k = \left\{ x \in [m]^{I'} : x_{i_s}/m \in \left[0, 1 - \frac{1}{K-s}\right) \text{ for all } s \in [k] \text{ and } x_{q_k}/m \in \left[0, \frac{1}{K-k}\right) \right\}.$$

We choose a bijection

$$M : \biguplus_{k\in[K/2]} D_k \to A, \tag{16}$$

which exists since the cardinalities of these sets are indeed equal (see derivation after (49) in Section 3). This lets us define another auxiliary transformation, referred to as the *subcube permutation map* Π_k. The composition of the densifying map ρ_k and the subcube permutation map Π_k gives us the glueing map τ.

Definition 14 (Subcube permutation map Π_k) *Define an injective map*

$$\Pi_k : \rho_k(S'_k) \to T_* \tag{17}$$

as follows. First, let $\eta : I \to I'$ be an arbitrary bijection. Given $x \in \rho_k(S'_k)$, write

$$x = (a, b, c),$$

where $a = x_{I'} \in D_k \subseteq [m]^{I'}$, $b = x_I \in [m]^I$ and $c = x_{[n]\setminus(I\cup I')} \in [m]^{[n]\setminus(I\cup I')}$. We let $\Pi_k(x) := z$, where

$$z_j = \begin{cases} b_{\eta^{-1}(j)} & \textit{if } j \in I' \\ (M(a))_{\eta(j)} & \textit{if } j \in I \\ c_j & \textit{o.w.} \end{cases}$$

In other words, $\Pi_k(x)$ replaces x_I with $x_{I'}$, replaces $x_{I'}$ with $M(x_I)$ and leaves coordinates outside of $I \cup I'$ untouched, so that

$$\Pi_k(z) = (b, M(a), c).$$

See Fig. 3 for an illustration.

A key property of the map Π_k is Lemma 46 (see Section 3). Intuitively, this lemma says that Π maps entire subspace to subspaces, which is a key property that we need our glueing maps to satisfy. This is because, as described in Section 2, if we were to upper bound the size of the maximum matching constructed by algorithm on a single gadget (like [Kap13] does), we would need to consider a vertex cover that is defined by the terminal subcube T_* and its downset. Our construction of a vertex cover in the concatenation of basic gadgets will use this approach, and we need (the downset of) the terminal subcube in one gadget to have 'nice structure' when mapped to another gadget using the glueing map τ. Our mapping Π_k is useful for this purpose, because the terminal subcube of a subsequent gadget is a subcube defined by coordinates in $[n] \setminus (I \cup I')$ (these coordinates are the set Λ above), and Lemma 46 shows that this set is still a subcube after an application of Π_k.

We can now define

Definition 15 (Glueing map τ) *For every $k \in [K/2]$ we define $\tau_k : S'_k \to T_*$ by letting $\tau_k(x) := \Pi_k(\rho_k(x))$. Define*

$$\tau : \biguplus_{k\in[K/2]} S'_k \to T_*$$

by letting $\tau(x) = \tau_k(x)$ for $x \in S'_k$.

This completes the definition of the glueing map τ. Note that so far we defined, for every $\ell \in [L]$, as basic gadget $G^\ell = (S^\ell, T^\ell, E^\ell)$ that is a geometric version of a 1/2-KVV gadget used in [ELSW13]. The gadgets are parameterized by sequences $J^\ell \in \mathring{\mathbf{B}}_0^\ell \times \cdots \times \mathbf{B}_{K/2}^\ell$, where

$$[n] = \mathbf{B}^0 \cup \mathbf{B}^1 \cup \ldots \cup \mathbf{B}^{L-1}$$

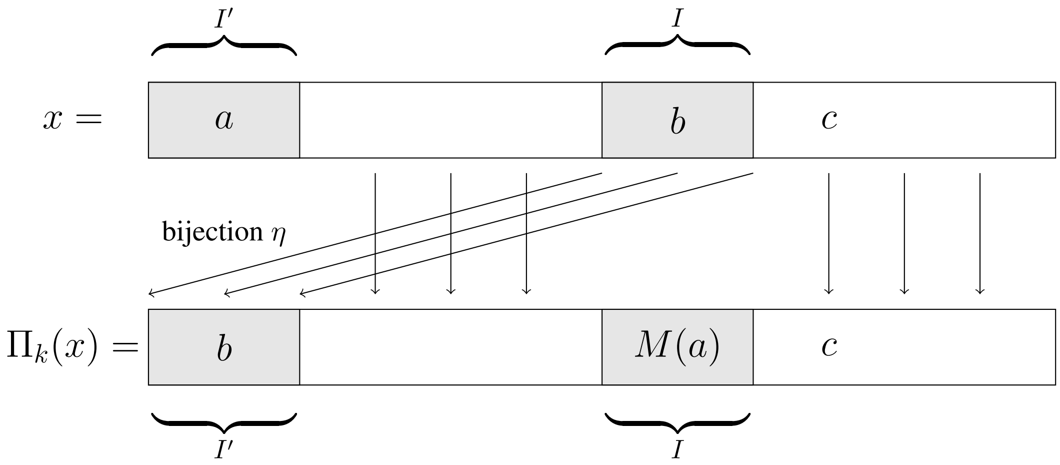


Figure 3: Illustration of the map Π_k. Note that Π_k simply leaves coordinates in $[n] \setminus (I \cup I')$, denoted by c, unchanged, copies coordinates in I to coordinates in I' using an arbitrarily chosen but fixed bijection η, and applies the map M to coordinates in I', assigning the result to coordinates in I.

is a partition of $[n]$ into coordinate blocks, one for each round $\ell \in [L]$, which are in turn partitioned into disjoint subblocks $\mathbf{B}^\ell = \mathbf{B}^\ell_0 \cup \ldots \cup \mathbf{B}^\ell_{K/2}$ corresponding to phases in which a given gadget is revealed to the algorithm. The sets $\mathring{\mathbf{B}}^\ell_k$ are subsets of $\mathbf{B}^\ell_k$ of comparable size, equal to $\mathbf{B}^\ell_k$ minus the extension and compression indices for the corresponding phase. We also defined bijections

$$\tau^\ell : S^\ell \to T^{\ell-1}_*$$

that we refer to as glueing maps. We now define our hard input distribution $\mathcal{D}$ on graphs $\widehat{G} = (P, Q, \widehat{E})$. A graph $\widehat{G} \sim \mathcal{D}$ is sampled as follows.

First, for every round $\ell \in [L]$ and phase $k \in [K/2]$ one **arbitrarily** selects the extension indices and compression indices appropriately – we do not dwell on this here and refer the reader to Section 3.7 for details. More importantly, one selects, for every $\ell \in [L]$ and $k \in [K/2]$, $J^\ell_k \sim UNIF(\mathring{\mathbf{B}}^\ell_k)$. Note that the vectors J^ℓ are the only random variables in the construction.

Edge set of $\widehat{G} = (P, Q, \widehat{E})$. We first define

$$\tau_*(x) = \begin{cases} \tau^\ell(x) & \text{if } x \in S^\ell \text{ for } \ell > 0 \\ x & \text{o.w..} \end{cases} \tag{18}$$

and for every edge $e = (u, v) \in E^\ell, u \in S^\ell, v \in T^\ell, \ell \in [L]$ define $\tau_*(e) = (\tau_*(u), v)$. We now let

$$\widehat{E} = \bigcup_{\ell \in [L]} \widehat{E}^\ell, \tag{19}$$

where

$$\widehat{E}^\ell = \bigcup_{k \in [K/2]} \bigcup_{j \in \mathring{\mathbf{B}}^\ell_k} \tau_*(E^\ell_{k,j}), \tag{20}$$

and $E^\ell_{k,j}$ is as in (8).

Ordering of edges of $\widehat{G}$ in the stream. The graph $G^\ell = (S^\ell, T^\ell, E^\ell)$ is presented in the stream over L *rounds* and $K/2$ *phases* as follows. For every $\ell \in \{1, \ldots, L-1\}$, for every $k \in [K/2]$, the edges in $\tau^\ell(E^\ell_k)$ are presented in the stream; the ordering within $\tau^\ell(E^\ell_k)$ is arbitrary.

The graph $\widehat{G}$ contains a nearly perfect matching (intuitively, this is because in our gadgets the set S^ℓ can always be nearly perfectly matched to $T^\ell \setminus T^\ell_*$):

Lemma 16 *The graph $\widehat{G} = (P, Q, \widehat{E})$ contains a matching of size $(1 - O(1/L))|P|$.*

The central part of our analysis is consists of designing a convenient vertex cover that lets us upper bound the size of matching constructed by a low space algorithm. The key concept underlying our analysis here is a map ν that we refer to as the *predecessor map*. The intuition for this map is a combination of the analysis of iterated KVV constructions in [ELSW13, HPT$^+$19], which essentially amount to a fixed point computation (the one in [ELSW13] is not phrased this way, but it appears that for our purposes this view is more useful).

Definition 17 (Predecessor map ν) *We define the map $\nu_{\ell,j}$ mapping* subsets $U \subseteq T^\ell$ *to subsets of $T^{\ell-j}$ by induction on $j \geq 0$ as follows. For $j = 0$ let $\nu_{\ell,0}(U) := U$. For $j > 0$ let*

$$\nu_{\ell,j}(U) := \tau^{\ell-(j-1)}(\textsc{DownSet}^{\ell-(j-1)}(\nu_{\ell,j-1}(U))).$$

We define the closure *map $\nu_{\ell,*}$ by*

$$\nu_{\ell,*}(U) := \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \nu_{\ell,j}(U).$$

We define the map $\mu_{\ell,j}$ mapping subsets $U \subseteq T^\ell$ *to subsets of $S^{\ell-j}$ by letting*

$$\mu_{\ell,j}(U) := \textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(U))$$

for $j = 0, \ldots, \ell$. We let

$$\mu_{\ell,*}(U) := \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \mu_{\ell,j}(U).$$

In the definition above we write $\textsc{DownSet}^\ell$ to denote the downset map of the ℓ-th basic gadget, and τ^ℓ the glueing map of the ℓ-th basic gadget.

We note that $\nu_{\ell,j}(U)$ is the set of vertices that the set U can be traced back to through j applications of the glueing maps τ, interleaved with applications of the $\textsc{DownSet}$ map (which is the reason we refer to ν as the predecessor map). Intuitively, this map is useful for our purposes because it allows us to find a vertex cover similar to what we obtained in Lemma 19 above, but at the same time consistent with the fixed point type argument implicit in [ELSW13] and explicit in [HPT$^+$19]. First let

$$\begin{aligned} A_P &= \bigcup_{\substack{\ell \in [L]\\ \ell \text{ even}}} \nu_{\ell,*}(T^\ell \setminus T^\ell_*) \\ A_Q &= \bigcup_{\substack{\ell \in [L]\\ \ell \text{ odd}}} \nu_{\ell,*}(T^\ell \setminus T^\ell_*). \end{aligned} \tag{21}$$

and

$$\begin{aligned} B_Q &= \bigcup_{\substack{\ell \in [L]\\ \ell \text{ even}}} \tau_*(\mu_{\ell,*}(T^\ell \setminus T^\ell_*)) \\ B_P &= \bigcup_{\substack{\ell \in [L]\\ \ell \text{ odd}}} \tau_*(\mu_{\ell,*}(T^\ell \setminus T^\ell_*)). \end{aligned} \tag{22}$$

We prove that $A_P \cap B_P = \emptyset$ and $A_P \cup B_P \approx P$ (similarly for A_Q and B_Q), as well as prove the following upper bounds on the cardinality of B_P and B_Q (which translates to the size of our vertex cover; recall that N is the number of vertices in T^ℓ):

Lemma 18 (See Lemma 70 in Section 3) *One has $|B_P| \leq (1 + O(1/L)) \cdot \frac{L}{2} \cdot \frac{N}{2} \cdot \frac{1}{1+\ln 2}$ and $|B_Q| \leq (1 + O(1/L)) \cdot \frac{L}{2} \cdot \frac{N}{2} \cdot \frac{1}{1+\ln 2}$.*

Lemma 19 (See Lemma 71 in Section 3) *For every matching M in G one has*

$$|M \cap (A_P \times (Q \setminus B_Q))| + \frac{1}{1 + \ln 2}|P| + O(|P|/L).$$

PROOF OUTLINE: Similarly to our analysis above with a single α-KVV gadget, we exhibit a vertex cover for M. Specifically, we add to the vertex cover one endpoint of every edge in

$$M \cap (A_P \times (Q \setminus B_Q)),$$

as well as all vertices in $P \setminus A_P \approx B_P$ and B_Q to the vertex cover. Note that this is indeed a vertex cover: $A_P \cap B_P = \emptyset$ and $A_Q \cap B_Q = \emptyset$, so every edge of M either has an endpoint in $P \setminus A_P$, or belongs to $A_P \times (Q \setminus B_Q)$, or belongs to $A_P \times B_Q$, in which case it has an endpoint in B_Q. The size of the vertex cover is

$$\begin{aligned} &|M \cap (A_P \times (Q \setminus B_Q))| + |P \setminus A_P| + |B_Q| \\ \approx &|M \cap (A_P \times (Q \setminus B_Q))| + |B_P| + |B_Q|, \end{aligned} \tag{23}$$

where we used the fact that $P \setminus A_P \approx B_P$ (see Lemma 19 for the precise version of this statement). By Lemma 18 we have

$$|B_P| \leq \frac{L}{2} \cdot \frac{N}{2} \frac{1}{1 + \ln 2}(1 + O(1/L))$$

and

$$|B_Q| \leq \frac{L}{2} \cdot \frac{N}{2} \frac{1}{1 + \ln 2}(1 + O(1/L)).$$

Putting the above together with (23) and recalling that

$$|P| = \left| \bigcup_{\text{even } \ell \in [L]} T^\ell \right| = L \cdot N/2$$

gives the result. ■

The equivalent of our key lemma(Lemma 10 in the simple analysis above) is given by

Lemma 20 (See Lemma 72 in Section 3) *For every matching $M \subseteq \widehat{E}$ one has*

$$M \cap (A_P \times (Q \setminus B_Q)) \subseteq \bigcup_{\ell \in [L], k \in [K/2]} \tau^\ell(E^\ell_{k, J^\ell_k}).$$

The proof relies on the fact that our glueing maps τ^ℓ only use a small number of coordinates, and map entire (sampled) subspaces in S'_k to subspaces in T_*.

Comparison of our vertex cover with that from Lemma 11. We note that, naturally, there are similarities between the vertex cover that we use to obtain the $\frac{1}{1+\ln 2}$ hardness and the vertex cover from Lemma 11. Indeed, as per the proof (sketch) of Lemma 11 the vertex cover contains one endpoint of every edge in

$$M \cap (A_P \times (Q \setminus B_Q)), \tag{24}$$

as well as all vertices in $P \setminus A_P \approx B_P$ and B_Q. Similarly to (10) above, we show that using Lemma 20 that the contribution of (24) can essentially be ignored. Thus, up to lower order terms, the vertex cover is the union of B_P and B_Q. Recall that as per (22)

$$B_Q = \bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \tau_*(\mu_{\ell,*}(T^\ell \setminus T^\ell_*))$$

and

$$B_P = \bigcup_{\substack{\ell \in [L] \\ \ell \text{ odd}}} \tau_*(\mu_{\ell,*}(T^\ell \setminus T^\ell_*)).$$

The application of τ_* above can be ignored for intuition, and we consider terms of the form

$$\mu_{\ell,*}(T^\ell \setminus T^\ell_*) = \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \mu_{\ell,j}(T^\ell \setminus T^\ell_*)$$

in the definition of B_Q above, where as per Definition 17 one has

$$\mu_{\ell,j}(T^\ell \setminus T^\ell_*) := \textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T^\ell_*))$$

for $j = 0, \ldots, \ell$. Note that the $j = 0$ term above in particular gives

$$\begin{aligned}
\mu_{\ell,0}(T^\ell \setminus T^\ell_*) &= \textsc{DownSet}^{\ell}(\nu_{\ell,0}(T^\ell \setminus T^\ell_*)) \\
&= \textsc{DownSet}^{\ell}(T^\ell \setminus T^\ell_*) \\
&= \textsc{DownSet}^{\ell}(T^\ell) \setminus \textsc{DownSet}^{\ell}(T^\ell_*) \\
&= S^\ell \setminus \textsc{DownSet}^{\ell}(T^\ell_*),
\end{aligned}$$

where we used the fact that $\nu_{\ell,0}$ is the identity map and the fact that $S^\ell = \textsc{DownSet}^{\ell}(T^\ell)$. Note that the last term in the equation above matches the second term in Lemma 11 (the first term is neglible, as we established). The other term in Lemma 11 is the terminal subcube itself, and is not present in our vertex cover since it is carefully split into different subsets, only some of which are added to the vertex cover – see Lemma 62 for a formal statement supporting this intuition (only a subset of the terms on the rhs of that lemma contribute to the vertex cover that we defined above, due to parity constraints).

Overview of the main construction. Our main construction, presented in Section 4 onwards, basically follows the logic outlined above and made precise in Section 3. However, instead of using orgthogonal directions, we use nearly orthogonal vectors, which gives the stronger lower bound of $N^{1+\Omega(1/\log\log N)}$ even for the streaming model of computation (as opposed to just our stylized generalized online algorithms model from Section 3). We made an effort to make the exposition of the main construction follow quite closely the simple model we present in Section 3. Still, the setting is different and new technical ideas are needed, mostly revolving around the fact that in the real construction we lose product structure, which leads to multiple error terms that need to be handled carefully. At a high level, we resolve this issue by defining various relevant maps 'locally'. Specifically, the definition of the *local permutation map* Π is roughly equivalent to (a concatenation of) our maps Π_k above, but works by first partitioning the space into appropriately defined low dimensional 'subspaces' and defining the map on every such subspace (see Section 5.10.2 for details). Intuitively, the reason for this is the fact that we only use nearly orthogonal vectors to define the edge set of the graph, and therefore all our maps need to be performing rather local operations, in order to avoid a degradation in the amount of orthogonality that we have.

Organization. The rest of the paper is organized as follows. In Section 3 we prove Theorem 5. Then main construction is then presented in Sections 4 onwards. We have invested effort into ensuring that the structure of the proof in Section 3 follows quite closely the structure of the main proof. As a consequence, subsections of Section 3 are in rather good correspondence with sections 4 onwards of the main paper.

3 Warm-up: a toy construction for the generalized online model

In this section we provide a toy version of our lower bound instance that shows that no generalized online algorithm (see Definition 3) with space $s = o(|P| \log |P|)$ can obtain a better (by an absolute constant) than $\frac{1}{1+\ln 2}$ approximation. Formally, we prove Theorem 5, restated here for convenience of the reader:

Theorem 5 *There exists a distribution $\mathcal{D}$ on input graphs $G = (V, E)$ with n vertices such that any generalized algorithm that finds a $(\frac{1}{1+\ln 2} + \eta)$-approximation to the maximum matching in G with probability at least 0.9 must remember $\Omega(n \log n)$ edges.*

We start by defining basic gadget graphs $G^\ell = (S^\ell, T^\ell, E^\ell)$ for $\ell \in [L]$ for an even integer L. Then input graph $G = (P, Q, E)$ is then an edge disjoint (but not vertex disjoint) union of graphs G^ℓ. Specifically, the P side of the bipartition will be

$$P = \bigcup_{\text{even } \ell \in [L]} T^\ell \tag{25}$$

and the Q side of the bipartition will be

$$Q = S^0 \cup \bigcup_{\text{odd } \ell \in [L]} T^\ell. \tag{26}$$

Note that among the sets S^ℓ only the set S^0 belongs to the vertex set of G.This is because we obtain G by glueing together instances of $G^\ell, \ell \in [L]$, using carefully designed maps τ^ℓ. For every $\ell = 1, \ldots, L/2 - 1$ the map τ^ℓ maps S^ℓ bijectively to a special subset $T_*^{\ell-1}$ of $T^{\ell-1}$ that we refer to as the *terminal subcube*. Thus we have

$$\tau^\ell : S^\ell \to T_*^{\ell-1}.$$

Organization. In what follows we first set up basic notation in Section 3.1, then specify global parameter setting in Section 3.2. We then define our basic gadgets G^ℓ in Section 3.3. We then define auxiliary transformations, namely sparsification and densification operations, in Section 3.4. We then define the glueing maps τ^ℓ in Section 3.5. Another key object in our analysis, the predecessor map ν, is defined in Section 3.6 – this map is key to defining a good upper bound for the matching M_{ALG} constructed by a small space algorithm. Finally we put the pieces together and give a proof of Theorem 5 in Section 3.7.

3.1 Notation and preliminaries

We start by setting up notation for the construction of basic gadgets $G^\ell = (S^\ell, T^\ell, E^\ell)$. For every $\ell \in [L]$ we have $|T^\ell| = N = m^n$, and have $|S^\ell| = N/2$. For every T^ℓ we select a subset (referred to as the terminal subcube of T^ℓ), denoted by T_*^ℓ, and for $\ell > 0$ carefully map vertices of S^ℓ bijectively to $T_*^{\ell-1}$. For every ℓ every vertex in T^ℓ and S^ℓ is equipped with a label from $[m]^n$ that we denote by

$$\text{label} : P \cup Q \to [m]^n.$$

For a pair of vertices $x \in P$ and $y \in Q$ we write $x \asymp y$ if $\text{label}(x) = \text{label}(y)$. For every $\ell \in [L]$ vertices in T^ℓ have distinct labels. The set S^ℓ will be partitioned into disjoint sets $S^\ell = S_0^\ell \cup \ldots \cup S_{K/2-1}^\ell$, and for every $k \in [K/2]$ vertices in S_k^ℓ also have distinct labels (their labels are a subset of the labels of T^ℓ). Thus, we will often think of vertices in G^ℓ as points in the hypercube when we think of vertices in T^ℓ, or vertices in S_k^ℓ and k is fixed. Throughout the paper we use the notation $[a] = \{0, 1, \ldots, a-1\}$ for a positive integer a. We partition $[n]$ into disjoint subsets

$$[n] = \mathbf{B}^0 \cup \mathbf{B}^1 \cup \ldots \cup \mathbf{B}^{L-1}$$

of equal size, i.e. $|\mathbf{B}^\ell| = n/L$ for every $\ell \in [L]$. For every ℓ we further partition $\mathbf{B}^\ell$ as

$$\mathbf{B}^\ell = \mathbf{B}_0^\ell \cup \ldots \cup \mathbf{B}_{K/2}^\ell,$$

where $|\mathbf{B}_k^\ell| = \frac{n}{L(K/2+1)}$, corresponding to $K/2$ *phases* in which the graph G^ℓ will be presented in the stream.

Special indices. The ℓ-th graph G^ℓ is parameterized by a vector

$$J^\ell \in \mathbf{B}_0^\ell \times \ldots \times \mathbf{B}_{K/2}^\ell$$

of indices. For $\ell \in [L]$ and $k \in [K]$ we use the notation $J_{<k}^\ell := (J_0^\ell, \ldots, J_{k-1}^\ell)$ and $J_{\geq k}^\ell := (J_k^\ell, \ldots, J_{K/2}^\ell)$.

Definition 21 (Compression and extension indices) *For every $\ell \in [L], \ell > 0$, the map τ^ℓ is parameterized by index $r^\ell \in \mathbf{B}_{K/2}^\ell$, referred to as the compression index for the terminal subcube T_*^ℓ, as well as a collection of auxiliary coordinates for every $k \in [K/2]$:*

- *$Ext_k^\ell \subseteq \mathbf{B}_k^\ell$ is a subset of size $K/2 + 1 - k$ referred to as the* extension indices *in phase k of round ℓ;*
- *$q_k^\ell \in \mathbf{B}_k^\ell \setminus Ext_k^\ell$ referred to as the* compression index *for the k-th phase of round ℓ.*

We let $\mathring{\mathbf{B}}_k^\ell = \mathbf{B}_k^\ell \setminus (Ext_k^\ell \cup \{q_k^\ell\})$ and let $\mathring{\mathbf{B}}_{K/2}^\ell = \mathbf{B}_{K/2}^\ell \setminus \{r^\ell\}$.

Property 22 *We will ensure that for every ℓ and $k \in [K/2+1]$ one has $J_k^\ell \in \mathring{\mathbf{B}}_k^\ell$, and in particular $J^\ell \cap \left(\{r^\ell\} \cup \bigcup_{k \in [K/2]} Ext_k^\ell \cup \{q_k^\ell\}\right) = \emptyset$.*

For convenience of notation we introduce

Definition 23 (Special coordinates) *For every ℓ we define the* special coordinates *in $\mathbf{B}^\ell$ by $\Psi(\mathbf{B}^\ell) := J^\ell \cup \{r^\ell\}$. We also let $\Psi(\mathbf{B}^{\geq \ell}) := \bigcup_{j \geq \ell} \Psi(\mathbf{B}^\ell)$.*

Definition 24 (Weight of $x \in [m]^n$) *For every $x \in [m]^n$ we define $wt(x) = \sum_{j \in [n]} x_j$.*

We will use

Claim 25 *There exists an absolute constant $C > 0$ such that for every integer $K > 0$ greater than an absolute constant one has* $\ln 2 - 1/K \leq \sum_{k \in [K/2]} \frac{1}{K-k} \leq \ln 2$.

Proof: One has for every integer $k \geq 0$, $\frac{1}{K} \cdot \frac{1}{1-(k+1)/K} \leq \int_{k/K}^{(k+1)/K} \frac{1}{1-x} dx \leq \frac{1}{K} \cdot \frac{1}{1-k/K}$, and hence $\sum_{k\in[K/2]} \frac{1}{K-k} = \frac{1}{K}\sum_{k\in[K/2]} \frac{1}{1-k/K} \leq \sum_{k\in[K/2]} \int_{k/K}^{(k+1)/K} \frac{1}{1-x} dx = \int_0^{1/2} \frac{1}{1-x} dx = \ln 2$, establishing the upper bound. Similarly,

$$\begin{aligned}\sum_{k\in[K/2]} \frac{1}{K-k} &= \frac{1}{K} - \frac{1}{K/2} + \frac{1}{K}\sum_{k=1}^{K/2} \frac{1}{1-k/K} \\ &\geq -\frac{1}{K} + \sum_{k\in[K/2]} \int_{k/K}^{(k+1)/K} \frac{1}{1-x} dx \\ &= -\frac{1}{K} + \int_0^{1/2} \frac{1}{1-x} dx = \ln 2 - \frac{1}{K},\end{aligned}$$

■

3.2 Parameter setting

We assume throughout this section that parameters m, W, K and L satisfy the following properties:

(p0) $(K-s) \mid W$ for all $s \in [K/2]$

(p1) $W \mid m/(K-s)$ for all $s \in [K/2]$

(p2) $L = K$

In the above we write $a \mid b$ if b/a is an integer.

Such a setting is possible:

Lemma 26 *For every constant K there exists a setting of parameters W, L and m that satisfies (p0)-(p2).*

Proof: Let $m = (\text{lcm}(K, K-1, \ldots, 3, 2, 1))^2$ and $W = \text{lcm}(K, K-1, \ldots, 3, 2, 1)$, where lcm stands for the least common multiple. ■

In what follows we define the individual instances G^ℓ and state their main properties in Section 3.3, then define the maps τ^ℓ in Section 3.5. We then give the proof of the lower bound in Section 3.7.

3.3 Basic gadgets G^ℓ

We give the construction of $G^\ell = (S^\ell, T^\ell, E^\ell)$ in this section. Since $\ell \in [L]$ is fixed, we write $T = T^\ell, S = S^\ell, E = E^\ell$ to simplify notation. We let $\mathbf{B} = \mathbf{B}^\ell$ and $\mathbf{B} = \mathbf{B}_0 \cup \ldots \cup \mathbf{B}_{K/2}$ denote the partition of $\mathbf{B}$.

Vertices of G: the T side of the bipartition. Let $K \geq 1$ be a large constant integer, let $m \geq 1$ be a large integer. Let

$$T = [m]^n$$

i.e. vertices in T are vectors of dimension n, with each co-ordinate taking values in $[m] = \{0, 1, 2, \ldots, m-1\}$. This way we have $N := |T| = m^n$, so $n = \Omega(\log N)$ for every constant m. The vertices on the S side of the bipartition will also be associated with points on the hypercube $[m]^n$, as defined below.

Let $T_0 = T$, and for every $k \in [K/2]$ let

$$T_{k+1} = \left\{ y \in T_k : y_{J_k}/m \in \left[0, 1 - \frac{1}{K-k}\right) \right\}, \tag{27}$$

so that

$$T_k = \left\{ y \in [m]^n : y_{J_s}/m \in \left[0, 1 - \frac{1}{K-s}\right) \text{ for all } s \in \{0, 1, \ldots, k-1\} \right\}. \tag{28}$$

Vertices of G: the S side of the bipartition. The set S of vertices is naturally partitioned into disjoint subsets

$$S = S_0 \uplus S_1 \uplus \ldots \uplus S_{K/2-1} \tag{29}$$

as follows. For every $k \in [K/2]$ we let

$$S_k \asymp \{x \in T_k : \mathrm{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W\} \tag{30}$$

In the definition above W is an integer parameter that we choose so that $W \mid m$ as per (p1), and $\mathrm{wt}(x) = \sum_{j\in[n]} x_j$ as per Definition 24.

Definition 27 (Down-set of a set in T) *For every $U \subseteq T$, $k \in [K/2]$, we define the* downset of U in S_k *by*

$$\textsc{DownSet}_k(U) = \{x \in S_k : \exists y \in U : y \asymp x\}$$

and define

$$\textsc{DownSet}(U) = \bigcup_{k\in[K/2]} \textsc{DownSet}_k(U).$$

We note that in the definition above the union on the rhs is a union of disjoint sets.

Remark 28 *We note that a given point in U has anywhere between 0 and $K/2$ images under the* DownSet *map.*

Remark 29 *Note that $S_k = \textsc{DownSet}_k(T_k)$ for every $k \in [K/2]$.*

Remark 30 *Note that if $U \subset T_k \setminus T_{k+1}$ for some $k \in [K/2]$, then $\textsc{DownSet}_s(U) = \emptyset$ for all $s \in \{k+1, \ldots, K/2-1\}$. Thus, in that case we have*

$$\textsc{DownSet}(U) = \bigcup_{s=0}^{k} \textsc{DownSet}_s(U).$$

We also let, for every $k \in [K/2]$ and $j \in \mathbf{B}_k$

$$\begin{aligned} T_k^j &= \left\{ y \in T_k : y_j/m \in \left[0, 1 - \frac{1}{K-k}\right) \right\} \\ S_k^j &= \left\{ x \in S_k : x_j/m \in \left[0, 1 - \frac{1}{K-k}\right) \right\}. \end{aligned} \tag{31}$$

Definition 31 (Terminal subcube) *We refer to $T_* := T_{K/2}$ as the* terminal subcube *of T.*

We gather basic bounds on the size of T_k's and S_k's in

Lemma 32 *One has*

(1) $|T_k| = (1 - \frac{k}{K}) \cdot |T_0|$ *for every $k \in [K/2+1]$;*

(2) $|S_k| = \frac{1}{K} \cdot |T_0|$ *for every $k \in [K/2]$.*

The proof is given in Appendix B.2. We now define the edge set of G.

Edges of G. Fix $k \in [K/2]$. For each coordinate $j \in \mathbf{B}_k$ for each $x \in [m]^n$ we denote the line in direction j going through x by

$$\text{line}_j(x) = \{x' \in [m]^n : x'_{-j} = x_{-j}\}, \tag{32}$$

where we write x_{-j} to denote the restriction of x on coordinates $[n] \setminus \{j\}$. We have

Lemma 33 *For all $s \in [K/2]$, for every $k \in [K/2]$, every $J_{<k} \in \mathbf{B}_{<k}$ for each $y \in T_k$ one has for each $j \in \mathbf{B}_k$*

(1) *$|line_j(y)| = m$ and $line_j(y) \subseteq T_k$;*

(2) *$|line_j(y) \setminus T_k^j| = \frac{1}{K-k} \cdot |line_j(y)|$;*

(3) *for every $y \in T_k$ one has $|line_j(y) \cap S_k| = \frac{1}{K-k} \cdot |line_j(y)|$;*

(4) *for every $y \in T_k$ one has $|line_j(y) \cap S_k^j| = \frac{1}{K-k} \cdot |line_j(y)| \cdot (1 - 1/(K-k))$.*

The proof of the lemma is given in Appendix B.1.

Remark 34 *Note that for every y, y' and every j one has either $line_j(y) = line_j(y')$ or $line_j(y) \cap line_j(y') = \emptyset$, i.e. lines in direction j partition T_k, and consequently also partition S_k.*

We now define the edges of G incident on S_k for every $k \in [K/2]$.

Definition 35 (Line cover in direction j) *For every $j \in \mathbf{B}_k$ a collection $C_k^j \subseteq T_k$ of representative points is called a* line cover of T_k in direction j *if*

$$T_k = \bigcup_{y \in C_k^j} line_j(y)$$

and $line_j(y) \cap line_j(y') = \emptyset$ for every $y, y' \in C_k^j$, $y \neq y'$.

Note that a line cover of T_k in direction j can be constructed by picking points $y \in T_k$ greedily until the union of lines in direction j through these points covers T_k. Every such line belongs to T_k by Lemma 33, **(1)**, and every two lines either are disjoint or coincide as per Remark 34.

Now for every j *except* the extension indices Ext_k or the compression index q_k (see Definition 21), i.e. for all

$$j \in \mathring{\mathbf{B}}_k = \mathbf{B}_k \setminus (\text{Ext}_k \cup \{q_k\}),$$

for every $y \in C_k^j$ for a line cover C_k^j of T_k in direction j (as per Definition 35), we include a complete bipartite graph between $\text{line}_j(y) \cap (T_k \setminus T_k^j)$ and $\text{line}_j(y) \cap S_k^j$. In other words, let $E = \bigcup_{k \in [K/2]} E_k$, where

$$E_k = \bigcup_{j \in \mathring{\mathbf{B}}_k} E_{k,j} \tag{33}$$

and

$$E_{k,j} = \bigcup_{y \in C_k^j} (\text{line}_j(y) \cap S_k^j) \times (\text{line}_j(y) \cap (T_k \setminus T_k^j)). \tag{34}$$

Note that E_k is fully determined by the first $k-1$ values of J, namely by the prefix $J_{<k}$.

We have

Lemma 36 *For every $k \in [K/2]$, every $i, j \in \mathbf{B}_k, i \neq j$, every $x \in C_k^i, y \in C_k^j$, where C_k^i and C_k^j are minimal line covers of T_k in direction i and j respectively, the edge sets*

$$(\mathit{line}_i(x) \cap S_k^i) \times (\mathit{line}_i(x) \cap (T_k \setminus T_k^i))$$

and

$$(\mathit{line}_j(y) \cap S_k^j) \times (\mathit{line}_j(y) \cap (T_k \setminus T_k^j))$$

are disjoint.

Proof: We argue by contradiction. Note that the complete graphs above have a nonempty intersection if and only if there exist a, b such that

$$a \in (\text{line}_i(x) \cap S_k^i) \cap (\text{line}_j(y) \cap S_k^j) \tag{35}$$

and

$$b \in (\text{line}_i(x) \cap (T_k \setminus T_k^i)) \cap (\text{line}_j(y) \cap (T_k \setminus T_k^j)). \tag{36}$$

Since $a, b \in \text{line}_j(y)$, we have

$$b_{-j} = a_{-j} \tag{37}$$

On the other hand, since $a \in \text{line}_i(x) \cap S_k^i \subseteq S_k^i$, we have by (31) that $a_i/m \in \left[0, 1 - \frac{1}{K-k}\right)$, and since $b \in \text{line}_i(x) \cap (T_k \setminus T_k^i) \subseteq T_k \setminus T_k^i$, we have by (27) that $b_i/m \in \left[1 - \frac{1}{K-k}, 1\right)$. On the other hand, we have $a_i = b_i$ by (37), a contradiction. ■

Lemma 37 (Matching of S to $T \setminus T_*$) *There exists a matching of a $(1 - O(1/K))$ fraction of S to $T \setminus T_*$ in E.*

Proof: For every $k \in [K/2]$ and $j = J_k$ we match almost all of S_k to $T_k \setminus T_k^j$ as follows. First note that for every $y, y' \in T_k$ one has either $\text{line}_j(y) = \text{line}_j(y')$ or $\text{line}_j(y) \cap \text{line}_j(y') = \emptyset$, i.e. lines in direction j partition T_k, and consequently also partition S_k. Thus, it suffices to define the matching on all lines in direction $j = J_k$ for each $y \in T_k$. By Lemma 33, **(2)**, we have

$$|\text{line}_j(y) \setminus T_k^j| = \frac{1}{K-k} \cdot |\text{line}_j(y)|$$

and by Lemma 33, **(3)**, one has

$$|\text{line}_j(y) \cap S_k^j| = \frac{1}{K-k} \cdot |\text{line}_j(y)|(1 + 1/(K-k)).$$

We match $\text{line}_j(y) \cap S_k$ to $\text{line}_j(y) \setminus T_k^j$ using the edges

$$(\text{line}_j(y) \cap S_k^j) \times (\text{line}_j(y) \cap (T_k \setminus T_k^j)),$$

which belong to E_k^j as per (34). This defines a matching of a $1 - O(1/K)$ fraction of S_k to T_k^j, where $j = J_k$.

Equipped with a matching of a $1 - O(1/K)$ fraction of S_k to T_k^j, where $j = J_k$, we now note that $T_{k+1} = T_k^j$ when $j = J_k$ for every $k \in [K/2]$ (see (31) and (27)), and therefore

$$T \setminus T_* = T \setminus T_{K/2} = \bigcup_{k \in [K/2]} T_k \setminus T_{k+1} = \bigcup_{k \in [K/2]} T_k \setminus T_k^{J_k},$$

where the union on the right hand side contains disjoint sets. Since $S_0, S_1, \ldots, S_{K/2-1}$ are disjoint, the union of constructed matchings is a matching of a $1 - O(1/K)$ fraction of S to $T \setminus T_*$, as required. ■

3.4 Subsampling and densification

Definition 38 *For a subset $F \subseteq [m]^n$ and a coordinate $r \in [n]$ we say that F* does not depend on r *if for every $x = (x_r, x_{-r}) \in F$ one has $(y, x_{-r}) \in F$ for every $y \in [m]$. Equivalently, F does not depend on r if*

$$F = \{z \in [m]^{[n]\setminus\{r\}} : z = x_{-r} \textit{ for some } x \in F\} \times [m].$$

Lemma 39 (Subsampling) *For every $U \subseteq [m]^n$ and $r \in [n]$ such that U does not depend on r (as per Definition 38), every integer λ such that $\lambda \mid W$, as long as $W \mid m$, one has*

$$|\{x \in U : \mathit{wt}(x) \in [0, 1/\lambda) \cdot W \pmod W\}| = \frac{1}{\lambda}|U|.$$

Proof: Let $U_{-r} := \{x_{-r} : x \in U\}$, where $x_{-r} \in [m]^{[n]\setminus\{r\}}$ stands for the projection of x to $[n] \setminus \{r\}$, and note that $U = U_{-r} \times [m]$. Furthermore, we have

$$\begin{aligned}&\{x \in U : \mathrm{wt}(x) \in [0, 1/\lambda) \cdot W \pmod W\}\\ &= \big\{(x', x'') \in U_{-r} \times [m] : \mathrm{wt}(x') + x'' \in [0, 1/\lambda) \cdot W \pmod W\big\}\end{aligned}$$

This in turn implies

$$\begin{aligned}&\big|\big\{(x', x'') \in U_{-r} \times [m] : \mathrm{wt}(x') + x'' \in [0, 1/\lambda) \cdot W \pmod W\big\}\big|\\ &= \sum_{x' \in U_{-r}} m \cdot \mathbf{Pr}_{x'' \sim UNIF([m])}[\mathrm{wt}(x') + x'' \in [0, 1/\lambda) \cdot W \pmod W]\end{aligned} \tag{38}$$

Since $W \mid m$ by assumption of the lemma, when x'' is uniformly random in $[m]$, $(\mathrm{wt}(x') + x'') \pmod W$ is uniformly random in $[W]$. Thus, for any $x' \in [m]^{[n]\setminus\{r\}}$ one has

$$\mathbf{Pr}_{x'' \sim UNIF([m])}[\mathrm{wt}(x') + x'' \in [0, 1/\lambda) \cdot W \pmod W] = \frac{1}{\lambda}.$$

Substituting this into (38), we get

$$\begin{aligned}&\big|\big\{(x', x'') \in U_{-r} \times [m] : \mathrm{wt}(x') + x'' \in [0, 1/\lambda) \cdot W \pmod W\big\}\big|\\ &= \sum_{x' \in U_{-r}} m \cdot \frac{1}{\lambda}\\ &= \frac{1}{\lambda}|U_{-r}| \cdot m\\ &= \frac{1}{\lambda}|U|,\end{aligned}$$

as required. ■

Definition 40 ((λ, r)-densifying map) *For $r \in [n]$ and integer $\lambda > 0$ the (λ, r)-densifying map $\rho : [m]^n \to [m]^n$ is defined as follows. We let $x \in [m]^n$, and write $x = (x', x'')$, $x' \in [m]^{[n]\setminus\{r\}}$, $x'' \in [m]$. Write*

$$x'' = aW + bW/\lambda + c,$$

where $a \in \{0, 1, \ldots, m/W - 1\}$, $b \in \{0, 1, \ldots, \lambda - 1\}$ and $c \in \{0, 1, \ldots, W/\lambda - 1\}$. We define $\rho(x)$ by letting, for $j \in [n]$:

$$(\rho(x))_j := \begin{cases} aW/\lambda + c & \textit{if } j = r\\ x_j & \textit{o.w.}\end{cases}$$

Remark 41 *Note that equivalently, one lets, for $j \in [n]$,*

$$(\rho(x))_j := \begin{cases} (x'' \pmod{W/\lambda}) + \frac{W}{\lambda} \cdot \lfloor x''/W)\rfloor & \textit{if } j = r \\ x_j & \textit{o.w.} \end{cases}$$

We have

Lemma 42 (Densification of a subsampled set) *For every integer $\lambda \geq 2$, every $r \in [n]$, every $U \subseteq [m]^n$ that does not depend on coordinate r (as per Definition 38) the (λ, r)-densifying map ρ (see Definition 40) maps*

$$\{x \in U : \mathit{wt}(x) \in [0, 1/\lambda) \cdot W \pmod{W}\}$$

bijectively to $\{x \in U : x_r/m \in [0, 1/\lambda)\}$.

Proof: We first prove that

$$\rho\left(\{x \in U : \mathrm{wt}(x) \in [0, 1/\lambda) \cdot W \pmod{W}\}\right) \subseteq \{x \in U : x_r/m \in [0, 1/\lambda)\}\,. \tag{39}$$

We let $x \in [m]^n$, and write $x = (x', x'')$, $x' \in [m]^{[n]\setminus\{r\}}$, $x'' \in [m]$. Write

$$x'' = aW + bW/\lambda + c,$$

where $a \in \{0, 1, \ldots, m/W - 1\}, b \in \{0, 1, \ldots, \lambda - 1\}$ and $c \in \{0, 1, \ldots, W/\lambda - 1\}$. As per Definition 40 one has for $j \in [n]$

$$(\rho(x))_j := \begin{cases} (aW/\lambda + c) \pmod{m/\lambda} & \text{if } j = r \\ x''_j & \text{o.w.} \end{cases}$$

Since U does not depend on r by assumption and

$$0 \leq a(W/\lambda) + c \leq (m/W - 1)(W/\lambda) + (W/\lambda - 1) = m/\lambda - 1,$$

we have $\rho(x) \in \{x \in U : x_r/m \in [0, 1/\lambda)\}$, as required. This establishes (39).

We now establish injectivity. Let $U_{-r} := \{x_{-r} : x \in U\}$, where $x_{-r} \in [m]^{[n]\setminus\{r\}}$ stands for the projection of x to $[n] \setminus \{r\}$, and note that $U = U_{-r} \times [m]$ since U does not depend on r by assumption. Furthermore, we have

$$\begin{aligned} &\{x \in U : \mathrm{wt}(x) \in [0, 1/\lambda) \cdot W \pmod{W}\} \\ &= \left\{(x', x'') \in U_{-r} \times [m] : \mathrm{wt}(x') + x'' \in [0, 1/\lambda) \cdot W \pmod{W}\right\} \end{aligned} \tag{40}$$

Now pick $x''_1, x''_2 \in [m]$ such that

$$\left\{(x', x''_i) \in U_{-r} \times [m] : \mathrm{wt}(x') + x''_i \in [0, 1/\lambda) \cdot W \pmod{W}\right\} \text{ for } i \in \{1, 2\}. \tag{41}$$

Write

$$x''_1 = a_1 W + b_1 W/\lambda + c_1 \;\text{ and }\; x''_2 = a_2 W + b_2 W/\lambda + c_2,$$

where $a_i \in \{0, 1, \ldots, m/W - 1\}, b_i \in \{0, 1, \ldots, \lambda - 1\}$ and $c_i \in \{0, 1, \ldots, W/\lambda - 1\}$, $i \in \{1, 2\}$. Suppose towards a contradiction that $\rho((x', x''_1)) = \rho((x', x''_2))$, i.e., that $a_1 = a_2$ and $c_1 = c_2$. We show that $b_1 = b_2$. We have

$$\begin{aligned} ((\mathrm{wt}(x') + x''_1) - (\mathrm{wt}(x') + x''_2)) \pmod{W} &= (x''_1 - x''_2) \pmod{W} \\ &= ((b_1 - b_2)W/\lambda) \pmod{W} \end{aligned} \tag{42}$$

Since $|b_1 - b_2| < \lambda$, $b_1 \neq b_2$ would contradict (41). Thus, we have $b_1 = b_2$, and the map ρ is injective.

Finally, note that by Lemma 39 one has

$$|\{x \in U : \mathrm{wt}(x) \in [0, 1/\lambda) \cdot W \pmod{W}\}| = \frac{1}{\lambda} \cdot |U| = |\{x \in U : x_r/m \in [0, 1/\lambda)\}|\,,$$

and hence ρ is a bijection. ■

3.5 Maps τ^ℓ identifying the basic gadgets

In this section we define the map τ^ℓ identifying vertices in S^ℓ in $G^\ell = (S^\ell, T^\ell, E^\ell)$ with vertices in $T_*^{\ell-1}$ of $G^{\ell-1} = (S^{\ell-1}, T^{\ell-1}, E^{\ell-1})$ for every $\ell \in [L], \ell > 0$:

$$\tau^\ell : S^\ell \to T_*^{\ell-1}.$$

Since ℓ is fixed for most of the section, we omit the superscript ℓ. We let $G' = (S', T', E')$ denote $G^\ell = (S^\ell, T^\ell, E^\ell)$, let $G = (S, T, E)$ denote $G^{\ell-1} = (S^{\ell-1}, T^{\ell-1}, E^{\ell-1})$, adopting similar notation for all other relevant quantities. Specifically, let $\mathbf{B}' := \mathbf{B}^\ell, \mathbf{B} := \mathbf{B}^{\ell-1}$, and let the special coordinate vectors be denoted by $J \in \mathbf{B}_0 \times \mathbf{B}_1 \times \ldots \times \mathbf{B}_{K/2}$, and $J' = \mathbf{B}'_0 \times \mathbf{B}'_1 \times \ldots \times \mathbf{B}'_{K/2}$ respectively. Thus, we define a bijection τ from S' to T_*:

$$\tau : S' \to T_*.$$

We start by defining τ on the sets S'_k for $k \in [K/2]$ (recall that $S' = S'_0 \uplus \ldots \uplus S'_{K/2-1}$). The restriction of τ to S'_k is denoted by τ_k:

$$\tau_k : S'_k \to T_*.$$

The images of τ_k that we define will be disjoint for different $k \in [K/2]$, i.e. these maps extend naturally to an injective map from the union of S'_k over all $k \in [K/2]$ to T_*.

Defining τ_k. Fix $k \in [K/2]$. Let $r \in \mathbf{B}$ denote the compression index of the terminal subcube T_*. Let $\mathrm{Ext}_k \subseteq \mathbf{B}'_k$ and $q_k \in \mathbf{B}'_k$ denote the k-th extension and compression indices (see Definition 21). Let ρ_k be a $(K-k, q_k)$-densifying map as per Definition 40. Now note that T'_k does not depend on q_k by Property 22. We thus have by Lemma 42 that

$$\rho_k(S'_k) = \left\{ x \in T'_k : x_{q_k}/m \in \left[0, \frac{1}{K-k}\right) \right\} \tag{43}$$

and ρ_k maps S'_k to the set on the rhs of (43) bijectively.

Now define index sets

$$I = J \cup \{r\} \subset [n] \tag{44}$$

and

$$I'_k = \{J'_0, \ldots, J'_{k-1}\} \cup \mathrm{Ext}_k \cup \{q_k\}. \tag{45}$$

We sometimes write I' instead of I'_k when the value of k is clear from context. Note that $I = \Psi(\mathbf{B})$ and for every k

$$|I| = |I'_k| = K/2 + 2. \tag{46}$$

This allows us to write

$$T_* \asymp A \times [m]^{[n]\setminus I}, \tag{47}$$

where

$$A = \left\{ x \in [m]^I : x_{J_s}/m \in \left[0, \frac{1}{K-s}\right) \text{ for all } s \in [K/2] \right\}.$$

Similarly, we write

$$\rho_k(S'_k) \asymp D_k \times [m]^{[n]\setminus I'_k}, \tag{48}$$

where as per (43)

$$D_k = \left\{ x \in [m]^{I'_k} : x_{i_s}/m \in \left[0, 1 - \frac{1}{K-s}\right) \text{ for all } s \in [k] \text{ and } x_{q_k}/m \in \left[0, \frac{1}{K-k}\right) \right\}.$$

Choose a bijection

$$M : \biguplus_{k \in [K/2]} D_k \to A. \tag{49}$$

This is possible because

$$\begin{aligned}
\sum_{k \in [K/2]} |D_k| &= \sum_{k \in [K/2]} \frac{|\rho_k(S'_k)|}{m^{n-|I'_k|}} && \text{(by (48))} \\
&= \sum_{k \in [K/2]} \frac{|S'_k|}{m^{n-|I'_k|}} && \text{(since } \rho_k \text{ is a bijection)} \\
&= \frac{1}{K} \sum_{k \in [K/2]} \frac{|T_0|}{m^{n-|I'_k|}} && \text{(since } |S'_k| = \frac{1}{K}|T_0| \text{ for all } k \in [K/2] \text{ by Lemma 32, } \textbf{(2)}\text{)} \\
&= \frac{1}{K} \sum_{k \in [K/2]} \frac{|T_0|}{m^{n-|I|}} && \text{(since } |I| = |I'_k| \text{ by (46))} \\
&= \frac{1}{2} \frac{|T_0|}{m^{n-|I|}} \\
&= \frac{|T_*|}{m^{n-|I|}} && \text{(since } |T_*| = |T_{K/2}| = \frac{1}{2}|T_0| \text{ by Lemma 32, } \textbf{(1)}\text{)} \\
&= |A|. && \text{(by (47))}
\end{aligned}$$

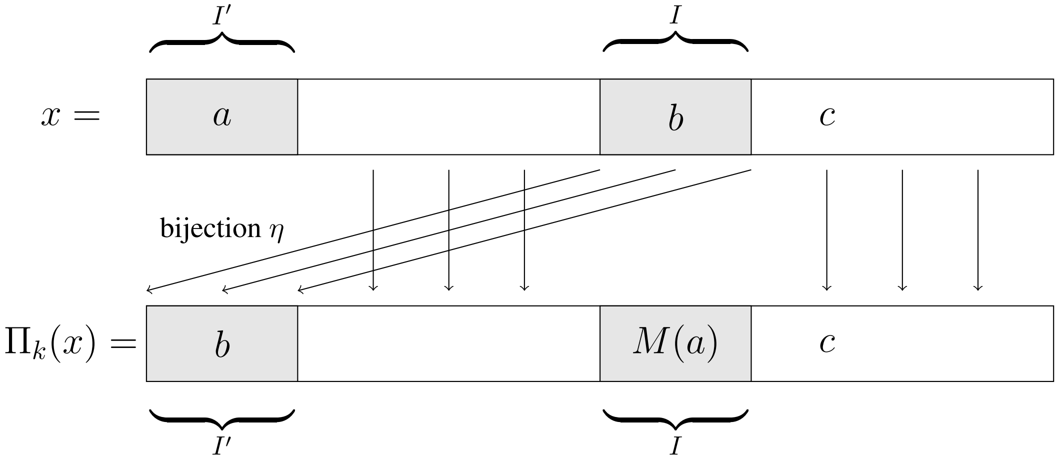


Figure 4: Illustration of the map Π_k. Note that Π_k simply leaves coordinates in $[n] \setminus (I \cup I')$, denoted by c, unchanged, copies coordinates in I to coordinates in I' using an arbitrarily chosen but fixed bijection η, and applies the map M to coordinates in I', assigning the result to coordinates in I.

Remark 43 *Note that for every $k \in [K/2]$ the set D_k is determined by I and I'_k, and A is determined by I. Thus, we can construct the map M incrementally, by fixing $M|_{D_k} : D_k \to A$ as soon as I'_k becomes known. The latter in fact amounts to knowing $\{J'_0, J'_1, \ldots, J'_{k-1}\}$, since we fix Ext_k and q_k for our hard input distribution.*

Definition 44 (Subcube permutation map Π_k) *Define an injective map*

$$\Pi_k : \rho_k(S'_k) \to T_* \tag{50}$$

by letting $\Pi_k(x)$ replace x_I with $x_{I'}$ (where $I' = I'_k$), replace $x_{I'}$ with $M(x_I)$ and leave coordinates outside of $I \cup I'$ untouched, so that

$$\Pi_k(z) = (b, M(a), c).$$

See Fig. 4 for an illustration.

Formally, we first let $\eta : I \to I'$ be an arbitrary bijection. Given $x \in \rho_k(S'_k)$, write

$$x = (a, b, c),$$

where $a = x_{I'} \in D_k \subseteq [m]^{I'}$, $b = x_I \in [m]^I$ and $c = x_{[n]\setminus(I\cup I')} \in [m]^{[n]\setminus(I\cup I')}$. We let

$$\Pi_k(x) := z,$$

where

$$z_j = \begin{cases} b_{\eta^{-1}(j)} & \textit{if } j \in I' \\ (M(a))_{\eta(j)} & \textit{if } j \in I \\ c_j & \textit{o.w.} \end{cases}$$

We will use

Definition 45 (Rectangle) *We say that a set R is a rectangle in $I \subset [n]$ if $R \subseteq [m]^I = \prod_{i\in I} A_i$, where $A_i \subseteq [m]$ for every $i \in I$ (i.e., R is the direct product of the sets $A_i, i \in I$).*

The following lemma establishes a key property of the map Π_k:

Lemma 46 (Basic properties of the permutation maps Π_k) *For every $k \in [K/2]$, every $x \in [m]^{I'}$ (where $I' = I'_k$), every rectangle R in $\Lambda \subseteq [n] \setminus (I \cup I')$ the rectangle*

$$F = \{x\} \times R \times [m]^{[n]\setminus(\Lambda\cup I')}$$

satisfies

$$\Pi_k(F) = \{M(x)\} \times R \times [m]^{[n]\setminus(\Lambda\cup I)},$$

where $M(x) \in [m]^I$ (as per (49)).

Remark 47 *Intuitively, this lemma says that Π maps entire subspace to subspaces, which is a key property that we need our glueing maps to satisfy. This is because, as described in Section 2, if we were to upper bound the size of the maximum matching constructed by algorithm on a single gadget (like [Kap13] does), we would need to consider a vertex cover that is defined by the terminal subcube T_* and its downset. Our construction of a vertex cover in the concatenation of basic gadgets will use this approach, and we need (the downset of) the terminal subcube in one gadget to have 'nice structure' when mapped to another gadget using the glueing map τ. Our mapping Π_k is useful for this purpose, because the terminal subcube of a subsequent gadget is a subcube defined by coordinates in $[n] \setminus (I \cup I')$ (these coordinates are the set Λ above), and Lemma 46 shows that this set is still a subcube after an application of Π_k.*

This lemma is crucially used in Lemma 65, and the rectangle R in question there is the following. We first take some rectangle F in $\Psi(\mathbf{B}^\ell)$ for some $\ell > 0$. Then we apply j iterations of the predecessor map ν to it, namely apply the map $\nu_{\ell,j}$. This results in a rectangle in some subset Λ of coordinates with $\Lambda \subseteq \Psi(\mathbf{B}^{\ell+j})$ – this rectangle essentially contains information about the trajectory of F through repeated invocations of the predecessor map ν. Lemma 46 essentially shows that the permutation map Π_k does not interfere with this information as long as Λ does not overlap with I', which is the case in the application in Lemma 65.

Proof: We first rewrite the input rectangle F as

$$F = \{x\} \times [m]^I \times \left(R \times [m]^{[n]\setminus(\Lambda \cup I' \cup I)}\right).$$

We can thus express every

$$z \in \{x\} \times [m]^I \times \left(R \times [m]^{[n]\setminus(\Lambda \cup I' \cup I)}\right)$$

as

$$z = (a, b, c),$$

where $a \in [m]^{I'}$, $b \in [m]^I$ and $c \in [m]^{[n]\setminus(I' \cup I)}$, and get by Definition 44

$$\Pi_k(z) = (b, M(a), c).$$

Thus, as z ranges over $\{x\} \times [m]^I \times \left(R \times [m]^{[n]\setminus(\Lambda \cup I' \cup I)}\right)$, the parameter a always equals x, b ranges over $[m]^I$ and c ranges over $R \times [m]^{[n]\setminus(\Lambda \cup I' \cup I)}$. Hence,

$$\Pi_k(F) = \{M(a)\} \times [m]^I \times R \times [m]^{[n]\setminus(\Lambda \cup I' \cup I)} = \{M(a)\} \times R \times [m]^{[n]\setminus(\Lambda \cup I')},$$

as required. ■

We can now define

Definition 48 (Glueing map τ) *For every $k \in [K/2]$ we define $\tau_k : S'_k \to T_*$ by letting*

$$\tau_k(x) := \Pi_k(\rho_k(x)). \tag{51}$$

Define

$$\tau : \biguplus_{k \in [K/2]} S'_k \to T_*$$

by letting $\tau(x) = \tau_k(x)$ for $x \in S'_k$.

Lemma 49 (Basic properties of τ) *The map τ is a bijective map from $\biguplus_{k \in [K/2]} S'_k$ to T_*.*

Proof: The map ρ_k is bijective by Lemma 42 (see discussion after (43) for more details) . The map Π_k is injective, since M is injective. Bijectivity of τ follows from the fact that images of D_k under M are disjoint, and since $\sum_{k \in [K/2]} |D_k| = |A|$ by (49). ■

Definition 50 (Basic coordinates Γ) *We define the set of* basic coordinates *as*

$$\Gamma = \bigcup_{\ell \in [L]} \left(\Psi(\mathbf{B}^\ell) \cup \bigcup_{k \in [K/2]} \left(\mathit{Ext}^\ell_k \cup \{q^\ell_k\} \right) \right).$$

Remark 51 *Note that $\Gamma \subseteq [n]$ contains all coordinates that densifying maps (Definition 40) and permutation maps (Definition 44) use across all L gadgets G^ℓ. This fact is crucial for the following lemma (Lemma 57).*

Lemma 52 *For every $\ell \in [L], \ell < L - 1$, every $x, y \in T^\ell_*$ such that $x_i = y_i$ for all $i \in \Gamma$ there exists $a \in [K/2]$ and $u, v \in S^{\ell+1}_a$ such that*

(1) *$x = \tau^{\ell+1}(u)$ and $y = \tau^{\ell+1}(v)$;*

(2) $u_\Gamma = v_\Gamma$.

Proof: We let $\tau := \tau^{\ell+1}$, $T_* := T_*^\ell$, $S' := S^{\ell+1}$. We also let $J := J^\ell, J' := J^{\ell+1}$, $r := r^{\ell+1}$, and $q_i := q_i^{\ell+1}$ and $\mathrm{Ext}_i := \mathrm{Ext}_i^{\ell+1}$ for $i \in [K/2]$ to simplify notation.

Since τ maps $S' = \bigcup_{f \in [K/2]} S'_f$ bijectively to T_*, there exist $f, g \in [K/2]$ and $u \in S'_f, v \in S'_g$ such that $x = \tau(u)$ and $y = \tau(v)$. Define

$$\begin{aligned} I &:= J^\ell \cup \{r^\ell\} \\ I'_f &:= J'_{<f} \cup \mathrm{Ext}_f \cup \{q_f\} \\ I'_g &:= J'_{<g} \cup \mathrm{Ext}_g \cup \{q_g\}. \end{aligned}$$

By Definition 48 this means that

$$x = \Pi_f(\rho_f(u)) \text{ and } y = \Pi_g(\rho_g(v)),$$

where Π_f, Π_g are subcube permutation maps as per Definition 44 and ρ_f and ρ_g are $(K - f, q_f)$ and $(K - g, q_g)$-densifying maps as per Definition 40 respectively. Now write

$$\rho_f(u) = (a_u, b_u, c_u), \text{ where } a_u \in D_f \subseteq [m]^{I'_f}, b_u \in [m]^I \text{ and } c_u \in [m]^{[n]\setminus(I \cup I'_f)}.$$

Similarly, write

$$\rho_g(v) = (a_v, b_v, c_v), \text{ where } a_v \in D_g \subseteq [m]^{I'_g}, b_v \in [m]^I \text{ and } c_v \in [m]^{[n]\setminus(I \cup I'_g)}.$$

Then we have by Definition 44

$$x = \Pi_f(\rho_f(u)) = \Pi_f((a_u, b_u, c_u)) = (b_u, M(a_u), c_u), \tag{52}$$

where the partition of coordinates on the right hand side is $I'_f \cup I \cup ([n] \setminus (I'_f \cup I))$ and

$$y = \Pi_g(\rho_g(v)) = \Pi_g((a_v, b_v, c_v)) = (b_v, M(a_v), c_v), \tag{53}$$

where the partition on the right hand side is $I'_g \cup I \cup ([n] \setminus (I'_g \cup I))$. Here $M : \biguplus_{k \in [K/2]} D_k \to A$ is the bijective map from (49). Since $x_\Gamma = y_\Gamma$ and $I = \Psi(\mathbf{B}^\ell) \subseteq \Gamma$ (as per Definition 50), we have $M(a_u) = M(a_v)$, and since M is a bijection from $\biguplus_{k \in [K/2]} D_k$ to A, this means that $g = f$ and $a_u = a_v$. This in turn means that $I'_f = I'_g$, and we let $I' := I'_f = I'_g$ to simplify notation. In particular, we now have that the partition of coordinates on the right hand side of (52) and (53) is the same. Since $I' \subseteq \Psi(\mathbf{B}^\ell) \cup \mathrm{Ext}'_f \cup \{q_f\} \subseteq \Gamma$ and $x_\Gamma = y_\Gamma$ by assumption, we have $b_u = b_v$. The assumption $x_\Gamma = y_\Gamma$ also implies

$$(c_u)_\Gamma = x_{\Gamma \cap ([n] \setminus (I \cup I'))} = y_{\Gamma \cap ([n] \setminus (I \cup I'))} = (c_v)_\Gamma.$$

Thus, we have $u_\Gamma = v_\Gamma$, as required. ■

3.6 The predecessor map ν and its properties

The predecessor map ν, defined below, is our main tool in defining a vertex cover that lets us bound the size of the matching constructed by a small space algorithm. Intuitively, the predecessor map $\nu_{\ell,j}$ maps a subset of T^ℓ for some $\ell \in [L]$ through j repeated applications of the glueing map τ^ℓ interleaved with applications of the DOWNSET map. This is a natural object, since our construction is motivated by the fact that for appropriately defined 'nice' subsets $U \subseteq T^\ell$, namely for appropriately defined rectangles (see Lemma 10 in Section 2), the edge boundary of the set $U \cup \mathrm{DOWNSET}^\ell(U)$ is very sparse, which is the basis of our hard input instance.

Definition 53 (Predecessor map ν) *We define the map $\nu_{\ell,j}$ mapping* subsets *$U \subseteq T^\ell$ to subsets of $T^{\ell-j}$ by induction on $j \geq 0$ as follows. For $j = 0$ let $\nu_{\ell,0}(U) := U$. For $j > 0$ let*

$$\nu_{\ell,j}(U) := \tau^{\ell-(j-1)}(\textsc{DownSet}^{\ell-(j-1)}(\nu_{\ell,j-1}(U))).$$

We define the closure *map $\nu_{\ell,*}$ by*

$$\nu_{\ell,*}(U) := \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \nu_{\ell,j}(U).$$

We define the map $\mu_{\ell,j}$ mapping subsets *$U \subseteq T^\ell$ to subsets of $S^{\ell-j}$ by letting*

$$\mu_{\ell,j}(U) := \textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(U))$$

for $j = 0, \ldots, \ell$. We let

$$\mu_{\ell,*}(U) := \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \mu_{\ell,j}(U).$$

Remark 54 *We stress that the maps $\nu_{\ell,j}$ as well as $\mu_{\ell,j}$ are defined as mapping* subsets *of T^ℓ to subsets of $T^{\ell-j}$ (resp. $S^{\ell-j}$). This is somewhat more convenient, as otherwise they would not be one to one maps from elements of T^ℓ to elements of $T^{\ell-j}$ (resp. $S^{\ell-j}$), because the* DownSet *function is not one to one as per Definition 27).*

Remark 55 *Note that the closure map $\nu_{\ell,*}$ takes a set U to a union of sets $\nu_{\ell,j}(U)$ for even j. The significance of the parity constraint on j lies, in particular, in the fact that if U is entirely contained in either the P or the Q side of the bipartition defined in* (25) *and* (26)*, the closure of U, namely $\nu_{\ell,*}(U)$, belongs to the same side of the bipartition. At the same time, the set $\mu_{\ell,*}(U)$ belongs to the other side of the bipartition due to the application of the* DownSet *map in Definition 53 above.*

The main results of this section are the following two lemmas.

The first lemmas is central to establishing the required upper bound on the size of the vertex cover (see Lemma 71) that bounds the performance of a small space algorithm in Section 3.7.

Lemma 56 *For every $\ell \in [L]$, every $j = 0, \ldots, \ell$, one has*

$$(\ln 2 - C/K)^j \frac{1}{2}(1 - \ln 2)|T^\ell| \leq |\mu_{\ell,j}(T^\ell \setminus T^\ell_*)| \leq (\ln 2 + C/K)^j \frac{1}{2}(1 - \ln 2)|T^\ell|.$$

The next lemma establishes the key structural property analogous to Lemma 10 in Section 2. The lemma is crucially used to upper bound the size of the matching that a low space algorithm can construct in Lemma 72 in Section 3.7 below.

Lemma 57 *For every $\ell \in [L]$, every $j = 0, \ldots, \ell$ the following conditions hold. For every*

$$x \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*) \subset T^\ell,$$

if $y \in T^\ell$ is such $y_i = x_i$ for all $i \in \Gamma$ (the set of basic coordinates as per Definition 50), then

$$y \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*).$$

Corollary 58 *For every $\ell \in [L]$, every $j = 0, \ldots, \ell$ for every*

$$x \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}) \subset T^\ell,$$

if $y \in S^\ell$ is such that $y_i = x_i$ for all $i \in \Gamma$ (the set of basic coordinates as per Definition 50), then

$$y \in \mu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}).$$

In what follows we start by establishing some basic properties of the predecessor map in Section 3.6.1, then prove Lemma 65 and Lemma 56 in Section 3.6.2 and finally prove the key structural property provided by Lemma 57 in Section 3.6.3.

3.6.1 Basic properties of the predecessor map

Claim 59 *For every $\ell \in [L]$, every $j = 1, \ldots, \ell$ and every $U \subseteq T^\ell$ one has* **(1)** $\nu_{\ell,j}(U) = \nu_{\ell-1,j-1}(\tau^\ell(\text{DOWNSET}^\ell(U))$ *and* **(2)** $\mu_{\ell,j}(U) = \mu_{\ell-1,j-1}(\tau^\ell(\text{DOWNSET}^\ell(U)))$. *Furthermore, for every $\ell \in [L]$, every $j = 0, \ldots, \ell$, $a = 0, \ldots, j$ and every $U \subseteq T^\ell$ one has* **(3)** $\nu_{\ell,j}(U) = \nu_{\ell-a,j-a}(\nu_{\ell,a}(U))$.

Proof: For **(1)** we have by Definition 53

$$\begin{aligned}
\nu_{\ell,j}(U) &= \tau^{\ell-(j-1)}(\text{DOWNSET}^{\ell-(j-1)}(\nu_{\ell,j-1}(U))) \\
&= \tau^{\ell-(j-1)}(\text{DOWNSET}^{\ell-(j-1)}(\tau^{\ell-(j-2)}(\text{DOWNSET}^{\ell-(j-2)}(\nu_{\ell,j-2}(U))))) \\
&= \tau^{\ell-(j-1)}(\text{DOWNSET}^{\ell-(j-1)}(\tau^{\ell-(j-2)}(\text{DOWNSET}^{\ell-(j-2)}(\ldots\tau^\ell(\text{DOWNSET}^\ell(U))\ldots)))) \\
&= \nu_{\ell-1,j-1}(\tau^\ell(\text{DOWNSET}^\ell(U)))
\end{aligned}$$

For **(2)** we have by Definition 53 and using **(1)**

$$\begin{aligned}
\mu_{\ell,j}(U) &= \text{DOWNSET}^{\ell-j}(\nu_{\ell,j}(U)) \\
&= \text{DOWNSET}^{\ell-j}(\nu_{\ell-1,j-1}(\tau^\ell(\text{DOWNSET}^\ell(U)))) \\
&= \mu_{\ell-1,j-1}(\tau^\ell(\text{DOWNSET}^\ell(U))).
\end{aligned}$$

Finally, **(3)** follows since by Definition 53

$$\begin{aligned}
\nu_{\ell,j}(U) &= \tau^{\ell-(j-1)}(\text{DOWNSET}^{\ell-(j-1)}(\nu_{\ell,j-1}(U))) \\
&= \tau^{\ell-(j-1)}(\text{DOWNSET}^{\ell-(j-1)}(\tau^{\ell-(j-2)}(\text{DOWNSET}^{\ell-(j-2)}(\nu_{\ell,j-2}(U))))) \\
&= \tau^{\ell-(j-1)}(\text{DOWNSET}^{\ell-(j-1)}(\tau^{\ell-(j-2)}(\text{DOWNSET}^{\ell-(j-2)}(\ldots\tau^\ell(\text{DOWNSET}^\ell(U))\ldots)))) \\
&= \nu_{\ell-a,j-a}(\nu_{\ell,a}(U)))
\end{aligned}$$

■

The following claim will help simplify our notation:

Claim 60 *For every $\ell \in [L]$, every $j \in 1, \ldots, \ell-1$ and every $U \subseteq T^\ell$ one has $|\mu_{\ell,j}(U)| = |\nu_{\ell,j+1}(U)|$.*

Proof: One has by Definition 53

$$\begin{aligned}
\nu_{\ell,j+1}(U) &= \tau^{\ell-j}(\text{DOWNSET}^{\ell-j}(\nu_{\ell,j}(U))) \\
&= \tau^{\ell-j}(\mu_{\ell,j}(U))),
\end{aligned}$$

and the claim follows since $\tau^{\ell-j}$ is injective by Lemma 49. ■

We note that the increment of the index j on the right hand side in the claim above is crucial, as in general $|\mu_{\ell,j}(U)|$ is very different from $|\nu_{\ell,j}(U)|$ (since DOWNSET is not a one to one map).

We also need

Lemma 61 (Basic properties of the maps $\nu_{\ell,j}$ and $\mu_{\ell,j}$) *The following conditions hold for the maps ν and μ defined above:*

(1) *for every $\ell \in [L]$ and every $0 \le j \le \ell$ the maps $\nu_{\ell,j}$ and $\mu_{\ell,j}$ are injective;*

(2) *every $\ell, \ell' \in [L]$ every $0 \le j \le \ell$, $0 \le j' \le \ell'$ one has*

$$\nu_{\ell,j}(T^\ell \setminus T^\ell_*) \cap \nu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) = \emptyset$$

unless $\ell = \ell'$ and $j = j'$.

(3) *every $\ell, \ell' \in [L]$ every $0 \le j \le \ell$, $0 \le j' \le \ell'$ one has*

$$\mu_{\ell,j}(T^\ell \setminus T^\ell_*) \cap \mu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) = \emptyset$$

unless $\ell = \ell'$ and $j = j'$.

Proof: **(1)** follows since τ is injective by Lemma 49 and DownSet is injective by construction (Definition 27).

We now show **(2)**. First note that $\nu_{\ell,j}(T^\ell \setminus T^\ell_*) \subseteq T^{\ell-j}$ and $\nu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) \subseteq T^{\ell'-j'}$, and hence the two sets are disjoint if $\ell - j \neq \ell' - j'$. Now suppose that $\ell - j = \ell' - j'$ and assume without loss of generality that $\ell \le \ell'$. Furthermore, we can assume that $\ell < \ell'$, since if $\ell = \ell'$, one must have $j = j'$ as otherwise the sets are disjoint by the previous argument. Now note that

$$\nu_{\ell',\ell'-\ell}(T^{\ell'} \setminus T^{\ell'}_*) = \tau^{\ell+1}(\textsc{DownSet}^{\ell+1}(\nu_{\ell',\ell'-\ell-1}(T^{\ell'} \setminus T^{\ell'}_*)) \subseteq T^\ell_*,$$

since the range of $\tau^{\ell+1}$ is T^ℓ_* by Definition 48. This means that

$$\begin{aligned}\nu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) &= \nu_{\ell,j}(\nu_{\ell',\ell'-\ell}(T^{\ell'} \setminus T^{\ell'}_*)) \qquad \text{(by Claim 59, (3), and using } \ell - j = \ell' - j'\text{)}\\ &\subseteq \nu_{\ell,j}(T^\ell_*),\end{aligned}$$

and we get that

$$\nu_{\ell,j}(T^\ell \setminus T^\ell_*) \cap \nu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) \subseteq \nu_{\ell,j}(T^\ell \setminus T^\ell_*) \cap \nu_{\ell,j}(T^\ell_*) = \emptyset$$

since $\nu_{\ell,j}$ is injective by **(1)**.

We now prove **(3)**. First note that by Definition 53

$$\mu_{\ell,j}(T^\ell \setminus T^\ell_*) \subseteq S^{\ell-j}$$

and

$$\mu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) \subseteq S^{\ell'-j'},$$

and hence similarly to above the two sets are disjoint unless $\ell - j = \ell' - j'$. **(3)** now follows by noting that, again using Definition 53, we get, since $\ell - j = \ell' - j'$ and DownSet is injective,

$$\begin{aligned}\mu_{\ell,j}(T^\ell \setminus T^\ell_*) \cap \mu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) &= \textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T^\ell_*)) \cap \textsc{DownSet}^{\ell'-j'}(\nu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*))\\ &= \textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T^\ell_*) \cap \nu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*))\\ &= \emptyset,\end{aligned}$$

where we used **(2)** in the last transition. ■

We will use

Lemma 62 *For every $\ell \in [L]$ one has*

$$T^\ell_* = \nu_{L-1,L-1-\ell}(T^{L-1}_*) \cup \bigcup_{j=1}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*)$$

and

$$T^\ell = \nu_{L-1,L-1-\ell}(T^{L-1}_*) \cup \bigcup_{j=0}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*).$$

Proof: We start by establishing the first result of the lemma, namely

$$T^\ell_* = \nu_{L-1,L-1-\ell}(T^{L-1}_*) \cup \bigcup_{j=1}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*) \tag{54}$$

by induction on $\ell = L-1, \dots, 0$.
Base: $\ell = L-1$**.** One has $T^\ell_* = \nu_{L-1,0}(T^L_*)$, as required, since $\nu_{L-1,0}$ is the identity map by definition (see Definition 53).
Inductive step: $\ell \to \ell - 1$**.** By the inductive hypothesis we have

$$T^\ell_* = \nu_{L-1,L-1-\ell}(T^{L-1}_*) \cup \bigcup_{j=1}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*).$$

Applying $\tau^\ell(\textsc{DownSet}^\ell(\cdot))$ to both sides of the equation above, we get, letting $Q = \nu_{L-1,L-1-\ell}(T^{L-1}_*)$ to simplify notation,

$$\begin{aligned}
\tau^\ell(\textsc{DownSet}^\ell(T^\ell_*)) &= \tau^\ell\left(\textsc{DownSet}^\ell\left(Q \cup \bigcup_{j=1}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*)\right)\right) \\
&= \tau^\ell\left(\textsc{DownSet}^\ell(Q)\right) \cup \bigcup_{j=1}^{L-1-\ell} \tau^\ell\left(\textsc{DownSet}^\ell\left(\nu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*)\right)\right) \\
&= \nu_{L-1,L-\ell}(T^{L-1}_*) \cup \bigcup_{j=1}^{L-1-\ell} \nu_{\ell+j,j+1}(T^{\ell+j} \setminus T^{\ell+j}_*) \qquad (55) \\
&= \nu_{L-1,L-\ell}(T^{L-1}_*) \cup \bigcup_{j=1}^{L-1-\ell} \nu_{(\ell-1)+(j+1),j+1}(T^{(\ell-1)+(j+1)} \setminus T^{(\ell-1)+(j+1)}_*) \\
&= \nu_{L-1,L-1-(\ell-1)}(T^{L-1}_*) \cup \bigcup_{j=2}^{L-\ell} \nu_{(\ell-1)+j,j}(T^{(\ell-1)+j} \setminus T^{(\ell-1)+j}_*)
\end{aligned}$$

We also have

$$\tau^\ell(\textsc{DownSet}^\ell(T^\ell \setminus T^\ell_*)) = \nu_{\ell,1}(T^\ell \setminus T^\ell_*) = \nu_{(\ell-1)+1,1}(T^\ell \setminus T^\ell_*). \tag{56}$$

We now recall that τ^ℓ maps S^ℓ bijectively to $T^{\ell-1}_*$ and $S^\ell = \textsc{DownSet}(T^\ell)$ (this follows by putting together the fact that $S^\ell = \biguplus_{k\in[K/2]} S^\ell_k$ with (30) and Definition 27), which implies

$$\begin{aligned}
T^{\ell-1}_* &= \tau^\ell(S^\ell) \qquad\qquad \text{(since } \tau^\ell \text{ bijectively maps } S^\ell \text{ to } T^{\ell-1}_*\text{)} \\
&= \tau^\ell(\textsc{DownSet}^\ell(T^\ell)) \qquad (57) \\
&= \tau^\ell(\textsc{DownSet}^\ell(T^\ell \setminus T^\ell_*)) \cup \tau^\ell(\textsc{DownSet}^\ell(T^\ell_*))
\end{aligned}$$

Substituting (55) and (56) into (57), we get

$$T_*^{\ell-1} = \nu_{L-1,L-\ell}(T_*^{L-1}) \cup \bigcup_{j\geq 1} \nu_{\ell-1+j,j}(T^{\ell-1+j} \setminus T_*^{\ell-1+j}),$$

as required. This completes the inductive claim and establishes the first result of the lemma.

Now in order to obtain the second result of the lemma we take the union of both sides of (54) with $T^\ell \setminus T_*^\ell$, writing $T^\ell \setminus T_*^\ell = \nu_{\ell+0,0}(T^{\ell+0} \setminus T_*^{\ell+0})$ on the rhs. This results in

$$T^\ell = (T^\ell \setminus T_*^\ell) \cup T_*^\ell = \nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j\geq 0} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}),$$

as required. ■

3.6.2 Proof of Lemma 56

We start with

Definition 63 (Rectangle consistent with a terminal subcube) *For every $\ell \in [L]$, every $I \subseteq [n]$, every fixing f of coordinates in I we say that f is* consistent with T_*^ℓ *if*

$$\{f\} \times [m]^{[n]\setminus I} \subseteq T_*^\ell.$$

We say that a rectangle R in $I \subseteq [n]$ (as per Definition 45) is consistent with T_*^ℓ if

$$R \times [m]^{[n]\setminus I} \subseteq T_*^\ell.$$

We first prove an auxiliary

Claim 64 *For every $\ell \in [L]$, every $I \subseteq [n]$, every rectangle R in I that is consistent with the terminal subcube T_*^ℓ the following conditions hold. If $I' = I \cap \Psi(\mathbf{B}^\ell)$ (see Definition 23) and $R = R_0 \times R_1$, where R_0 is a rectangle in I' and R is a rectangle in $I \setminus I'$, then for every $f_0 \in R_0$ one has that $\{f_0\} \times R_1$ is consistent with the terminal subcube T_*^ℓ.*

Proof: Since R is consistent with T_*^ℓ by assumption, we have $R \times [m]^{[n]\setminus I} = R_0 \times R_1 \times [m]^{[n]\setminus I} \subseteq T_*^\ell$, and hence for every $f_0 \in R_0$ one has $\{f_0\} \times R_1 \times [m]^{[n]\setminus I}$, i.e. $\{f_0\} \times R_1$ is consistent with T_*^ℓ. ■

The lemma below is an important tool that we will use in the actual proof of Lemma 56. The lemma bounds the size of a subset of the terminal subcube under the predecessor map:

Lemma 65 *For every $\ell \in [L]$, every $j = 0, \ldots, \ell$, every fixing f of coordinates in $\Psi(\mathbf{B}^\ell)$ consistent with T_*^ℓ (as per Definition 63), every rectangle R in $\Psi(\mathbf{B}^{>\ell})$ the rectangle*

$$F := \{f\} \times R \times [m]^{[n]\setminus\Psi(\mathbf{B}^{\geq\ell})},$$

satisfies

$$(\ln 2 - C/K)^j |F| \leq |\nu_{\ell,j}(F)| \leq (\ln 2)^j |F|$$

for an absolute constant $C > 0$.

Proof: The proof is by induction on j. The inductive claim is that for every $\ell \in [L]$, every fixing f of coordinates in $\Psi(\mathbf{B}^\ell)$ consistent with T_*^ℓ, every rectangle Y in $\Psi(\mathbf{B}^{>\ell})$ the rectangle

$$F = \{f\} \times Y \times [m]^{[n]\setminus\Psi(\mathbf{B}^{\geq\ell})},$$

satisfies

$$(\ln 2 - C/K)^j |F| \leq |\nu_{\ell,j}(F)| \leq (\ln 2)^j |F|$$

for an absolute constant $C > 0$.

Base: $j = 0$. We have $|\nu_{\ell,j}(F)| = |\nu_{\ell,0}(F)| = |F|$, as required.

Inductive step: $j \to j+1$**.** Fix $\ell \in [L]$ and fix $k \in [K/2]$. We write $T := T^\ell, T_* := T_*^\ell$, as well as $\tau := \tau^\ell$, $\textsc{DownSet} := \textsc{DownSet}^\ell$ to simplify notation. Let $J := J^{\ell-1}$, let $J' := J^\ell$. Let $q_k := q_k^\ell$ denote the k-th compression index in $\mathbf{B}^\ell$, and let $r' = r^\ell$ and $r = r^{\ell-1}$ denote the compression indices for $\mathbf{B}^\ell$ and $\mathbf{B}^{\ell-1}$ respectively. Note that $\ell > 0$, since otherwise we must have $j = 0$.

Let ρ_k be the $(K-k, q_k)$-compressing map as per Definition 40. Since f is consistent with T_*, we have $F \subseteq T_k$. Furthermore, since $q_k \notin \Psi(\mathbf{B}^{\geq \ell})$ (see Definition 21 and Property 22), we have that the rectangle F does not depend on coordinate q_k (as per Definition 38). This means that by Lemma 42 the map ρ_k maps

$$\textsc{DownSet}_k(F) \asymp \left\{x \in F : \mathrm{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W\right\}$$

bijectively to

$$\left\{x \in F : x_{q_k}/m \in \left[0, \frac{1}{K-k}\right)\right\}, \tag{58}$$

which in particular implies

$$|\rho(\textsc{DownSet}_k(F))| = \frac{1}{K-k}|F|. \tag{59}$$

Let f_0 denote the restriction of f to $J'_{<k} \subseteq \Psi(\mathbf{B}^\ell)$ and let f_1 denote the restriction of f to $\Psi(\mathbf{B}^\ell) \setminus J'_{<k} = J'_{\geq k} \cup \{r'\}$. Recall the definitions of the index set I' (see (45))

$$I' = J'_{<k} \cup \mathrm{Ext}_k \cup \{q_k\}$$

and index set I (see (44))

$$I = J \cup \{r\}.$$

We let $H = \mathrm{Ext}_k \cup \{q_k\}$ for convenience, and define for $a \in [m]^H$

$$F(a) := \{(f_0, a)\} \times \{f_1\} \times Y \times [m]^{[n] \setminus (\Psi(\mathbf{B}^{\geq \ell}) \cup H)}. \tag{60}$$

We note that $(f_0, a) \in [m]^{I'}$ – this property makes it convenient to reason about the image of $F(a)$ under τ_k, as we show below. Also note that rectangles $F(a)$ defined above are disjoint for distinct choices of a and

$$\rho_k(\textsc{DownSet}_k(F)) = \bigcup_{a \in Q} F(a), \tag{61}$$

where $Q = [m]^{\mathrm{Ext}_k} \times \left\{0, 1, \ldots, \frac{m}{K-k} - 1\right\}$ by (58). We now apply Lemma 46 to rectangle $F(a)$ for $a \in Q$. We invoke Lemma 46 with $x = (f_0, a) \in [m]^{I'}$, rectangle $R = \{f_1\} \times Y$ and

$$\Lambda = \Psi(\mathbf{B}^{>\ell}) \cup J'_{\geq k} \cup \{r'\}.$$

We note that $[n] \setminus (\Lambda \cup I') = [n] \setminus (\Psi(\mathbf{B}^{\geq \ell}) \cup H)$, which is consistent with (60). Also note that $\Lambda \subset \Psi(\mathbf{B}^{\geq \ell})$. By Lemma 46 we get

$$\Pi_k \left(\{x\} \times R \times [m]^{[n] \setminus (\Lambda \cup I')}\right) = \{M(x)\} \times R \times [m]^{[n] \setminus (\Lambda \cup I)},$$

where $M(x) \in [m]^I$ is consistent with the terminal subcube T_* by definition of M (see (49)). Substituting the setting of x and R, we get $\Pi_k(F(a)) = \widehat{F}(a)$, where

$$\widehat{F}(a) = \{M(x)\} \times \{f_1\} \times Y \times [m]^{[n]\setminus(\Lambda\cup I)}.$$

This together with (61) implies

$$\Pi_k(\rho_k(\textsc{DownSet}_k(F))) = \bigcup_{a\in Q} \widehat{F}(a). \tag{62}$$

We now apply the inductive hypothesis to $\widehat{F}(a)$ with fixing $M(x) \in [m]^{\Psi(\mathbf{B}^{\ell-1})}$ of coordinates and rectangle $R = \{f_1\} \times Y \in [m]^\Lambda$. The preconditions of the lemma are satisfied since $\Lambda \subseteq \Psi(\mathbf{B}^{\geq \ell})$. The inductive hypothesis gives

$$(\ln 2 - C/K)^{j-1}|\widehat{F}(a)| \leq |\nu_{\ell-1,j-1}(\widehat{F}(a))| \leq (\ln 2)^{j-1}|\widehat{F}(a)|. \tag{63}$$

Applying the function $\nu_{\ell-1,j-1}$ to both sides of (62), and using (63), the fact that $\nu_{\ell-1,j-1}$ is injective as well as the fact that $\widehat{F}(a)$ are disjoint for different $a \in [m]^H$ we have

$$\begin{aligned}
|\nu_{\ell-1,j-1}(\Pi_k(\rho_k(\textsc{DownSet}_k(F)))| &= \left|\bigcup_{a\in Q} \nu_{\ell-1,j-1}(\widehat{F}(a))\right| \\
&= \sum_{a\in Q} \left|\nu_{\ell-1,j-1}(\widehat{F}(a))\right| \\
&\geq \sum_{a\in Q} (\ln 2 - C/K)^{j-1} \left|\widehat{F}(a)\right| \\
&= (\ln 2 - C/K)^{j-1} \sum_{a\in Q} \left|\widehat{F}(a)\right| \\
&= (\ln 2 - C/K)^{j-1} \sum_{a\in Q} |F(a)| \\
&= (\ln 2 - C/K)^{j-1} \left|\bigcup_{a\in Q} F(a)\right| \\
&= (\ln 2 - C/K)^{j-1} \left|\rho_k(\textsc{DownSet}_k(F))\right| \\
&= (\ln 2 - C/K)^{j-1} \frac{1}{K-k} \left|F\right|.
\end{aligned} \tag{64}$$

In the fifth transition we used the fact that $|F(a)| = |\widehat{F}(a)|$, which follows by Lemma 46 together with the fact that Π_k is injective. In the seventh transition we used (61). The final transition uses (59).

For the upper bound we similarly have, applying the function $\nu_{\ell-1,j-1}$ to both sides of (62), and using (63), the fact that $\nu_{\ell-1,j-1}$ is injective as well as the fact that $\widehat{F}(a)$ are disjoint for different $a \in [m]^H$ we have

$$\begin{aligned}
|\nu_{\ell-1,j-1}(\Pi_k(\rho_k(\textsc{DownSet}_k(F)))| &= \left|\bigcup_{a\in Q} \nu_{\ell-1,j-1}(\widehat{F}(a))\right| \\
&= \sum_{a\in Q} \left|\nu_{\ell-1,j-1}(\widehat{F}(a))\right| \\
&\leq \sum_{a\in Q} (\ln 2)^{j-1} \left|\widehat{F}(a)\right| \\
&= (\ln 2)^{j-1} \sum_{a\in Q} \left|\widehat{F}(a)\right| \\
&= (\ln 2)^{j-1} \sum_{a\in Q} |F(a)| \\
&= (\ln 2)^{j-1} \left|\bigcup_{a\in Q} F(a)\right| \\
&= (\ln 2)^{j-1} \left|\rho_k(\textsc{DownSet}_k(F))\right| \\
&= (\ln 2)^{j-1} \frac{1}{K-k} |F| .
\end{aligned} \tag{65}$$

In the fifth transition we used the fact that $|F(a)| = |\widehat{F}(a)|$, which follows by Lemma 46 together with the fact that Π_k is injective. In the seventh transition we used (61). The final transition uses (59).

We now get, summing the above over $k \in [K/2]$

$$|\nu_{\ell,j}(F)| = \sum_{k\in[K/2]} |\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_k(F)))| \geq \left(\sum_{k\in[K/2]} \frac{1}{K-k}\right) \cdot (\ln 2 - C/K)^{j-1} |F| \tag{66}$$

and

$$|\nu_{\ell,j}(F)| = \sum_{k\in[K/2]} |\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_k(F)))| \leq \left(\sum_{k\in[K/2]} \frac{1}{K-k}\right) \cdot (\ln 2)^{j-1} |F| \tag{67}$$

At the same time one has by Claim 25

$$\ln 2 - 1/K \leq \sum_{k\in[K/2]} \frac{1}{K-k} \leq \ln 2$$

Putting this together with (66) and (67) completes the proof of the inductive step (we assume that $C \geq 1$), and completes the proof of the lemma. ■

Corollary 66 *For every $\ell \in [L]$, every $j = 0, \ldots, \ell$, every rectangle R in $\Psi(\mathbf{B}^{\geq \ell})$ consistent with the terminal subcube T_*^ℓ (as per Definition 63) the extended rectangle*

$$F = R \times [m]^{[n]\setminus\Psi(\mathbf{B}^{\geq \ell})}$$

satisfies

$$(\ln 2 - C/K)^j |F| \leq |\nu_{\ell,j}(F)| \leq (\ln 2)^j |F|$$

for an absolute constant $C > 0$.

Proof: Write $R = R_0 \times R_1$, where R_0 is a rectangle in $\Psi(\mathbf{B}^\ell)$ and R_1 is a rectangle in $\Psi(\mathbf{B}^{>\ell})$ (this is possible by Definition 45 of a rectangle). We have

$$F = \bigcup_{a \in R_0} F(a), \tag{68}$$

where

$$F(a) = \{a\} \times R_1 \times [m]^{[n] \setminus \Psi(\mathbf{B}^{\geq \ell})}.$$

Note that by Claim 64 every $f \in R_0$ is consistent with the terminal subcube since R is consistent with the terminal subcube by assumption. Thus, the preconditions of Lemma 65 are satisfied, and we have

$$(\ln 2 - C/K)^j |F(a)| \leq |\nu_{\ell,j}(F(a))| \leq (\ln 2)^j |F(a)|. \tag{69}$$

Applying $\nu_{\ell,j}$ to (68), combining with (69) and using the fact that $\nu_{\ell,j}$ is injective by Lemma 61, we get

$$\begin{aligned} |\nu_{\ell,j}(F)| &= \sum_{a \in R_0} |\nu_{\ell,j}(F(a))| \\ &\leq (\ln 2)^j \sum_{a \in R_0} |F(a)| \\ &= (\ln 2)^j |F|. \end{aligned}$$

Similarly, we get

$$\begin{aligned} |\nu_{\ell,j}(F)| &= \sum_{a \in R_0} |\nu_{\ell,j}(F(a))| \\ &\geq (\ln 2 - C/K)^j \sum_{a \in R_0} |F(a)| \\ &= (\ln 2 - C/K)^j |F|. \end{aligned}$$

■

We now give

Proof of Lemma 56: We write $T := T^\ell, T_* := T^\ell_*$, as well as $\tau := \tau^\ell$, $\text{DownSet} := \text{DownSet}^\ell$ to simplify notation. We start by writing

$$\mu_{\ell,j}(T \setminus T_*) = \mu_{\ell,j}(T \setminus T_{K/2}) = \bigcup_{k \in [K/2]} \mu_{\ell,j}(T_k \setminus T_{k+1}).$$

Since $\mu_{\ell,j}$ is injective by Lemma 61, **(1)**, one has $\mu_{\ell,j}(T_k \setminus T_{k+1}) \cap \mu_{\ell,j}(T_{k'} \setminus T_{k'+1}) = \emptyset$ for distinct $k, k' \in [K/2]$ (indeed, as the sets T_k are nested, $T_k \setminus T_{k+1}$ are disjoint for distinct k). Thus,

$$|\mu_{\ell,j}(T \setminus T_*)| = \sum_{k \in [K/2]} |\mu_{\ell,j}(T_k \setminus T_{k+1})|, \tag{70}$$

and in order to bound $|\mu_{\ell,j}(T \setminus T_*)|$ it suffices to bound $|\mu_{\ell,j}(T_k \setminus T_{k+1})|$ for every $k \in [K/2]$. Fix $k \in [K/2]$. We have

$$\begin{aligned} \mu_{\ell,j}(T_k \setminus T_{k+1}) &= \mu_{\ell-1,j-1}(\tau(\text{DownSet}(T_k \setminus T_{k+1}))) \\ &= \bigcup_{s=0}^{k} \mu_{\ell-1,j-1}(\tau(\text{DownSet}_s(T_k \setminus T_{k+1}))), \end{aligned}$$

where the first transition uses Claim 59, **(2)**, and the second transition is by Definition 27 and Remark 30. We bound $|\mu_{\ell,j}(T_k \setminus T_{k+1})|$ by bounding the size of individual terms on the rhs of the equation above. This suffices since $\mu_{\ell-1,j-1}(\tau(\textsc{DownSet}_s(T_k \setminus T_{k+1})))$ are disjoint for different s – this follows by noting that $\textsc{DownSet}_s(T_k \setminus T_{k+1}))$ are disjoint for different s by construction, τ is bijective by Lemma 49 and $\mu_{\ell-1,j-1}$ is injective by Lemma 61, **(1)**. Formally,

$$|\mu_{\ell,j}(T_k \setminus T_{k+1})| = \sum_{s=0}^{k} |\mu_{\ell-1,j-1}(\tau(\textsc{DownSet}_s(T_k \setminus T_{k+1})))|.$$

Furthermore, since for every set $U \subseteq T^{\ell-1}$ one has

$$|\mu_{\ell-1,j-1}(U)| = |\nu_{\ell-1,j}(U)|,$$

by Claim 60, we have

$$|\mu_{\ell,j}(T_k \setminus T_{k+1})| = \sum_{s=0}^{k} |\nu_{\ell,j-1}(\tau(\textsc{DownSet}_s(T_k \setminus T_{k+1})))|. \tag{71}$$

Bounding the rhs of (71)**.** We now bound the terms on the rhs of (71). Let $J = J^\ell$ and $r = r^\ell$ to simplify notation. For $s \in \{0, 1, \dots, k\}$ let $q_s := q_s^\ell$ and let ρ_s be the $(K - s, q_s)$-densifying map as per Definition 40. Define

$$I' := J_{<s} \cup \mathrm{Ext}_s \cup \{q_s\}.$$

Since $T_k \setminus T_{k+1}$ does not depend on q_s (by Property 22; see also Definition 38), we have by Lemma 42

$$\begin{aligned}\rho_s(\textsc{DownSet}_s(T_k \setminus T_{k+1})) \asymp \Bigg\{x \in [m]^n : {} & x_{J_t}/m \in \left[0, 1 - \frac{1}{K-t}\right) \text{ for all } t = 0, \dots, k-1 \\ & \text{and} \\ & x_{J_k}/m \in \left(1 - \frac{1}{K-k}, 1\right] \\ & \text{and} \\ & x_{q_s}/m \in \left[0, \frac{1}{K-s}\right)\Bigg\}.\end{aligned} \tag{72}$$

Define

$$\begin{aligned}Q = \Bigg\{x \in [m]^{I'} : {} & x_{J_t}/m \in \left[0, 1 - \frac{1}{K-t}\right) \text{ for all } t = 0, \dots, s-1 \Bigg\} \\ & \text{and} \\ & x_{q_s}/m \in \left[0, \frac{1}{K-s}\right)\Bigg\}\end{aligned} \tag{73}$$

and, letting $\Lambda := \Psi(\mathbf{B}^{\geq \ell}) \setminus J_{<s}$,

$$\begin{aligned}R = \Bigg\{x \in [m]^{\Lambda} : {} & x_{J_t}/m \in \left[0, 1 - \frac{1}{K-t}\right) \text{ for all } t = s, \dots, k-1 \\ & \text{and} \\ & x_{J_k}/m \in \left(1 - \frac{1}{K-k}, 1\right]\Bigg\}.\end{aligned} \tag{74}$$

so that

$$\rho_s(\textsc{DownSet}_s(T_k \setminus T_{k+1})) = Q \times R \times [m]^{[n]\setminus(\Lambda \cup I')} = \bigcup_{a \in Q} F(a). \tag{75}$$

Further, for $a \in Q \subseteq [m]^{I'}$ let

$$F(a) := \{a\} \times R \times [m]^{[n]\setminus(\Lambda \cup I')}.$$

We note that $F(a) \cap F(a') = \emptyset$ for $a \neq a'$. By Lemma 46 we have

$$\begin{aligned} \Pi_s(F(a)) &= \Pi_s\left(\{a\} \times R \times [m]^{[n]\setminus(\Lambda \cup I')}\right) \\ &= \{M(a)\} \times R \times [m]^{[n]\setminus(\Lambda \cup I)} := \widehat{F}(a). \end{aligned} \tag{76}$$

Since $M(a) \in [m]^I$ (see (44) and (49)) is consistent with the terminal subcube T_*^ℓ, we get by Lemma 65

$$(\ln 2 - C/K)^j |\widehat{F}(a)| \leq |\nu_{\ell-1,j}(\widehat{F}(a))| \leq (\ln 2)^j |\widehat{F}(a)|. \tag{77}$$

We now apply $\nu_{\ell-1,j}(\Pi_s(\cdot))$ to both sides of (75), obtaining

$$\begin{aligned} |\nu_{\ell-1,j}(\Pi_s(\rho_s(\textsc{DownSet}_s(T_k \setminus T_{k+1}))))| &= \sum_{a \in Q} |\nu_{\ell-1,j}(\Pi_s(F(a)))| \\ &= \sum_{a \in Q} |\nu_{\ell-1,j}(\widehat{F}(a))|, \end{aligned} \tag{78}$$

where the last transition uses the definition of $\widehat{F}(a)$ in (76). At the same time we have by (77)

$$\begin{aligned} \sum_{a \in Q} \left|\nu_{\ell-1,j}(\widehat{F}(a))\right| &\geq \sum_{a \in Q} (\ln 2 - C/K)^j \left|\widehat{F}(a)\right| \\ &= (\ln 2 - C/K)^j \sum_{a \in Q} \left|\widehat{F}(a)\right| \\ &= (\ln 2 - C/K)^j \sum_{a \in Q} |F(a)| \\ &= (\ln 2 - C/K)^j \, |\rho_s(\textsc{DownSet}_s(T \setminus T_*))| \\ &= (\ln 2 - C/K)^j \frac{1}{K-s} |T_k \setminus T_{k+1}|. \end{aligned}$$

and

$$\begin{aligned} \sum_{a \in Q} \left|\nu_{\ell-1,j}(\widehat{F}(a))\right| &\leq \sum_{a \in Q} (\ln 2)^j \left|\widehat{F}(a)\right| \\ &= (\ln 2)^j \sum_{a \in Q} \left|\widehat{F}(a)\right| \\ &= (\ln 2)^j \sum_{a \in Q} |F(a)| \\ &= (\ln 2)^j \, |\rho_s(\textsc{DownSet}_s(T_k \setminus T_{k+1}))| \\ &= (\ln 2)^j \frac{1}{K-s} |T_k \setminus T_{k+1}|. \end{aligned}$$

In both cases above the last transition uses the fact that

$$|\rho_s(\textsc{DownSet}_s(T_k \setminus T_{k+1}))| = \frac{1}{K-s}|T_k \setminus T_{k+1}|,$$

which follows by noting that $T_k \setminus T_{k+1}$ does not depend on q_s (by Property 22) and using Lemma 42. Putting the above bounds together with (78) gives

$$(\ln 2 - C/K)^j \frac{1}{K-s}|T_k \setminus T_{k+1}| \leq |\nu_{\ell-1,j}(\tau_s(\textsc{DownSet}_s(T_k \setminus T_{k+1})))| \leq (\ln 2)^j \frac{1}{K-s}|T_k \setminus T_{k+1}|$$

We now get by (71)

$$\begin{aligned} |\mu_{\ell,j}(T_k \setminus T_{k+1})| &= \sum_{s=0}^{k} |\nu_{\ell-1,j}(\tau_s(\textsc{DownSet}_s(T_k \setminus T_{k+1})))| \\ &\geq (\ln 2 - C/K)^j \left(\sum_{s=0}^{k} \frac{1}{K-s}\right)|T_k \setminus T_{k+1}| \end{aligned}$$

and

$$\begin{aligned} |\mu_{\ell,j}(T_k \setminus T_{k+1})| &= \sum_{s=0}^{k} |\nu_{\ell-1,j}(\tau_s(\textsc{DownSet}_s(T_k \setminus T_{k+1})))| \\ &\leq (\ln 2)^j \left(\sum_{s=0}^{k} \frac{1}{K-s}\right)|T_k \setminus T_{k+1}| \end{aligned}$$

Now using (70) and the fact that

$$|T_k \setminus T_{k+1}| = \left(1 - \frac{k}{K}\right) \cdot |T_0^\ell| - \left(1 - \frac{k+1}{K}\right) \cdot |T_0^\ell| = \frac{1}{K}|T_0^\ell|$$

for every $k \in [K/2]$ by Lemma 32, **(1)**, we get

$$(\ln 2 - C/K)^j \gamma |T_0| \leq |\mu_{\ell,j}(T \setminus T_*)| \leq (\ln 2)^j \gamma |T_0| \tag{79}$$

for

$$\gamma = \frac{1}{K}\sum_{k\in[K/2]}\left(\sum_{s=0}^{k}\frac{1}{K-s}\right).$$

Finally, we note that

$$\begin{aligned} \frac{1}{K}\sum_{k\in[K/2]}\left(\sum_{s=0}^{k}\frac{1}{K-s}\right) &= \sum_{s=0}^{K/2-1}\sum_{k=s}^{K/2-1}\frac{1}{K-s} \\ &= \frac{1}{K}\sum_{s=0}^{K/2-1}\frac{K/2-s}{K-s} \\ &= \frac{1}{K}\sum_{s=0}^{K/2-1}\left(1-\frac{K/2}{K-s}\right) \\ &= \frac{1}{2}-\frac{1}{2}\sum_{s=0}^{K/2-1}\frac{1}{K-s}, \end{aligned}$$

and thus by Claim 25

$$\frac{1}{2}(1-\ln 2) \leq \gamma \leq \frac{1}{2}(1-\ln 2 + 1/K).$$

Combining this with (79) gives

$$(\ln 2 - C/K)^j \frac{1}{2}(1-\ln 2)|T_0| \leq |\mu_{\ell,j}(T \setminus T_*)| \leq (\ln 2 + C/K)^j \frac{1}{2}(1-\ln 2)|T_0|$$

as required. ■

3.6.3 Proof of key structural property (Lemma 57)

We now present

Proof of Lemma 57: Our proof is by induction on j. The inductive claim is

> For every $\ell \in [L]$, for every $x \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}) \subseteq T^\ell$, every $y \in T^\ell$, if $y_i = x_i$ for all $i \in \Gamma$ (see Definition 50), then $y \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})$.

Base: $j = 0$. Recall that $\nu_{\ell,0}$ is the identity map. Letting $J := J^\ell$, we have

$$T^\ell \setminus T_*^\ell = \left\{ z \in T^\ell : z_{J_k}/m \in \left[1 - \frac{1}{K-k}, 1\right) \text{ for some } k \in [K/2+1] \right\}.$$

Let $k \in [K/2+1]$ be such that $x_{J_k}/m \in \left[1 - \frac{1}{K-k}, 1\right)$. Since $y_i = x_i$ for all $i \in \Gamma$, and in particular for $i \in \Psi(\mathbf{B}^\ell)$ (which includes $J_0, \ldots, J_{K/2}$ and in particular J_k), we get $y_{J_k}/m \in \left[1 - \frac{1}{K-k}, 1\right)$ and therefore $y \in T^\ell \setminus T_*^\ell = \nu_{\ell,0}(T^\ell \setminus T_*^\ell)$ as required.

Inductive step: $j-1 \to j$**.** By Lemma 52 there exists $a \in [K/2]$ as well as $u, v \in S_a^{\ell+1}$ such that $x = \tau^{\ell+1}(u)$, $y = \tau^{\ell+1}(v)$ and $u_\Gamma = v_\Gamma$ (the set of basic coordinates as per Definition 50). Let $x' \in T^{\ell+1}, y' \in T^{\ell+1}$ be such that $x' \asymp u$ and $y' \asymp v$, and note that $x'_\Gamma = y'_\Gamma$. Now recall that by Definition 53

$$\nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}) = \tau^{\ell+1}(\textsc{DownSet}^{\ell+1}(\nu_{(\ell+1)+(j-1),j-1}(T^{(\ell+1)+(j-1)} \setminus T_*^{(\ell+1)+(j-1)}))).$$

Since $x \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})$ by assumption, we get that

$$x' \in \nu_{(\ell+1)+(j-1),j-1}(T^{(\ell+1)+(j-1)} \setminus T_*^{(\ell+1)+(j-1)}),$$

and therefore by the inductive hypothesis, using the fact that $x'_\Gamma = y'_\Gamma$, we get

$$y' \in \nu_{(\ell+1)+(j-1),j-1}(T^{(\ell+1)+(j-1)} \setminus T_*^{(\ell+1)+(j-1)}).$$

As a consequence $y \in \tau^{\ell+1}(\textsc{DownSet}^{\ell+1}(\{y'\})) \subseteq \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})$, as required. ■

We also give

Proof of Corollary 58: Let $y' \in T^\ell$ be such that $y \asymp y'$ – such a y' exists by definition of S^ℓ, and note that $y'_\Gamma = x_\Gamma$ since $y_\Gamma = x_\Gamma$ by assumption of the corollary. We have

$$y' \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})$$

by Lemma 57. Since $\mu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}) = \textsc{DownSet}^\ell(\nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}))$, we get $y \in \mu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})$, as required. ■

3.7 Proof of Theorem 5

We now define the hard input distribution $\mathcal{D}$ on graphs $\widehat{G} = (P, Q, \widehat{E})$. A graph $\widehat{G} \sim \mathcal{D}$ is sampled as follows. First, for every round $\ell \in [L]$ and phase $k \in [K/2]$ one **arbitrarily** selects

1. the extension indices Ext_k^ℓ from $\mathbf{B}_k^\ell$;
2. a compression index q_k^ℓ in $\mathbf{B}_k^\ell \setminus \text{Ext}_k^\ell$.

One also selects $r^\ell \in \mathbf{B}_{K/2}^\ell$ arbitrarily. Recall that for $k \in [K/2]$ we let (see Definition 21)

$$\mathring{\mathbf{B}}_k^\ell = \mathbf{B}_k^\ell \setminus (\text{Ext}_k^\ell \cup \{q_k^\ell\})$$

and $\mathring{\mathbf{B}}_{K/2}^\ell = \mathbf{B}_{K/2}^\ell \setminus \{r^\ell\}$. Finally, one selects, for every $\ell \in [L]$ and $k \in [K/2]$,

$$J_k^\ell \sim UNIF(\mathring{\mathbf{B}}_k^\ell)$$

independently.

Edge set of $\widehat{G} = (P, Q, \widehat{E})$. We first define

$$\tau_*(x) = \begin{cases} \tau^\ell(x) & \text{if } x \in S^\ell \text{ for } \ell > 0 \\ x & \text{o.w.} \end{cases} \tag{80}$$

and define for every edge $e = (u, v) \in E^\ell, u \in S^\ell, v \in T^\ell, \ell \in [L]$

$$\tau_*(e) = (\tau_*(u), v). \tag{81}$$

We now let

$$\widehat{E} = \bigcup_{\ell \in [L]} \widehat{E}^\ell, \tag{82}$$

where

$$\widehat{E}^\ell = \bigcup_{k \in [K/2]} \bigcup_{j \in \mathring{\mathbf{B}}_k^\ell} \tau_*(E_{k,j}^\ell), \tag{83}$$

and $E_{k,j}^\ell$ is defined by (34).

Ordering of edges of $\widehat{G}$ in the stream. The graph $G^\ell = (S^\ell, T^\ell, E^\ell)$ is presented in the stream over L *rounds* and $K/2$ *phases* as follows. For every $\ell \in \{1, \ldots, L-1\}$, for every $k \in [K/2]$, the edges in $\tau^\ell(E_k^\ell)$ are presented in the stream; the ordering within $\tau^\ell(E_k^\ell)$ is arbitrary.

We have

Lemma 67 *The graph $\widehat{G} = (P, Q, \widehat{E})$ contains a matching of size $(1 - O(1/L))|P|$.*

Proof: By Lemma 37 for every $\ell \in [L], \ell > 0$ there exists a matching M^ℓ in E^ℓ that matches a $(1 - O(1/K))$ fraction of S^ℓ to $T^\ell \setminus T_*^\ell$. Since τ^ℓ is injective by Lemma 49, we have that $\tau^\ell(M^\ell)$ is also a matching. Furthermore, since τ^ℓ maps S^ℓ to $T_*^{\ell-1}$, avoiding vertices in $T^{\ell-1} \setminus T_*^{\ell-1}$, which may be matched by $\tau^{\ell-1}(M^{\ell-1})$, we have that the union of edges

$$\bigcup_{\ell \in [L], \ell > 0} \tau^\ell(M^\ell)$$

forms a matching. For every ℓ we have $|M^\ell| = (1 - O(1/K))|S^\ell|$, and by Lemma 32, **(2)**, one has $|S^\ell| = \sum_{k\in[K/2]} |S^\ell_k| = \frac{1}{2}|T^\ell| = \frac{1}{2}N$. Since by Lemma 32, **(1)**, with $k = K/2$ one has $|T^\ell_k| = \frac{1}{2}|T^\ell|$, we have by (25)

$$\begin{aligned}|P| &= \left|\left(\bigcup_{\text{even } \ell\in[L]} T^\ell\right)\right|\\ &= \sum_{\text{even } \ell\in[L]} |T^\ell|\\ &= (L/2)\cdot N\\ &= L\cdot N/2.\end{aligned}$$

This means that $\bigcup_{\ell\in[L],\ell>0} \tau^\ell(M^\ell)$ is a matching of size $(L-1)\cdot(1-O(1/K))\cdot N/2 = (1-O(1/L))|P|$, since $L \leq K$ by (p2). ■

Upper bounding size of matching constructed by a low space algorithm. The following sets of vertices are hard to match well, as we show below:

$$\begin{aligned}A_P &= \bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}} \nu_{\ell,*}(T^\ell \setminus T^\ell_*)\\ A_Q &= \bigcup_{\substack{\ell\in[L]\\ \ell \text{ odd}}} \nu_{\ell,*}(T^\ell \setminus T^\ell_*).\end{aligned} \tag{84}$$

To show that A_P and A_Q are hard to match well, we show that the subset of edges of G retained by a small space generalized online algorithm typically admits a small vertex cover that avoids A_P and A_Q. The two sets below (and some other vertices that contribute lower order terms to the size of the vertex cover) will be included:

$$\begin{aligned}B_Q &= \bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}} \tau_*(\mu_{\ell,*}(T^\ell \setminus T^\ell_*))\\ B_P &= \bigcup_{\substack{\ell\in[L]\\ \ell \text{ odd}}} \tau_*(\mu_{\ell,*}(T^\ell \setminus T^\ell_*)).\end{aligned} \tag{85}$$

We have

Claim 68 *$A_P \cap B_P = \emptyset$ and $A_Q \cap B_Q = \emptyset$.*

Proof: We prove the first claim (the proof of the second is analogous). One has by (84)

$$\begin{aligned}A_P &= \bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}} \nu_{\ell,*}(T^\ell \setminus T^\ell_*)\\ &= \bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}} \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \nu_{\ell,j}(T^\ell \setminus T^\ell_*)\end{aligned} \tag{86}$$

and by (85)

$$\begin{aligned}
B_P &= \bigcup_{\substack{\ell\in[L]\\ \ell\text{ odd}}} \tau_*(\mu_{\ell,*}(T^\ell\setminus T^\ell_*))\\
&= \bigcup_{\substack{\ell\in[L]\\ \ell\text{ odd}}} \bigcup_{\substack{j=0\\ j\text{ even}}}^{\ell} \tau_*(\mu_{\ell,j}(T^\ell\setminus T^\ell_*))\\
&= \bigcup_{\substack{\ell\in[L]\\ \ell\text{ odd}}} \bigcup_{\substack{j=0\\ j\text{ even}}}^{\ell} \tau^{\ell-j}(\mu_{\ell,j}(T^\ell\setminus T^\ell_*))\\
&= \bigcup_{\substack{\ell\in[L]\\ \ell\text{ odd}}} \bigcup_{\substack{j=0\\ j\text{ even}}}^{\ell} \nu_{\ell,j+1}(T^\ell\setminus T^\ell_*),
\end{aligned} \tag{87}$$

where we used the definition of τ_* (see (80)) in the third transition and Definition 53 in the forth transition. Disjointness now follows by Lemma 61, **(2)**, since the range of (ℓ, j) pairs in (86) is disjoint from the range of $(\ell, j+1)$ pairs in (87). ■

Before exhibiting the vertex cover, we show that $A_P \cup B_P$ is almost all of P, and $A_Q \cup B_Q$ is almost all of Q:

Lemma 69 (Almost partition of P and Q) *One has $|P\setminus(A_P\cup B_P)| = O(N)$ and $|Q\setminus(A_Q\cup B_Q)| = O(N)$ for sets A_P, A_Q, B_P, B_Q defined in* (84) *and* (85).

Proof: Recall that by (25) and (26) $P\cup Q = S^0\cup\bigcup_{\ell\geq 0} T^\ell$. We have by Lemma 62

$$T^\ell_* = \nu_{L-1,L-1-\ell}(T^{L-1}_*) \cup \bigcup_{j=1}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j}\setminus T^{\ell+j}_*).$$

Putting these two equalities together, and letting $D = \bigcup_{j=0}^{L-1}\nu_{L-1,L-1-\ell}(T^{L-1}_*)$ to simplify notation, we get

$$\begin{aligned}
P\cup Q &= S^0 \cup \bigcup_{\ell\geq 0} T^\ell\\
&= S^0\cup D\cup\left(\bigcup_{\ell\geq 0}\bigcup_{j\geq 0}\nu_{\ell+j,j}(T^{\ell+j}\setminus T^{\ell+j}_*)\right)\\
&= S^0\cup D\cup \bigcup_{\ell=0}^{L-1}\bigcup_{j=0}^{\ell}\nu_{\ell,j}(T^\ell\setminus T^\ell_*)\\
&= S^0\cup D\cup\left(\bigcup_{\substack{\ell\geq 0\\ \ell\text{ even}}}\bigcup_{j=0}^{\ell}\nu_{\ell,j}(T^\ell\setminus T^\ell_*)\right)\cup\left(\bigcup_{\substack{\ell\geq 0\\ \ell\text{ odd}}}\bigcup_{j=0}^{\ell}\nu_{\ell,j}(T^\ell\setminus T^\ell_*)\right)
\end{aligned} \tag{88}$$

Note that it follows from Corollary 66 that $|D| = O(N)$. Indeed,

$$\begin{aligned}
|D| &= \left|\bigcup_{j=0}^{L-1} \nu_{L-1,L-1-\ell}(T_*^{L-1})\right| \\
&\leq \sum_{j\geq 0} |\nu_{\ell,j}(T_*^{L-1})| \\
&\leq \sum_{j\geq 0} (\ln 2)^j |T_*^{L-1}| \\
&= \frac{1}{1-\ln 2}|T_*^{L-1}| \\
&= \frac{1}{2(1-\ln 2)}N \\
&= O(N).
\end{aligned}$$

Thus, since $|S^0| = \sum_{k\in[K/2]} |S_k^0| = N/2$ by Lemma 32, **(2)**, it suffices to show that the union of the third and forth terms above equals $A_P \cup A_Q \cup B_P \cup B_Q$. To that effect we note that for every $\ell = 0, \dots, L-1$ and $j = 0, \dots, \ell$

$$\nu_{\ell,j+1}(T^\ell \setminus T_*^\ell) = \tau^{\ell-j}(\textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T_*^\ell))).$$

This means that the third term on the last line of (88) can be rewritten as

$$\begin{aligned}
&\bigcup_{\substack{\ell\geq 0\\ \ell \text{ even}}} \bigcup_{j=0}^{\ell} \nu_{\ell,j}(T^\ell \setminus T_*^\ell) \\
&= \bigcup_{\substack{\ell\geq 0\\ \ell \text{ even}}} \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \Big(\nu_{\ell,j}(T^\ell \setminus T_*^\ell) \cup \tau^{\ell-j}(\textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T_*^\ell)))\Big) \\
&= \bigcup_{\substack{\ell\geq 0\\ \ell \text{ even}}} \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \Big(\nu_{\ell,j}(T^\ell \setminus T_*^\ell) \cup \tau_*(\textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T_*^\ell)))\Big) \\
&= \left(\bigcup_{\substack{\ell\geq 0\\ \ell \text{ even}}} \nu_{\ell,*}(T^\ell \setminus T_*^\ell)\right) \cup \left(\bigcup_{\substack{\ell\geq 0\\ \ell \text{ even}}} \tau_*(\mu_{\ell,*}(T^\ell \setminus T_*^\ell))\right) \\
&= A_P \cup B_Q,
\end{aligned}$$

where τ_* is as defined in (80), and we let $\tau^0(U) = \emptyset$ for every U for convenience to simplify notation.

Similarly, we get for the forth term on the last line of (88)

$$
\begin{aligned}
&\bigcup_{\substack{\ell\geq 0\\ \ell \text{ odd}}}\bigcup_{j=0}^{\ell}\nu_{\ell,j}(T^\ell\setminus T_*^\ell)\\
&=\left(\bigcup_{\substack{\ell\geq 0\\ \ell \text{ odd}}}\bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell}\nu_{\ell,j}(T^\ell\setminus T_*^\ell)\right)\cup\left(\bigcup_{\substack{\ell\geq 0\\ \ell \text{ odd}}}\bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell}\tau^{\ell-j}(\textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell\setminus T_*^\ell)))\right)\\
&=\left(\bigcup_{\substack{\ell\geq 0\\ \ell \text{ odd}}}\nu_{\ell,*}(T^\ell\setminus T_*^\ell)\right)\cup\left(\bigcup_{\substack{\ell\geq 0\\ \ell \text{ odd}}}\tau_*(\mu_{\ell,*}(T^\ell\setminus T_*^\ell))\right)\\
&=\left(\bigcup_{\substack{\ell\geq 0\\ \ell \text{ odd}}}\nu_{\ell,*}(T^\ell\setminus T_*^\ell)\right)\cup\left(\bigcup_{\substack{\ell\geq 0\\ \ell \text{ odd}}}\tau_*(\mu_{\ell,*}(T^\ell\setminus T_*^\ell))\right)\\
&=A_Q\cup B_P,
\end{aligned}
$$

as required. ■

The next lemma upper bounds the cardinality of B_P and B_Q, which later leads to our upper bound on the size of the constructed vertex cover.

Lemma 70 *One has*

$$|B_P|\leq(1+O(1/L))\cdot\frac{L}{2}\cdot\frac{N}{2}\cdot\frac{1}{1+\ln 2}$$

and

$$|B_Q|\leq(1+O(1/L))\cdot\frac{L}{2}\cdot\frac{N}{2}\cdot\frac{1}{1+\ln 2}.$$

Proof: We prove the bound for B_Q (the bound for B_P is analogous). Using (85) we get

$$
\begin{aligned}
|B_Q|&=\left|\bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}}\tau_*(\mu_{\ell,*}(T^\ell\setminus T_*^\ell))\right|\\
&\leq\left|\bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}}\mu_{\ell,*}(T^\ell\setminus T_*^\ell)\right|\\
&\leq\sum_{\substack{\ell\in[L]\\ \ell \text{ even}}}|\mu_{\ell,*}(T^\ell\setminus T_*^\ell)|,
\end{aligned}
$$

so it suffices to upper bound the summands above. For every $\ell\in[L]$ by Definition 53

$$\left|\mu_{\ell,*}(T^\ell\setminus T_*^\ell)\right|=\left|\bigcup_{\substack{0\leq j\leq\ell\\ j\ even}}\mu_{\ell,j}(T^\ell\setminus T_*^\ell)\right|\leq\bigcup_{\substack{0\leq j\leq\ell\\ j\ even}}\left|\mu_{\ell,j}(T^\ell\setminus T_*^\ell)\right| \tag{89}$$

and by Lemma 56 we have for an absolute constant $C > 0$

$$|\mu_{\ell,j}(T^\ell \setminus T^\ell_*)| \leq \frac{1}{2}(\ln 2 + C/K)^j(1 - \ln 2)|T^\ell|.$$

Summing over all even j as per (89), we get

$$\begin{aligned}\left|\mu_{\ell,*}(T^\ell \setminus T^\ell_*)\right| &\leq \sum_{\substack{0\leq j\leq \ell\\ j\ even}} \frac{1}{2}(\ln 2 + C/K)^j(1 - \ln 2)|T^\ell|\\ &\leq \frac{1}{2}(1-\ln 2)|T^\ell|\sum_{j\geq 0}(\ln 2 + C/K)^{2j}\\ &= \frac{1}{2}(1-\ln 2)|T^\ell|\frac{1}{1-(\ln 2 + C/K)^2}\\ &\leq (1+O(1/K))\frac{1}{2}(1-\ln 2)|T^\ell|\frac{1}{1-(\ln 2)^2}\\ &= (1+O(1/K))\frac{1}{2}\frac{1}{1+\ln 2}|T^\ell|.\end{aligned}$$

Summing the above over all even $\ell \in [L]$ and recalling that $|T^\ell| = N$ and using the fact that $L \leq K$ by (p2) gives the required bound. ■

Lemma 71 *For every matching M in G one has*

$$|M| \leq |M \cap (A_P \times (Q \setminus B_Q))| + \frac{1}{1+\ln 2}|P| + O(|P|/L).$$

Proof: We exhibit a vertex cover of appropriate size for M. Specifically, we add to the vertex cover one endpoint of every edge in

$$M \cap (A_P \times (Q \setminus B_Q)),$$

as well as all vertices in $P \setminus A_P \approx B_P$ and B_Q. Note that this is indeed a vertex cover: $A_P \cap B_P = \emptyset$ and $A_Q \cap B_Q = \emptyset$ by Claim 68, so every edge of M either has an endpoint in $P \setminus A_P$, or belongs to $A_P \times (Q \setminus B_Q)$, or belongs to $A_P \times B_Q$, in which case it has an endpoint in B_Q.

The size of the vertex cover is

$$\begin{aligned}&|M \cap (A_P \times (Q \setminus B_Q))| + |P \setminus A_P| + |B_Q|\\ \leq&|M \cap (A_P \times (Q \setminus B_Q))| + |B_P| + |B_Q| + O(N),\end{aligned} \tag{90}$$

where we used Lemma 69 to conclude that

$$|P \setminus A_P| \leq |B_P| + |P \setminus (A_P \cup B_P)| = |B_P| + O(N).$$

By Lemma 70 we have

$$|B_P| \leq \frac{L}{2}\cdot\frac{N}{2}\frac{1}{1+\ln 2}(1+O(1/L))$$

and

$$|B_Q| \leq \frac{L}{2}\cdot\frac{N}{2}\frac{1}{1+\ln 2}(1+O(1/L)).$$

Putting the above together with (90) and recalling that by (25)

$$|P| = \left| \bigcup_{\text{even } \ell \in [L]} T^\ell \right| = L \cdot N/2$$

gives the result. ■

We now prove

Lemma 72 *For every matching $M \subseteq \widehat{E}$ one has*

$$M \cap (A_P \times (Q \setminus B_Q)) \subseteq \bigcup_{\ell \in [L], k \in [K/2]} \tau^\ell(E^\ell_{k, J^\ell_k}).$$

Proof of Lemma 72: Consider an edge $(u, v) \in \widehat{E}$ such that $u \in A_P, v \in Q \setminus B_Q$. Let $\ell \in [L]$ be an even integer such that $u \in T^\ell$. Such an ℓ exists because by (84) one has

$$A_P = \bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \nu_{\ell,*}(T^\ell \setminus T^\ell_*)$$

and by Definition 53 one has

$$\nu_{\ell,*}(T^\ell \setminus T^\ell_*) := \bigcup_{\substack{i=0 \\ i \text{ even}}}^{\ell} \nu_{\ell,i}(T^\ell \setminus T^\ell_*),$$

so that

$$\nu_{\ell,*}(T^\ell \setminus T^\ell_*) \subseteq \bigcup_{\text{even } \ell \in [L]} T^\ell_*.$$

To summarize, we have

$$u \in \nu_{\ell+i,i}(T^{\ell+i} \setminus T^{\ell+i}_*) \tag{91}$$

for a unique choice of even $\ell \in [L]$ and even i (uniqueness follows by Lemma 61, **(2)**). We now consider two cases: depending on whether $v \in T^{\ell-1}$ (**case 1**) or $v \in T^{\ell+1}$ (**case 2**).

Case 1. In this case there exists a unique $y \in S^\ell$ such that $\tau^\ell(y) = v$. Indeed, otherwise the edge (u, v) would not be in the graph $\widehat{G}$ as per (82). Let $x = u$ for convenience. We now show using Corollary 58 that

$$y \in \mu_{\ell+i,i}(T^{\ell+i} \setminus T^{\ell+i}_*),$$

which implies, by (85) together with the definition of $\mu_{\ell,*}$ (Definition 53), that $v = \tau^\ell(y) \in B_Q$. We first verify that preconditions of Corollary 58 are satisfied. Let $k \in [K/2]$ be the unique index such that both $x \in T^\ell_k$ and $y \in S^\ell_k$ (uniqueness follows since $(x, y) \in E^\ell_k$ due to $(u, v) \in \widehat{E}$, and the edge sets in (34) are disjoint by Lemma 36). We have $(u, v) \in \widehat{E}$ by assumption, which means that $(x, y) \in E^\ell_k$, and therefore $y_i = x_i$ for all $i \in [n], i \neq j$ for some $j \in \mathring{\mathbf{B}}^\ell_k$ by (32) and (34). We assume towards a contradiction that $j \neq J^\ell_k$. Since

$$\mathring{\mathbf{B}}^\ell_k \cap \Gamma = \{J^\ell_k\},$$

we thus get that $x_\Gamma = y_\Gamma$, and preconditions of Corollary 58 are indeed satisfied. We thus get that $x \in \nu_{\ell+i,i}(T^{\ell+i} \setminus T^{\ell+i}_*)$, implies $y \in \mu_{\ell+i,i}(T^{\ell+i} \setminus T^{\ell+i}_*)$. At the same time by Definition 53 for every $\ell \in [L]$

$$\mu_{\ell,*}(T^\ell \setminus T^\ell_*) := \bigcup_{\substack{i=0 \\ i \text{ even}}}^{\ell} \mu_{\ell,i}(T^\ell \setminus T^\ell_*),$$

which means that $y \in \mu_{\ell,*}(T^\ell \setminus T^\ell_*)$ (recall that i is even) and thus $v = \tau^\ell(y) \in \tau_*(\mu_{\ell,*}(T^\ell \setminus T^\ell_*)) \subseteq B_Q$, as required.

Case 2. In this case there exists a unique $x' \in S^{\ell+1}$ such that $\tau^{\ell+1}(x') = u$. Indeed, otherwise the edge (u, v) would not be in the graph $\widehat{G}$ as per (82); uniqueness follows by injectivity of τ^ℓ (by Lemma 49). Let $y = v$. Let $k \in [K/2]$ be the unique index such that both $x' \in S_k^{\ell+1}$ and $y \in T_k^{\ell+1}$ (uniqueness follows since $(x', y) \in E_k^{\ell+1}$ due to $(u, v) \in \widehat{E}$, and the edge sets in (34) are disjoint by Lemma 36). Let $x \in T^{\ell+1}$ be such that $x \asymp x'$ – such a vertex exists by definition of $S^{\ell+1}$ – see (29).

We have $(u, v) \in \widehat{E}$ by assumption, which means that $(x, y) \in E^{\ell+1}$, and therefore $y_i = x_i$ for all $i \in [n], i \neq j$ for some $j \in \mathring{\mathbf{B}}_k^{\ell+1}$ by (32) and (34). We assume towards a contradiction that $j \neq J_k^{\ell+1}$. Since

$$\mathring{\mathbf{B}}_k^{\ell+1} \cap \Gamma = \{J_k^{\ell+1}\},$$

we thus get that $x_\Gamma = y_\Gamma$, and we can apply Lemma 57 to x and y. By (91) we have

$$\begin{aligned} u &= \tau^{\ell+1}(x') \\ &\in \nu_{\ell+i,i}(T^{\ell+i} \setminus T_*^{\ell+i}) \\ &\subseteq \tau^{\ell+1}\left(\mu_{\ell+i,i-1}(T^{\ell+i} \setminus T_*^{\ell+i})\right), \end{aligned}$$

and therefore

$$x' \in \mu_{\ell+i,i-1}(T^{\ell+i} \setminus T_*^{\ell+i}).$$

Since

$$\mu_{\ell+i,i-1}(T^{\ell+i} \setminus T_*^{\ell+i}) = \textsc{DownSet}^{\ell+1}(\nu_{\ell+i,i-1}(T^{\ell+i} \setminus T_*^{\ell+i})),$$

we have

$$\begin{aligned} x &\in \nu_{\ell+i,i-1}(T^{\ell+i} \setminus T_*^{\ell+i}) \\ &= \nu_{(\ell+1)+(i-1),i-1}(T^{(\ell+1)+(i-1)} \setminus T_*^{(\ell+1)+(i-1)}) \end{aligned}$$

By Lemma 57[3] we thus have [4]

$$\begin{aligned} y &\in \nu_{(\ell+1)+(i-1),i-1}(T^{(\ell+1)+(i-1)} \setminus T_*^{(\ell+1)+(i-1)}) \\ &= \tau^{\ell+2}(\mu_{\ell+i,i-2}(T^{\ell+i} \setminus T_*^{\ell+i})). \end{aligned}$$

At the same time by Definition 53 for every $\ell \in [L]$

$$\mu_{\ell,*}(T^\ell \setminus T_*^\ell) := \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \mu_{\ell,j}(T^\ell \setminus T_*^\ell),$$

which means that $y = v \in B_Q$, as required. ■

Definition 73 (Ordering on (ℓ, k) pairs) *We write $(\ell', k') < (\ell, k)$ iff $\ell' < \ell$ or $\ell' = \ell$ but $k' < k$. We write $(\ell', k') \leq (\ell, k)$ iff $\ell' < \ell$ or $\ell' = \ell$ but $k' < k$.*

Definition 74 *For $\ell \in [L]$ and $k \in [K/2]$ we write*

$$\widehat{G}_{(\ell,k)} = (P, Q, \widehat{E}_k^\ell),$$

[3] Note that we are applying the lemma with $\ell + 1$ as opposed to ℓ here, since $x, y \in T^{\ell+1}$.

[4] When $\ell + 1 = L - 1$, we have $\ell + 2 = L$, which does not technically correspond to a gadget in our input graph. However, we think of artifically adding such a gadget here to handle this corner case for simplicity.

and write

$$\widehat{G}_{\leq(\ell,k)} = \left(P, Q, \bigcup_{\substack{\ell'\in[L],k'\in[K/2]\\(\ell',k')\leq(\ell,k)}} \widehat{E}^{\ell'}_{k'}\right).$$

Definition 75 *For every $\ell \in [L], k \in [K/2+1]$ define $\Lambda_{\ell,k} := (J^\ell_k)$. We write $\Lambda_{<(\ell,k)} = \left(\Lambda_{\ell',k'}\right)_{(\ell',k')<(\ell,k)}$.*

Note that $\widehat{G}_{\leq(\ell,k)}$ is fully determined by $\Lambda_{<(\ell,k)}$. Here it is important to note that the restriction of the map τ^ℓ onto $S^\ell_{\leq k}$ is indeed determined by $\Lambda_{<(\ell,k)}$ – see Remark 43.

We prove

Theorem 76 *For any sufficiently large constant K, any generalized online algorithm ALG with space budget $s = o(|P|\log|P|)$ cannot output a matching M_{ALG} satisfying*

$$|M_{ALG}| \geq \left(\frac{1}{1+\ln 2} + O(1/K)\right)|M_{OPT}|$$

with probability more than $1/10$.

Proof: Since we are evaluating the performance of the algorithm with respect to a distribution, by Yao's minimax principle we may assume that ALG is deterministic.

We have by Lemma 71 that the size of the maximum matching M_{ALG} in G is upper bounded by

$$|M_{ALG} \cap A_P \times (Q \times B_Q)| + \left(\frac{1}{1+\ln 2} + O(1/K)\right)|P|, \tag{92}$$

where we used the fact that $L = K$ as per (p2).

Recall that in every round $\ell \in [L]$ and every phase $k \in [K/2]$ of round ℓ the algorithm is presented with edges in

$$\widehat{E}^\ell_k = \bigcup_{j\in\mathring{\mathbf{B}}^\ell_k} \widehat{E}^\ell_{k,j},$$

as per (82) and (83). Let $\text{ALG}^\ell_k \subseteq \widehat{E}^\ell_k$ denote the subset of $\widehat{E}^\ell_k$ remembered by ALG (recall the definition of the generalized online model – see Definition 3). Note that since we are assuming that ALG is deterministic, the set ALG^ℓ_k is fully determined by $\Lambda_{<(\ell,k)}$ (which determines $\widehat{G}_{\leq(\ell,k)}$). At the same time, recall that conditioned on $\Lambda_{<(\ell,k)}$, the index J^ℓ_k is uniformly random in $\mathring{\mathbf{B}}^\ell_k$:

$$J^\ell_k \sim UNIF(\mathring{\mathbf{B}}^\ell_k).$$

Thus, one has, for any $\Lambda_{<(\ell,k)}$,

$$\begin{aligned}
\mathbf{E}_{\widehat{G}\sim\mathcal{D}}\left[|\text{ALG}^\ell_k \cap \widehat{E}^\ell_{k,J^\ell_k}||\Lambda_{<(\ell,k)}\right] &= \sum_{j\in\mathring{\mathbf{B}}^\ell_k} |\text{ALG}^\ell_k \cap \widehat{E}^\ell_{k,j}| \cdot \mathbf{Pr}[J^\ell_k = j|\Lambda_{<(\ell,k)}] \\
&= \frac{1}{|\mathring{\mathbf{B}}^\ell_k|}\sum_{j\in\mathring{\mathbf{B}}^\ell_k} |\text{ALG}^\ell_k \cap \widehat{E}^\ell_{k,j}| \\
&= \frac{1}{|\mathring{\mathbf{B}}^\ell_k|}|\text{ALG}^\ell_k| \\
&\leq \frac{1}{n/(2KL)}|\text{ALG}^\ell_k| \\
&\leq \frac{1}{n/(2KL)}s
\end{aligned} \tag{93}$$

In the third transition we used the fact that $E^{\ell}_{k,j}$ are disjoint for different $j \in \mathring{\mathbf{B}}^{\ell}_{k}$ by Lemma 36, and therefore $\widehat{E}^{\ell}_{k,j}$ are also disjoint for different j since τ_* is injective (in turn, because individual maps τ^{ℓ} are injective by Lemma 49 and have disjoint ranges). In the forth transition we used the fact that

$$|\mathring{\mathbf{B}}^{\ell}_{k}| \geq |\mathbf{B}^{\ell}_{k}| - |\mathrm{Ext}^{\ell}_{k} \cup \{q^{\ell}_{k}\}| \geq n/(KL) - K \geq n/(2KL)$$

since n is sufficiently large as a function of K and L. In the forth transition we used the assumption that the total number of edges remembered by ALG is bounded by s. Now by Lemma 72 one has

$$M_{ALG} \cap (A_P \times (Q \setminus B_Q)) \subseteq \bigcup_{\ell \in [L], k \in [K/2]} \tau^{\ell}(E^{\ell}_{k,J^{\ell}_{k}}),$$

and therefore

$$\begin{aligned} |M_{ALG} \cap (A_P \times (Q \setminus B_Q))| &\leq \sum_{\ell \in [L], k \in [K/2]} |\mathrm{ALG}^{\ell}_{k} \cap \tau^{\ell}(E^{\ell}_{k,J^{\ell}_{k}})| \\ &= \sum_{\ell \in [L], k \in [K/2]} |\mathrm{ALG}^{\ell}_{k} \cap \widehat{E}^{\ell}_{k,J^{\ell}_{k}}|, \end{aligned}$$

since ALG can only output edges that it remembered as per model definition (Definition 3). Taking expectations of both sides and using (93), we get

$$\begin{aligned} \mathbf{E}_{\widehat{G}\sim\mathcal{D}}\left[|M_{ALG} \cap (A_P \times (Q \setminus B_Q))|\right] &\leq \sum_{\ell \in [L], k \in [K/2]} \mathbf{E}_{\widehat{G}\sim\mathcal{D}}\left[|\mathrm{ALG}^{\ell}_{k} \cap \widehat{E}^{\ell}_{k,J^{\ell}_{k}}|\right] \\ &\leq \sum_{\ell \in [L], k \in [K/2]} \mathbf{E}_{\widehat{G}\sim\mathcal{D}}\left[|\mathrm{ALG}^{\ell}_{k} \cap \widehat{E}^{\ell}_{k,J^{\ell}_{k}}|\right] \\ &\leq LK \cdot \frac{1}{n/(2KL)} s \\ &\leq 2L^2K^2 \cdot \frac{s}{n} \\ &= O\left(\frac{s}{\log |P|}\right), \end{aligned}$$

where the last transition uses the fact that $n = \log_m N = \Omega(\log n) = \Omega(\log |P|)$. Since $s = o(|P| \log |P|)$ by assumption, we get

$$\mathbf{E}_{\widehat{G}\sim\mathcal{D}}\left[|M_{ALG} \cap (A_P \times (Q \setminus B_Q))|\right] = o(|P|),$$

and therefore by Markov's inequality

$$\mathbf{Pr}_{\widehat{G}\sim\mathcal{D}}\left[|M_{ALG} \cap (A_P \times (Q \setminus B_Q))| > (1/L)|P|\right] = o(1).$$

Finally, we note that the graph $\widehat{G}$ contains a matching M_{OPT} satisfying $|M_{OPT}| \geq (1 - O(1/L))|P|$ by Lemma 67. Combining the above bounds with (92), we get

$$\mathbf{Pr}_{\widehat{G}\sim\mathcal{D}}\left[|M_{ALG}| > \left(\frac{1}{1+\ln 2} + O(1/L)\right)|M_{OPT}|\right] = o(1),$$

as required. ■

Proof of Theorem 5: Follows directly by Theorem 76 by setting K to be a sufficiently large constant. ■

4 Main result

In the rest of the paper we prove our main result, i.e. Theorem 1. We define the individual instances G^ℓ, establish their main properties and define the glueing map τ^ℓ in Section 5. We then define the predecessor map ν and establish its main properties in Section 6. We then give the proof of the lower bound in Section 7.

5 Basic gadgets and the glueing map τ

The input graph $G = (P, Q, E)$ is a edge disjoint (but not vertex disjoint) union of graphs $G^\ell = (S^\ell, T^\ell, E^\ell), \ell \in [L]$, that we define below. For every $\ell \in [L]$ we have $|T^\ell| = N = m^n$, and have $|S^\ell| \approx N/2$. The instances G^ℓ are then tied together via carefully designed maps τ^ℓ:

$$\tau^\ell : S^\ell \to T_*^{\ell-1},$$

where $T_*^{\ell-1}$ is a special subset of $T^{\ell-1}$ that we refer to as the *terminal subcube* of $T^{\ell-1}$. The maps τ^ℓ are injective, but not defined on the entirety of S^ℓ: a small fraction of vertices are left unmapped, and contribute to various error terms in our analyisis. Overall, this mapping ensures that the bipartition $P \cup Q$ of the graph G satisfies

$$P \approx \bigcup_{\text{even } \ell \in [L/2]} T^\ell$$

and

$$Q \approx S^0 \cup \bigcup_{\text{odd } \ell \in [L/2]} T^\ell.$$

The $\approx$ sign in the equations above reflects a small fraction of vertices in $S^\ell, \ell \in [L], \ell > 0$, that the corresponding map τ^ℓ is not defined on – see (239) and (240) in Section 7 below.

5.1 Basic definitions and notation

Throughout the paper we use the notation $[a] = \{0, 1, \ldots, a-1\}$ for a positive integer a.

Associating vertices with points in the hypercube $[m]^n$. Every vertex in P and Q is equipped with a label from $[m]^n$ which we denote by

$$\text{label} : P \cup Q \to [m]^n.$$

For a pair of vertices $x \in P$ and $y \in Q$ we write $x \asymp y$ if $\text{label}(x) = \text{label}(y)$. For every $\ell \in [L]$ vertices in T^ℓ have distinct labels, and for every $k \in [K/2]$ vertices in S_k^ℓ also have distinct labels (their labels are a subset of the labels of T^ℓ). Thus, we will often think of vertices in G^ℓ as points in the hypercube when we think of vertices in T^ℓ, or vertices in S_k^ℓ and k is fixed.

Definition 77 (Weight of a vertex (or point in the hypercube)) *For every $x \in [m]^n$ we define*

$$wt(x) = \sum_{j \in [n]} x_j.$$

We will routinely apply the weight function to vertices of G. For a vertex x of G we write $wt(x)$ to denote $wt(label(x))$.

Definition 78 (Boundary points) *We define the set $B \subset [m]^n$ of boundary points by*

$$B = \{x \in [m]^n : x_i < n^2 \text{ or } x_i > m - n^2 \text{ for some } i \in [n]\}.$$

We have

Claim 79 *The fraction of boundary points in $[m]^n$ is bounded by $1/n^{10}$ long as $m \geq n^{20}$ and $n > 2$, which we assume throughout the paper.*

Proof: This follows by a union bound. Pick a point $x \in [m]^n$ uniformly at random. The probability that a a fixed coordinate is smaller than n^2 of larger than $m - n^2$ is at most $2n^2/m$. Thus, the probability that at least one coordinate of x is at most n^2 or at least $m - n^2$ is bounded by $2n^3/m$ by a union bound. Since $m \geq n^{20}$ by assumption, the result follows. ■

We note that the assumption of Claim 79 above is satisfied by property (p0) of parameter setting that we ensure throughout this section.

Family of fixed weight vectors $\mathcal{F}$ with small pairwise dot products. We let $\mathcal{F}$ be a family of vectors in $\{0,1\}^n$ of Hamming weight $w = (\epsilon/2)n$ such that for every $\mathbf{u}, \mathbf{v} \in \mathcal{F}$ one has

$$\langle \mathbf{u}, \mathbf{v} \rangle \leq \epsilon w.$$

Fix such a family $\mathcal{F}$ with $|\mathcal{F}| = 2^{\Omega(\epsilon^2 n)}$. The existence of such a family can be established by the probabilistic method – we include the proof in Appendix C.1 for completeness. We partition $\mathcal{F}$ into disjoint subsets of equal size, letting

$$\mathcal{F} = \mathbf{B}^0 \cup \mathbf{B}^1 \cup \ldots \cup \mathbf{B}^{L-1},$$

where $\mathbf{B}^i \cap \mathbf{B}^j = \emptyset$ if $i \neq j$. For every $\ell \in [L]$ the set of vectors $\mathbf{B}^\ell$ will be used to define a corresponding graph G^ℓ, and these graphs will be presented to the algorithm in the stream sequentially for $\ell \in [L]$. Every set $\mathbf{B}^\ell$ is partitioned as

$$\mathbf{B}^\ell = \mathbf{B}^\ell_0 \cup \ldots \cup \mathbf{B}^\ell_{K/2}, \tag{94}$$

where $|\mathbf{B}^\ell_k| = \frac{1}{L(K/2+1)} \cdot |\mathcal{F}|$ for $k \in [K/2+1]$, and $\mathbf{B}^\ell_k \cap \mathbf{B}^\ell_{k'} = \emptyset$ for $k \neq k'$. The ℓ-th graph G^ℓ is mainly parameterized by a sequence

$$\mathbf{J}^\ell \in \mathbf{B}^\ell_0 \times \ldots \times \mathbf{B}^\ell_{K/2}, \tag{95}$$

i.e., $\mathbf{J}^\ell_k \in \mathbf{B}^\ell_k$ for $k \in [K/2+1]$, as well as a vector $\mathbf{r}^\ell \in \mathbf{B}^\ell_{K/2}$ that we refer to as the ℓ-th compression vector (see Definition 81 below).

Definition 80 (Special vectors of the ℓ-th instance) *We refer to $\mathbf{J}^\ell$ and $\mathbf{r}^\ell$ as the* special vectors *of instance G^ℓ, and let*

$$\Psi(\mathbf{B}^\ell) := (\mathbf{J}^\ell, \mathbf{r}^\ell).$$

We also define the extended special coordinates

$$\widetilde{\Psi}(\mathbf{B}^\ell) := \mathbf{J}^\ell \cup \{\mathbf{r}^\ell\} \cup \bigcup_{k \in [K]} (\mathrm{Ext}^\ell_k \cup \{\mathbf{q}^\ell_k\}). \tag{96}$$

For every $\ell \in [L], \ell > 0$, the map τ^ℓ is parameterized by vector $\mathbf{r}^\ell \in \mathbf{B}^\ell$, referred to as the *compression vector* for the terminal subcube T^ℓ_*, as well as a collection of *extension vectors* for every $k \in [K/2]$.

Definition 81 (Compression vectors and extension vectors) *For every $k \in [K/2]$*[5] *let*

$$\mathit{Ext}^\ell_k \subseteq \mathbf{B}^\ell_k$$

denote a set of $K/2+1-k$ vectors referred to as the extension vectors *and*

$$\mathbf{q}^\ell_k \in \mathbf{B}^\ell_k \setminus \mathit{Ext}^\ell_k$$

denote the compression vector *for the k-th phase of the graph G^ℓ. Let $\mathbf{r}^\ell \in \mathbf{B}^\ell_{K/2}$ denote the ℓ-th* compression vector.

Define for $k \in [K/2]$

$$\mathring{\mathbf{B}}^\ell_k = \mathbf{B}^\ell_k \setminus (\{\mathbf{q}^\ell_k\} \cup \mathrm{Ext}^\ell_k) \tag{97}$$

and let

$$\mathring{\mathbf{B}}^\ell_{K/2} = \mathbf{B}^\ell_{K/2} \setminus \{\mathbf{r}^\ell\}. \tag{98}$$

For every $\ell \in [L]$ and $k \in [K/2+1]$ select

$$\mathbf{J}^\ell_k \in \mathring{\mathbf{B}}^\ell_k.$$

5.2 Parameter setting

We choose parameters $\epsilon, \delta, M, W, K$ and L so that ϵ, δ, L only depend on K and the following properties are satisfied:

(p0) $m = n^{20}$

(p1) $W/w = \mathrm{lcm}(K, K-1, \ldots, 2, 1)$

(p2) $\delta^{-1} \cdot \mathrm{lcm}(K, K-1, \ldots, 2, 1) \cdot W/w \mid M/w$.

(p3) $\Delta = \frac{1}{\mathrm{lcm}(K, K-1, K-2, \ldots, 2, 1)}$; note that $\Delta \leq 1/K$ and that $\Delta \cdot M/w$ is an integer by (p2).

(p4) $L = \sqrt{K}$

(p5) $\delta \leq \Delta^{100K^2}$

(p6) $\epsilon \leq \delta^2$

(p7) $\epsilon \geq w/M$

In the above we write $\mathrm{lcm}(a_1, a_2, \ldots, a_s)$ to denote the least common multiple of $a_1, a_2, \ldots, a_s$. For $a > 0, b > 0$ we write $a \mid b$ if b/a is an integer.

Lemma 82 *For every constant K there exists a setting of ϵ as a function of K and a setting of parameters M, W, Δ, L, δ and $m = poly(n)$ that satisfies (p0)-(p7).*

[5] Note that we only define the extension vectors Ext^ℓ_k and the compression vector $\mathbf{q}^\ell_k$ for $k \in [K/2] = \{0, 1, 2, \ldots, K/2-1\}$, even though the sequence $\mathbf{J}^\ell$ is of length $K/2+1$. This is for convenience in defining the glueing map τ^ℓ – see Section 5.10 for more details.

Proof: For any $\epsilon \in (0,1)$ such that $(1/\epsilon)^{1/3}$ is an integer, let $w = (\epsilon/2)n$, as required by the construction of the set $\mathcal{F}$, and let

$$\delta = \epsilon^{1/2},$$

ensuring that (p6) holds with equality. Let

$$M = w/\epsilon = n/2,$$

so that (p7) is satisfied with equality. Let $W = \text{lcm}(K, K-1, \ldots, 2, 1) \cdot w$, as per (p1). Note that in order to satisfy (p2), it suffices to ensure that

$$\begin{aligned} \frac{M/w}{\delta^{-1} \cdot \text{lcm}(K, K-1, \ldots, 2, 1) \cdot W/w} &= \frac{1/\epsilon}{\epsilon^{-1/2} \cdot (\text{lcm}(K, K-1, K-2, \ldots, 2, 1))^2} \\ &= \frac{(1/\epsilon)^{1/2}}{(\text{lcm}(K, K-1, K-2, \ldots, 2, 1))^2} \end{aligned}$$

is an integer. We let

$$1/\epsilon = (\text{lcm}(K, K-1, K-2, \ldots, 2, 1))^{400K^2},$$

ensuring that

$$\begin{aligned} \frac{(1/\epsilon)^{1/2}}{(\text{lcm}(K, K-1, K-2, \ldots, 2, 1))^2} &= \frac{\left((\text{lcm}(K, K-1, K-2, \ldots, 2, 1))^{400K^2}\right)^{1/2}}{(\text{lcm}(K, K-1, K-2, \ldots, 2, 1))^2} \\ &= (\text{lcm}(K, K-1, K-2, \ldots, 2, 1))^{200K^2-2}, \end{aligned}$$

ensuring that (p2) holds.

We set $\Delta = \frac{1}{\text{lcm}(K, K-1, K-2, \ldots, 2, 1)}$ as per (p3), and verify that

$$\begin{aligned} \delta &= (1/\epsilon)^{1/2} \\ &= \left((\text{lcm}(K, K-1, K-2, \ldots, 2, 1))^{-400K^2}\right)^{1/2} \\ &= \text{lcm}(K, K-1, K-2, \ldots, 2, 1))^{-200K^2} \\ &\leq \Delta^{100K^2}, \end{aligned}$$

so (p5) is satisfied.

Finally, we let $L = \sqrt{K}$, satisfying (p4). Letting K be a sufficiently large constant and n sufficiently large as a function of K and letting $m = n^{20}$ to satisfy (p0) completes the setting of parameters. ■

5.3 Basic gadgets G^ℓ: vertex set and main definitions

In this section we define our gadgets $G^\ell = (S^\ell, T^\ell, E^\ell)$. Since ℓ is fixed throughout this section, we omit the superscript and let $S = S^\ell, T = T^\ell, E = E^\ell$.

Vertices of G and their labels. Let $m \geq 1$ be a sufficiently large integer. We have $|T| = m^n$, and label vertices in T with points in the hypercube $[m]^n$, where $[m] = \{0, 1, 2, \ldots, m-1\}$. The labelling defines a bijective mapping from the vertex set T to $[m]^n$, and we hence sometimes refer to vertices in T as simply points in $[m]^n$. The vertices on the S side of the bipartition will also be labelled with points on the hypercube $[m]^n$, as defined below. The average degree of a vertex in our construction will be $2^{\Omega_\epsilon(n)}$, which translates to average degree $N^{\Omega_\epsilon(1/\log\log N)}$ when $m = \text{poly}(n)$ (this is how we set m as per Lemma 82).

The set S of vertices is partitioned into disjoint subsets $S = S_0 \uplus S_1 \uplus \ldots \uplus S_{K/2-1}$ whose vertices are also labeled with elements of $[m]^n$. We now define S_k for $k \in [K/2]$. Let $\mathbf{B} := \mathbf{B}^\ell$ as per (94), so that $\mathbf{B} = \mathbf{B}_0 \cup \ldots \cup \mathbf{B}_{K/2}$, and let $\mathbf{J} := \mathbf{J}^\ell$ as per (95). For every vertex $y \in S \cup T$ and vector $\mathbf{u} \in \mathcal{F}$ we use the notation

$$\langle y, \mathbf{u} \rangle = \sum_{s \in [n]} y_s \cdot \mathbf{u}_s,$$

where y_s stands for the s-th coordinate of the label of y. In what follows we often write, for two vertices $x, y \in S \cup T$ and a vector $\mathbf{u} \in \mathbb{Z}^n$

$$x = y + \mathbf{u}$$

if the label of x can be obtained by adding $\mathbf{u}$ to the label of y, i.e. $x_s = y_s + \mathbf{u}_s$ for every $s \in [n]$. Similarly, we often write $x = y + \mathbf{u}$ when $x \in S \cup T$ and $y \in [m]^n$ if the label of x is the sum of y and $\mathbf{u}$. In other words, we treat vertices of G and points in $[m]^n$ where this does not lead to confusion (see Remark 84).

Nested sequence $T = T_0 \supset T_1 \supset \ldots \supset T_{K/2}$ and downsets $S_0, S_1, \ldots, S_{K/2-1}$. We let $T_0 = T$, i.e. every $x \in T_0$ is labeled with an element of $[m]^n$. For every $k \in [K/2]$ let

$$T_{k+1} := \left\{ y \in T_k : \langle y, \mathbf{j}_k \rangle \pmod{M} \in \left[0, 1 - \frac{1}{K-k}\right) \cdot M \right\}. \tag{99}$$

Note that $T_0 \supset T_1 \supset \ldots \supset T_{K/2}$ form a nested sequence. Also note that for every $k \in [K/2]$ one has

$$T_k := \left\{ y \in T_0 : \langle y, \mathbf{j}_s \rangle \pmod{M} \in \left[0, 1 - \frac{1}{K-s}\right) \cdot M \text{ for all } s \in \{0, 1, \ldots, k-1\} \right\}. \tag{100}$$

The innermost set in this sequence is a central object of our construction:

Definition 83 (Terminal subcube) *We refer to $T_* := T_{K/2}$ as the* terminal subcube.

Recall that for a pair of vertices $x, y \in S \cup T$ the relation $x \asymp y$ stands for ‘the label of x equals the label of y’. We extend this relation to sets in the natural way, writing $A \asymp B$ for $A, B \subseteq S \cup T$ if there exists a bijective map $\pi : A \to B$ such that for every $x \in A$ one has $x \asymp \pi(x)$. With this notation we define

$$S_k :\asymp \left\{ x \in T_k : \mathrm{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \right\}, \tag{101}$$

The above stands for S_k being a set of vertices such that $S_k \asymp \widetilde{T}_k$, where

$$\widetilde{T}_k := \left\{ x \in T_k : \mathrm{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \right\}$$

is the set of vertices in T_k whose weight modulo W belongs to a certain range. We stress here that unlike the collection of sets T_k, the sets S_k are disjoint.

Remark 84 *The labels of vertices in S_k for any $k \in [K/2]$ are distinct, the labels of vertices in S_k are a subset of the labels of vertices in S_l for $k > l$. Thus, while a vertex in T is uniquely identified by its label, a vertex in S is not. However, a vertex in S is uniquely identified by its label together with the index $k \in [K/2]$ of the set S_k that it belongs to.*

We also let, for every $k \in [K/2]$ and $\mathbf{j} \in \mathbf{B}_k$

$$\begin{aligned} T_k^{\mathbf{j}} &= \left\{ y \in T_k : \langle y, \mathbf{j} \rangle \pmod M \in \left[0, 1 - \frac{1}{K-k}\right) \cdot M \right\} \\ S_k^{\mathbf{j}} &= \left\{ x \in S_k : \langle x, \mathbf{j} \rangle \pmod M \in \left[0, 1 - \frac{1}{K-k}\right) \cdot M \right\}. \end{aligned} \tag{102}$$

We gather basic bounds on the sizes of the sets T_k, S_k in

Lemma 85 *One has*

- **(1)** *For every $k \in [K/2+1]$ one has $|T_k| = (1 \pm \sqrt{\epsilon}) \cdot |T_0|(1 - k/K)$;*
- **(2)** *For every $k \in [K/2]$ one has $|S_k| = (1 \pm \sqrt{\epsilon}) \cdot |T_0|/K$;*
- **(3)** *For every $k \in [K/2]$, every $\mathbf{j} \in \mathbf{B}_k$ one has $|S_k^{\mathbf{j}}| = (1 \pm \sqrt{\epsilon})(1 - \frac{1}{K-k})|T_0|/K$.*
- **(4)** *For every $k \in [K/2]$, every $\mathbf{j} \in \mathbf{B}_k$ one has $|T_k^{\mathbf{j}}| = (1 \pm \sqrt{\epsilon})(1 - \frac{k+1}{K})|T_0|$.*

Remark 86 *Note that the sets S_k are defined for $k \in [K/2]$, whereas T_k is defined for $k \in [K/2+1]$ – this is to ensure that the number of vertices in the terminal subcube T_* can be made arbitrarily close to the total size of $\biguplus_{k \in [K/2]} S_k$ for any fixed K by choosing ϵ sufficiently small, simplifying the definition and analysis of the glueing maps τ^ℓ (see Section 5.10) that map sets of the latter type to sets of the former type.*

Since per (101) for every $k \in [K/2]$ the set S_k is essentially a subsampling of the corresponding set T_k, for every $U \subseteq T_k$ we define the projection of U to S_k, denoted by $\textsc{DownSet}_k(U)$, as the set of vertices in S_k whose labels match the labels of vertices in U:

Definition 87 (Downset of a subset of T) *For every $U \subseteq T$ and $k \in [K/2]$ we define the* downset of U in *S_k by*

$$\textsc{DownSet}_k(U) = \{x \in S_k : \exists y \in U \text{ s.t. } x \asymp y\}.$$

We define

$$\textsc{DownSet}(U) = \bigcup_{k \in [K/2]} \textsc{DownSet}_k(U).$$

Remark 88 *We note that* $\textsc{DownSet}$ *is defined as a map from subsets of T to subsets of S. This certainly defines a natural mapping from elements of T: element $x \in T$ is mapped to* $\textsc{DownSet}(\{x\})$*, i.e. the downset of the singleton set containing x. However, this map is not one to one:* $\textsc{DownSet}(\{x\})$ *may be a set of size up to $K/2$ (note, however, that for every $k \in [K/2]$ one has $|\textsc{DownSet}_k(\{x\})| \leq 1$).*

Remark 89 *Note that if $U \subset T_k \setminus T_{k+1}$ for some $k \in [K/2]$, then $\textsc{DownSet}_s(U) = \emptyset$ for all $s \in \{k+1, \ldots, K/2-1\}$. Thus, in that case we have*

$$\textsc{DownSet}(U) = \bigcup_{s=0}^{k} \textsc{DownSet}_s(U).$$

5.4 Edges of G

Similarly to our construction in Section 3, we define the edge set of G to be a union of constant size complete bipartite subgraphs, where for every $k \in [K/2]$ and every direction $\mathbf{j} \in \mathbf{B}_k$ the edge set $E_k \subseteq T_k \times S_k$ consists of a disjoint union of small bipartite subgraphs for every 'line' in direction $\mathbf{j}$. Unlike the construction of Section 3, it takes more care to define lines appropriately when $\mathbf{j}$ is not just a coordinate direction, but rather a general binary vector in $\mathcal{F}$, and different directions are not necessarily orthogonal, but rather just have small dot products. For that we first need

Definition 90 (Block of x with respect to a vector j) *For $\mathbf{j} \in \mathcal{F}$ we define block$_{\mathbf{j}}(x) := \lfloor \langle x, \mathbf{j} \rangle / M \rfloor$.*

We can now define

Definition 91 (Line through x in direction j) *For each $\mathbf{j} \in \mathbf{B}_k$ for each $x \in [m]^n$ we denote the line in direction $\mathbf{j}$ going through x by*

$$\textit{line}_{\mathbf{j}}(x) = \left\{ x' \in [m]^n : x' = x + \lambda \cdot \mathbf{j} \textit{ for } \lambda \in \mathbb{Z} \textit{ s.t. } \textit{block}_{\mathbf{j}}(x') = \textit{block}_{\mathbf{j}}(x) \right\}.$$

Some basic properties of lines are given in

Claim 92 (Basic bounds on lines) *For every $\mathbf{j} \in \mathcal{F}$:*

(1) *for every $x \in [m]^n$ one has $|\textit{line}_{\mathbf{j}}(x)| \leq M/w$ and for every $x \in [m]^n \setminus B$ one has $|\textit{line}_{\mathbf{j}}(x)| = M/w$; furthermore, for every $x \in [m]^n$ and $y \in \textit{line}_{\mathbf{j}}(x)$ one has $y = x + \lambda \cdot \mathbf{j}$ for some integer λ satisfying $|\lambda| \leq 2M/w$.*

(2) *for every $x \in [m]^n \setminus B$, for every $c \in \Delta \cdot \mathbb{Z} \cap [0, 1)$ one has*

$$|\{y \in \textit{line}_{\mathbf{j}}(x) : \langle y, \mathbf{j} \rangle \pmod{M} \in [c, c + \delta) \cdot M\}| = \delta \cdot M/w.$$

(3) *for every $x \in [m]^n \setminus B$, for every $c \in \Delta \cdot \mathbb{Z} \cap (0, 1]$ one has*

$$|\{y \in \textit{line}_{\mathbf{j}}(x) : \langle y, \mathbf{j} \rangle \pmod{M} \in [c - \delta, c) \cdot M\}| = \delta \cdot M/w.$$

Proof: We start by proving some useful basic facts, and the proceed to prove **(1), (2)** and **(3)**. First note that for $x \in [m]^n$ and $x' = x + \lambda \cdot \mathbf{j} \in \mathbb{Z}^n$ (but not necessarily in $[m]^n$) one has

$$\langle x', \mathbf{j} \rangle = \langle x + \lambda \cdot \mathbf{j}, \mathbf{j} \rangle = \langle x, \mathbf{j} \rangle + \lambda \cdot w. \tag{103}$$

This means that $|\lambda| \leq 2M/w$ for all such $x' \in \text{line}_{\mathbf{j}}(x)$, as otherwise $\text{block}_{\mathbf{j}}(x') \neq \text{block}_{\mathbf{j}}(x)$. By Definition 78 we have $n^2 \leq x_i \leq m - n^2$ for all $x \in [m]^n \setminus B$ and $i \in [n]$. Thus, for all such x we have, since $\mathbf{j} \in \{0, 1\}^n$,

$$n^2 - 2M/w \leq x_i + \lambda \cdot \mathbf{j}_i \leq m - n^2 + 2M/w$$

for all $i \in [n]$. By (p1) and (p2) together with the fact that n is sufficiently large as a function of $M/w, W/w, K, L, \Delta$, and δ, we get

$$0 \leq x_i + \lambda \cdot \mathbf{j}_i \leq m - 1$$

for all $i \in [n]$. Thus,

$$x' = x + \lambda \cdot \mathbf{j} \in [m]^n. \tag{104}$$

We now prove **(1)**. Let $q = \langle x, \mathbf{j} \rangle \pmod{M}$ to simplify notation, so that $\langle x, \mathbf{j} \rangle = \text{block}_{\mathbf{j}}(x) \cdot M + q$. Further, let $a = \lfloor \frac{1}{w} q \rfloor$ and $b = q \pmod{w}$. With this notation in place we have

$$\langle x', \mathbf{j} \rangle = \langle x + \lambda \cdot \mathbf{j}, \mathbf{j} \rangle = \langle x, \mathbf{j} \rangle + \lambda \cdot w = \text{block}_{\mathbf{j}}(x) \cdot M + (a + \lambda) \cdot w + b. \tag{105}$$

We thus have

$$\text{block}_{\mathbf{j}}(x') = \lfloor (\text{block}_{\mathbf{j}}(x) \cdot M + (a+\lambda) \cdot w + b)/M \rfloor = \text{block}_{\mathbf{j}}(x) + \lfloor ((a+\lambda) \cdot w + b)/M \rfloor,$$

and hence $\text{block}_{\mathbf{j}}(x') = \text{block}_{\mathbf{j}}(x)$ if and only if $((a-\lambda) \cdot w + b)/M \in [0,1)$. On the other hand, since $b \in \{0,1,\ldots,w-1\}$, we have

$$\{\lambda \in \mathbb{Z} : ((a+\lambda) \cdot w + b)/M \in [0,1)\} = \{-a, \ldots, -a + M/w - 1\},$$

which is a set of size M/w since $w \mid M$ by (p2). This proves the upper bound in **(1)**. For the lower bound we note that if $x \in [m]^n \setminus B$, then every $x' = x + \lambda \cdot \mathbf{j}$ such that $\text{block}_{\mathbf{j}}(x') = \text{block}_{\mathbf{j}}(x)$ one has $|\lambda| \leq 2M/w$, and therefore $x' \in [m]^n$ by (104) (see argument above for more details). This implies the lower bound, and hence the equality in **(1)**. In particular, we get for $x \in [m]^n \setminus B$

$$\text{line}_{\mathbf{j}}(x) = \{x + \lambda \cdot \mathbf{j} : \lambda \in \{-a, \ldots, -a + M/w - 1\}. \tag{106}$$

We now prove **(2)**. First note that by (106) we have

$$\begin{aligned}
&|\{y \in \text{line}_{\mathbf{j}}(x) : \langle y, \mathbf{j} \rangle \pmod{M} \in [c, c+\delta) \cdot M\}| \\
&= |\{\lambda \in \{-a, \ldots, -a + M/w - 1\} : \langle x + \lambda \cdot \mathbf{j}, \mathbf{j} \rangle \pmod{M} \in [c, c+\delta) \cdot M\}| \\
&= |\{\lambda \in \{-a, \ldots, -a + M/w - 1\} : (a+\lambda) \cdot w + b \in [c, c+\delta) \cdot M\}|\,.
\end{aligned}$$

Since $\delta^{-1} \mid M/w$ by (p2), $c \in \Delta \cdot \mathbb{Z} \cap [0,1)$ by assumption of the claim and $\Delta \mid M/w$ by (p3), we can write $c \cdot M = \alpha \cdot w$ and $c + \delta = \beta \cdot w$ for integers $\alpha, \beta \in \{0, 1, \ldots, M/w - 1\}$, $\alpha < \beta$ (here we used the fact that $\delta < \Delta$ by (p5)). The last line of the equation above can thus be rewritten as

$$\begin{aligned}
&|\{\lambda \in \{-a, \ldots, -a + M/w - 1\} : (a+\lambda) \cdot w + b \in [c, c+\delta) \cdot M\}| \\
&= |\{\lambda \in \{-a, \ldots, -a + M/w - 1\} : \alpha \cdot w \leq (a+\lambda) \cdot w + b < \beta \cdot w\}| \\
&= \beta - \alpha \\
&= (\beta \cdot w - \alpha \cdot w)/w \\
&= ((c+\delta) \cdot M - c \cdot M)/w \\
&= \delta \cdot M/w,
\end{aligned}$$

where the second equality holds because $b \in \{0, \ldots, w-1\}$ and the fourth equality is by definition of α and β. This proves **(2)**. The proof of **(3)** is analogous. ■

Lemma 93 (Lines form a partition) *For every $\mathbf{j} \in \mathcal{F}$, every $x, x' \in [m]^n$ one has either line$_{\mathbf{j}}(x) =$ line$_{\mathbf{j}}(x')$ or line$_{\mathbf{j}}(x) \cap$ line$_{\mathbf{j}}(x') = \emptyset$.*

The proof of the lemma follows from a more general statement about subspaces (see Claim 109 and Lemma 111) and its proof is given in Section 5.5.

Definition 94 (Minimal j-line cover) *We say that a set $C \subset [m]^n$ is a minimal $\mathbf{j}$-line cover if $\bigcup_{x \in C}$ line$_{\mathbf{j}}(x) = [m]^n$ and line$_{\mathbf{j}}(x) \cap$ line$_{\mathbf{j}}(x') = \emptyset$ for $x, x' \in C$, $x \neq x'$.*

We now define the edges of G incident on S_k for every $k \in [K/2]$. For every $\mathbf{j} \in \mathring{\mathbf{B}}_k$ let

$$C_{\mathbf{j}} \subset [m]^n \tag{107}$$

be a minimal $\mathbf{j}$-line cover as per Definition 94. For every $y \in C$, we include a complete bipartite graph between $\text{line}_{\mathbf{j}}(y) \cap \text{Int}_\delta(S_k^{\mathbf{j}})$ and $\text{line}_{\mathbf{j}}(y) \cap (T_k \setminus T_k^{\mathbf{j}})$: let $E = \bigcup_{k \in [K/2]} E_k$, where

$$E_k = \bigcup_{\mathbf{j} \in \overset{\circ}{\mathbf{B}}_k} E_{k,\mathbf{j}} \tag{108}$$

and

$$E_{k,\mathbf{j}} = \bigcup_{y \in C_{\mathbf{j}}} (\text{line}_{\mathbf{j}}(y) \cap \text{Int}_\delta(S_k^{\mathbf{j}})) \times (\text{line}_{\mathbf{j}}(y) \cap (T_k \setminus T_k^{\mathbf{j}})). \tag{109}$$

In the equation above we use the notation $\text{Int}_\delta(S_k^{\mathbf{j}})$ for the δ-*interior* of the set $S_k^{\mathbf{j}}$, which we now define. First recall that by (100) and definition of S_k in (101) we have

$$\begin{aligned} S_k \asymp \Bigg\{ & y \in [m]^n : \langle y, \mathbf{j}_s \rangle \pmod M \in \left[0, 1 - \frac{1}{K-s}\right) \cdot M \text{ for all } s \in \{0, 1, \ldots, k-1\} \\ & \text{and} \\ & \text{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W \Bigg\} \end{aligned}$$

and

$$\begin{aligned} S_k^{\mathbf{j}} \asymp \Bigg\{ & y \in [m]^n : \langle y, \mathbf{j}_s \rangle \pmod M \in \left[0, 1 - \frac{1}{K-s}\right) \cdot M \text{ for all } s \in \{0, 1, \ldots, k-1\} \\ & \text{and} \\ & \langle y, \mathbf{j} \rangle \pmod M \in \left[0, 1 - \frac{1}{K-k}\right) \cdot M \\ & \text{and} \\ & \text{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W \Bigg\} \end{aligned}$$

The interior of $S_k^{\mathbf{j}}$, denoted by $\text{Int}_\delta(S_k^{\mathbf{j}})$, is simply the set of points in $S_k^{\mathbf{j}}$ that satisfy all the constraints above (except the subsampling constraint) with a margin of δ:

$$\begin{aligned} \text{Int}_\delta(S_k^{\mathbf{j}}) \asymp \Bigg\{ & y \in [m]^n : \langle y, \mathbf{j}_s \rangle \pmod M \in \left[\delta, 1 - \frac{1}{K-s} - \delta\right) \cdot M \text{ for all } s \in \{0, 1, \ldots, k-1\} \\ & \text{and} \\ & \langle y, \mathbf{j} \rangle \pmod M \in \left[\delta, 1 - \frac{1}{K-k} - \delta\right) \cdot M \\ & \text{and} \\ & \text{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W \Bigg\} \end{aligned} \tag{110}$$

Remark 95 *We note that our definition of the interior $\text{Int}_\delta(S_k^{\mathbf{j}})$ of $S_k^{\mathbf{j}}$ is a special case of Definition 103 below. We prefer to present it here first before presenting the more general version to alleviate notation in the definition of the basic gadgets G^ℓ.*

Remark 96 *Note that the edge set E_k is fully defined by the prefix $\mathbf{J}_{<k}$ (note that we consider the compression indices and extension indices fixed and $\mathbf{J}$ variable; this is useful since in the actual hard input distribution we will fix the compression and extension indices arbitrarily, and select $\mathbf{J}$ uniformly at random from $\mathring{\mathbf{B}}_0 \times \mathring{\mathbf{B}}_1 \times \ldots \times \mathring{\mathbf{B}}_{K/2}$ – see Section 7).*

Remark 97 *We note that the edge set defined in* (109) *does not depend on the specific choice of a cover $C_{\mathbf{j}}$ used, i.e. any minimal* $\mathbf{j}$*-line cover produces the same edge set as per* (109)*.*

The following lemma shows that the complete bipartite graphs defined above are disjoint (this will be useful for analyzing a subsampling of the gadgets G^ℓ later in Section 7)

Lemma 98 *For every $k \in [K/2]$, every $\mathbf{i}, \mathbf{j} \in \mathring{\mathbf{B}}_k, \mathbf{i} \neq \mathbf{j}$, every $x \in C_{\mathbf{i}}, y \in C_{\mathbf{j}}$, where $C_{\mathbf{i}}$ and $C_{\mathbf{j}}$ are minimal* $\mathbf{i}$*- and* $\mathbf{j}$*-line covers respectively, the edge sets*

$$(\textit{line}_{\mathbf{i}}(x) \cap \textit{Int}_\delta(S_k^{\mathbf{i}})) \times (\textit{line}_{\mathbf{i}}(x) \cap (T_k \setminus T_k^{\mathbf{i}}))$$

and

$$(\textit{line}_{\mathbf{j}}(y) \cap \textit{Int}_\delta(S_k^{\mathbf{j}})) \times (\textit{line}_{\mathbf{j}}(y) \cap (T_k \setminus T_k^{\mathbf{j}}))$$

are disjoint.

Proof: We argue by contradiction. Note that the edge sets above intersect if and only if there exist a, b such that

$$a \in (\text{line}_{\mathbf{i}}(x) \cap \text{Int}_\delta(S_k^{\mathbf{i}})) \cap (\text{line}_{\mathbf{j}}(y) \cap \text{Int}_\delta(S_k^{\mathbf{j}})) \tag{111}$$

and

$$b \in (\text{line}_{\mathbf{i}}(x) \cap (T_k \setminus T_k^{\mathbf{i}})) \cap (\text{line}_{\mathbf{j}}(y) \cap (T_k \setminus T_k^{\mathbf{j}})). \tag{112}$$

Since $a, b \in \text{line}_{\mathbf{j}}(y)$, we have by Claim 92, **(1)**, that

$$b = a + \lambda \cdot \mathbf{j}$$

for some integer λ with $|\lambda| \leq 2M/w$. This in particular means that

$$|\langle b, \mathbf{i}\rangle - \langle a, \mathbf{i}\rangle| = |\lambda| \langle \mathbf{j}, \mathbf{i}\rangle \leq |\lambda| \cdot \epsilon w \leq 2\epsilon M. \tag{113}$$

On the other hand, since $a \in \text{Int}_\delta(S_k^{\mathbf{i}})$, we have by (102) together with (110) (see also Definition 103)

$$\langle a, \mathbf{i}\rangle \pmod M \in \left[\delta, 1 - \frac{1}{K-k} - \delta\right) \cdot M.$$

Putting this together with (113) yields

$$(\delta - 2\epsilon)M \leq \langle b, \mathbf{i}\rangle \pmod M \leq (1 - \frac{1}{K-k} - \delta + 2\epsilon) \cdot M,$$

and thus since $\epsilon \leq \delta^2 < 2\delta$ by (p6), we get

$$\langle b, \mathbf{i}\rangle \pmod M \in \left[0, 1 - \frac{1}{K-k}\right) \cdot M, \tag{114}$$

a contradiction with the assumption that $b \in T_k \setminus T_k^{\mathbf{i}}$ by (112). ■

5.5 Rectangles and their properties

Our construction in this section is at a high level quite similar to the construction from Section 3. Unfortunately, however, it is more complicated, mainly due to the fact that we cannot rely on clean product structure of naturally defined rectangles (see Definition 45). However, our analysis is still based on a concept of a rectangle, which we define below – see Definition 99. While this is no longer a product set since our vectors in $\mathcal{F}$ are not orthogonal, but merely have small dot product, rectangles as per Definition 99 still behave is rather similar way to product sets. This section is devoted to proving some basic properties of rectangles that facilitate later analysis.

For two vectors $\mathbf{a}, \mathbf{b}$ of the same dimension we use the notation $\mathbf{a} < \mathbf{b}$ for $\mathbf{a}$ being coordinate-wise smaller than $\mathbf{b}$. We often index coordinates of a vector by elements of some set. For example, $\mathbf{a} \in [0,1)^{\mathbf{I}}$ stands for $\mathbf{a}$ being a vector of length $|\mathbf{I}|$ whose entries are $\mathbf{a}_{\mathbf{i}}, \mathbf{i} \in \mathbf{I}$, and for a subset $\mathbf{H} \subset \mathbf{I}$ we write $\mathbf{a}_{\mathbf{H}}$ to denote the restriction of $\mathbf{a}$ to elements of $\mathbf{H}$.

Definition 99 (Rectangles) *For every $\mathbf{I} \subseteq \mathcal{F}$, every $\mathbf{c}, \mathbf{d} \in [0,1]^{\mathbf{I}}, \mathbf{c} < \mathbf{d}$ the set*

$$\textsc{Rect}(\mathbf{I}, \mathbf{c}, \mathbf{d}) := \{y \in [m]^n : \langle y, \mathbf{i} \rangle \pmod{M} \in [\mathbf{c}_{\mathbf{i}}, \mathbf{d}_{\mathbf{i}}) \cdot M \textit{ for all } \mathbf{i} \in \mathbf{I}\}$$

is called a rectangle.

It is useful to introduce a more lightweight intermediate definition of rectangles with all side lengths equal to a parameter Δ – see Definition 100 below. This definition is useful since we can express every rectangle with coordinates divisible by Δ as a disjoint union of cubes, and at the same time cubes are somewhat more compact to represent, and will serve as our basic building blocks in what follows.

Definition 100 (Cubes) *For every $\mathbf{I} \subseteq \mathcal{F}$, every $\mathbf{a} \in \Delta \cdot \mathbb{Z} \cap [0,1)^{\mathbf{I}}$ we let*

$$\textsc{Rect}(\mathbf{I}, \mathbf{a}) = \{y \in [m]^n : \langle y, \mathbf{i} \rangle \pmod{M} \in [\mathbf{a}_{\mathbf{i}}, \mathbf{a}_{\mathbf{i}} + \Delta) \cdot M \textit{ for all } \mathbf{i} \in \mathbf{I}\}$$

denote a rectangle with all side lengths equal to Δ.

Claim 101 (Decomposition into subcubes) *For every $\mathbf{I}, \mathbf{H} \subseteq \mathcal{F}, \mathbf{I} \cap \mathbf{H} = \emptyset$, every $\mathbf{a}, \mathbf{b} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I} \cup \mathbf{H}}, \mathbf{a} < \mathbf{b}$, the rectangle $F = \textsc{Rect}(\mathbf{I} \cup \mathbf{H}, \mathbf{a}, \mathbf{b})$ satisfies*

$$F = \bigcup_{\mathbf{f} \in Q} \textsc{Rect}(\mathbf{I} \cup \mathbf{H}, (\mathbf{f}, \mathbf{a}_{\mathbf{H}}), (\mathbf{f} + \Delta \cdot \mathbf{1}_{\mathbf{I}}, \mathbf{b}_{\mathbf{H}})),$$

where

$$Q = \{0, \Delta, 2\Delta, \ldots, 1 - \Delta\}^{\mathbf{I}} \cap \prod_{\mathbf{i} \in \mathbf{I}} [\mathbf{a}_{\mathbf{i}}, \mathbf{b}_{\mathbf{i}}).$$

In particular, $|Q| = \Delta^{-|\mathbf{I}|} \prod_{\mathbf{i} \in \mathbf{I}} (\mathbf{b}_{\mathbf{I}} - \mathbf{a}_{\mathbf{I}})$.

Proof: Recall that by Definition 99 one has

$$\textsc{Rect}(\mathbf{I} \cup \mathbf{H}, \mathbf{a}, \mathbf{b}) = \{y \in [m]^n : \langle y, \mathbf{i} \rangle \pmod{M} \in [\mathbf{a}_{\mathbf{i}}, \mathbf{b}_{\mathbf{i}}) \cdot M \text{ for all } \mathbf{i} \in \mathbf{I} \cup \mathbf{H}\},$$

which means that

$$\begin{aligned}\{y \in [m]^n :&\langle y, \mathbf{i}\rangle \pmod M \in [\mathbf{a_i}, \mathbf{b_i}) \cdot M \text{ for all } \mathbf{i} \in \mathbf{I} \cup \mathbf{H}\} \\ = \{y \in [m]^n :&\langle y, \mathbf{i}\rangle \pmod M \in [\mathbf{a_i}, \mathbf{b_i}) \cdot M \text{ for all } \mathbf{i} \in \mathbf{I} \\ &\text{and} \\ &\langle y, \mathbf{i}\rangle \pmod M \in [\mathbf{a_i}, \mathbf{b_i}) \cdot M \text{ for all } \mathbf{i} \in \mathbf{H}\} \\ = \bigcup_{\mathbf{f} \in Q} \{y \in [m]^n :&\langle y, \mathbf{i}\rangle \pmod M \in [\mathbf{f_i}, \mathbf{f_i} + \Delta) \cdot M \text{ for all } \mathbf{i} \in \mathbf{I} \\ &\text{and} \\ &\langle y, \mathbf{i}\rangle \pmod M \in [\mathbf{a_i}, \mathbf{b_i}) \cdot M \text{ for all } \mathbf{i} \in \mathbf{H}\},\end{aligned}$$

where

$$Q = \{0, \Delta, 2\Delta, \ldots, 1 - \Delta\}^{\mathbf{I}} \cap \prod_{\mathbf{i} \in \mathbf{I}} [\mathbf{a_i}, \mathbf{b_i}).$$

It remains to note that for every $\mathbf{f} \in Q$ one has

$$\begin{aligned}\{y \in [m]^n :&\langle y, \mathbf{i}\rangle \pmod M \in [\mathbf{f_i}, \mathbf{f_i} + \Delta) \cdot M \text{ for all } \mathbf{i} \in \mathbf{I} \\ &\text{and} \\ &\langle y, \mathbf{i}\rangle \pmod M \in [\mathbf{a_i}, \mathbf{b_i}) \cdot M \text{ for all } \mathbf{i} \in \mathbf{H}\} \\ &= \textsc{Rect}(\mathbf{I} \cup \mathbf{H}, (\mathbf{f}, \mathbf{a_H}), (\mathbf{f} + \Delta \cdot \mathbf{1_I}, \mathbf{b_H})).\end{aligned}$$

■

As mentioned below, cubes will serve as our basic building blocks. For example, the local permutation map $\Pi_{R' \to R}$ (see Definition 117 in Section 5.10.2 below) is defined on individual cubes and then extended to a global map Π^* (see Definition 124), ultimately letting us define the glueing map τ (see Definition 125 below).

Lemma 102 (Bounds on sizes of rectangles) *For every* $\mathbf{I} \subseteq \mathcal{F}$ *such that* $|\mathbf{I}| \le K^2$, *for every* $\mathbf{c}, \mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}}$, $\mathbf{c} < \mathbf{d}$,

$$\gamma = \prod_{\mathbf{i} \in \mathbf{I}} (\mathbf{d_i} - \mathbf{c_i})$$

and

$$R = \textsc{Rect}(\mathbf{I}, \mathbf{c}, \mathbf{d}),$$

the following conditions hold:

(1) *the cardinality of* R *is bounded as*

$$(1 - \sqrt{\epsilon})\gamma \le |R|/m^n \le (1 + \sqrt{\epsilon}) \cdot \gamma$$

(2) *for every positive integer* $\lambda \le K$, *if*

$$R' = \{x \in R : \mathit{wt}(x) \pmod W \in [0, 1/\lambda) \cdot W\},$$

then the cardinality of R' *is bounded as*

$$\frac{1}{\lambda} \cdot (1 - \sqrt{\epsilon})\gamma \le \left|R'\right| / m^n \le \frac{1}{\lambda} \cdot (1 + \sqrt{\epsilon})\gamma.$$

We now prove Lemma 85, restated here for convenience of the reader:
Lemma 85 *(Restated) One has*

- **(1)** *For every* $k \in [K/2+1]$ *one has* $|T_k| = (1 \pm \sqrt{\epsilon}) \cdot |T_0|(1 - k/K)$*;*
- **(2)** *For every* $k \in [K/2]$ *one has* $|S_k| = (1 \pm \sqrt{\epsilon}) \cdot |T_0|/K$*;*
- **(3)** *For every* $k \in [K/2]$*, every* $\mathbf{j} \in \mathbf{B}_k$ *one has* $|S_k^{\mathbf{j}}| = (1 \pm \sqrt{\epsilon})(1 - \frac{1}{K-k})|T_0|/K$*.*
- **(4)** *For every* $k \in [K/2]$*, every* $\mathbf{j} \in \mathbf{B}_k$ *one has* $|T_k^{\mathbf{j}}| = (1 \pm \sqrt{\epsilon})(1 - \frac{k+1}{K})|T_0|$*.*

Proof: We start with **(1)**. Let $R = \textsc{Rect}(\mathbf{J}, \mathbf{c}, \mathbf{d})$, where $\mathbf{J} = \mathbf{J}_{<k}$ and for every $s = 0, \ldots, k-1$ one has $\mathbf{c}_{\mathbf{j}_s} = 0$ and $\mathbf{d}_{\mathbf{j}_s} = 1 - \frac{1}{K-s}$, and note that $R = T_k$ by (100) . By Lemma 102, **(1)**, one has

$$(1 - \sqrt{\epsilon})\gamma \leq |\textsc{Rect}(\mathbf{I}, \mathbf{c}, \mathbf{d})|/m^n \leq (1 + \sqrt{\epsilon}) \cdot \gamma,$$

where

$$\begin{aligned}
\gamma &= \prod_{\mathbf{i} \in \mathbf{I}} (\mathbf{d}_{\mathbf{i}} - \mathbf{c}_{\mathbf{i}}) \\
&= \prod_{s=0}^{k-1} \left(1 - \frac{1}{K-s}\right) \\
&= \prod_{s=0}^{k-1} \frac{K-s-1}{K-s} \\
&= \frac{K-(k-1)-1}{K} \\
&= 1 - k/K,
\end{aligned}$$

as required. The proof of **(4)** is analogous.

We now prove **(2).** Let $R = T_k = \textsc{Rect}(\mathbf{I}, \mathbf{c}, \mathbf{d})$, where $\mathbf{I} = \mathbf{J}_{<k}$ and for every $s = 0, \ldots, k-1$ one has $\mathbf{c}_{\mathbf{j}_s} = 0$ and $\mathbf{d}_{\mathbf{j}_s} = 1 - \frac{1}{K-s}$. Let

$$R' := \{x \in R : \mathrm{wt}(x) \pmod W \in [0, 1/(K-k)) \cdot W\},$$

and note that $R' = S_k$ by (101). Then by Lemma 102, **(2)**, with $\lambda = K - k$ and

$$\gamma = \prod_{s=0}^{k-1} (\mathbf{d}_{\mathbf{j}_s} - \mathbf{c}_{\mathbf{j}_s}) = \prod_{s=0}^{k-1} \left(1 - \frac{1}{K-s}\right) = 1 - \frac{k}{K}$$

we have

$$\frac{1}{K-k} \cdot (1 - \sqrt{\epsilon}) \left(1 - \frac{k}{K}\right) \leq |R'|/m^n \leq \frac{1}{K-k} \cdot (1 + \sqrt{\epsilon}) \left(1 - \frac{k}{K}\right).$$

Simplifying, we get

$$(1 - \sqrt{\epsilon})\frac{1}{K} \leq |R'|/m^n \leq (1 + \sqrt{\epsilon})\frac{1}{K},$$

as required.

We now prove **(3)**. Similarly to **(2)**, let $R = T_k = \textsc{Rect}(\mathbf{I}, \mathbf{c}, \mathbf{d})$, where $\mathbf{I} = \mathbf{J}_{<k} \cup \{\mathbf{j}\}$. For every $s = 0, \ldots, k-1$ one has $\mathbf{c}_{\mathbf{j}_s} = 0$ and $\mathbf{d}_{\mathbf{j}_s} = 1 - \frac{1}{K-s}$. Also let $\mathbf{c}_{\mathbf{j}} = 0$ and $\mathbf{d}_{\mathbf{j}} = 1 - \frac{1}{K-k}$. Let

$$R' := \{x \in R : \mathrm{wt}(x) \pmod W \in [0, 1/(K-k)) \cdot W\},$$

and note that $R' = S_k^{\mathbf{j}}$ by (102). Then by Lemma 102, **(2)**, with $\lambda = K - k$ and

$$\gamma = (\mathbf{d_j} - \mathbf{c_j}) \cdot \prod_{s=0}^{k-1} (\mathbf{d}_{\mathbf{j}_s} - \mathbf{c}_{\mathbf{j}_s}) = \left(1 - \frac{1}{K-k}\right) \prod_{s=0}^{k-1} \left(1 - \frac{1}{K-s}\right) = \left(1 - \frac{1}{K-k}\right)\left(1 - \frac{k}{K}\right)$$

we have

$$\frac{1}{K-k} \cdot (1 - \sqrt{\epsilon}) \left(1 - \frac{1}{K-k}\right)\left(1 - \frac{k}{K}\right) \leq |R'|/m^n \leq \frac{1}{K-k} \cdot (1 + \sqrt{\epsilon}) \left(1 - \frac{1}{K-k}\right)\left(1 - \frac{k}{K}\right).$$

Simplifying, we get

$$(1 - \sqrt{\epsilon}) \left(1 - \frac{1}{K-k}\right) \frac{1}{K} \leq |R'|/m^n \leq (1 + \sqrt{\epsilon}) \left(1 - \frac{1}{K-k}\right) \frac{1}{K},$$

as required.

■

5.6 Interior and exterior of a rectangle

The main difference between our main construction in this section and the toy construction from Section 3 is the fact that vectors in $\mathcal{F}$ are not orthogonal, but merely have small dot products. As a consequence, we generally need to introduce some 'padding' to our construction to obtain the same induced properties as we did in the original construction. For example, note that for the basic Lemma 36 that shows that edge sets $E_{k,j}$ defined in (34) are disjoint for distinct $j \in \mathbf{B}_k$ it was sufficient to ensure that we have introduce a complete bipartite graph between $\text{line}_j(y) \cap S_k^j$ and $\text{line}_j(y) \cap (T_k \setminus T_k^j)$ – the fact that (the downset of) T_k^j is subtracted in the second set was enough to guarantee disjointness. To ensure similar property with nearly orthogonal vectors, however, one must include some 'margin of error' in the construction – this is why the corresponding definition in our main construction (see (109)) uses the interior $\text{Int}_\delta(S_k^{\mathbf{j}})$ as opposed to just $S_k^{\mathbf{j}}$. We define the interior now.

Definition 103 (δ-interior of (a downset of) a rectangle) *For $\mathbf{I} \subseteq \mathcal{F}$, $\mathbf{c}, \mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}}, \mathbf{c} < \mathbf{d}$, the δ-interior $Int_\delta(F)$ of the rectangle $F = \text{RECT}(\mathbf{I}, \mathbf{c}, \mathbf{d})$ is defined as*

$$Int_\delta(F) = \{y \in [m]^n \setminus B : \langle y, \mathbf{i} \rangle \pmod{M} \in [\mathbf{c_i} + \delta, \mathbf{d_i} - \delta) \cdot M \textit{ for all } \mathbf{i} \in \mathbf{I}\},$$

where the set B of boundary points is as in Definition 78. For every $k \in [K/2]$ we define

$$Int_\delta(\text{DOWNSET}_k(F)) = \left\{ y \in Int_\delta(F) : wt(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \right\}.$$

The following simple claim is the rationale behind our definition of the interior of a rectangle:

Lemma 104 (Vertex neighborhood of Int$_\delta(R)$ is contained in R) *If $\epsilon < \delta$, for every rectangle $R \subseteq [m]^n$, $R = (\mathbf{I}, \mathbf{a}, \mathbf{b})$, $\mathbf{a}, \mathbf{b} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}}, \mathbf{a} < \mathbf{b}$, every $\mathbf{r} \in \mathcal{F} \setminus \mathbf{I}$ for every integer λ such that $|\lambda| \leq M/w$, for every $x \in Int_\delta(R)$ one has $x + \lambda\mathbf{r} \in R$.*

Proof: For every $\mathbf{i} \in \mathbf{I}$ one has

$$|\langle x + \lambda \cdot \mathbf{r}, \mathbf{i} \rangle - \langle x, \mathbf{i} \rangle| = |\lambda| \cdot \langle \mathbf{r}, \mathbf{i} \rangle \leq (M/w) \cdot \epsilon \cdot w \leq \epsilon M < \delta M$$

since $\mathbf{r} \in \mathcal{F} \setminus \mathbf{I}$ by assumption of the lemma. Since

$$x \in \text{Int}_\delta(F) = \{y \in [m]^n \setminus B : \langle y, \mathbf{i} \rangle \pmod{M} \in [\mathbf{c_i} + \delta, \mathbf{d_i} - \delta) \cdot M \text{ for all } \mathbf{i} \in \mathbf{I}\}$$

by assumption, we get that

$$x+\lambda\cdot\mathbf{r}\in\{y\in[m]^n:\langle y,\mathbf{i}\rangle\pmod M\in[\mathbf{c_i},\mathbf{d_i})\cdot M\text{ for all }\mathbf{i}\in\mathbf{I}\}=F,$$

as required. Note that the assumption that $x\in\mathrm{Int}_\delta(F)\subseteq[m]^n\setminus B$ is used to ensure that for every $j\in[n]$ one has $0\le(x+\lambda\cdot\mathbf{r})_j<m$, and therefore $x+\lambda\cdot\mathbf{r}\in[m]^n$. Indeed, we have

$$|(x+\lambda\cdot\mathbf{r})_j-x_j|\le|\lambda|\le M/w,$$

and therefore since $n^2\le x_j\le m-n^2$ by assumption that $x\not\in B$, together with the fact that M/w is a constant depending on K (by (p0), (p1) and (p2)) and n is sufficiently large, we get that $0\le(x+\lambda\cdot\mathbf{r})_j<m$. ■

We also define

Definition 105 (δ-exterior of a rectangle) *For $\mathbf{I}\subseteq\mathcal{F}$, $\mathbf{c},\mathbf{d}\in(\Delta\cdot\mathbb{Z}\cap[0,1])^{\mathbf{I}}$, $\mathbf{c}<\mathbf{d}$, the δ-exterior $Ext_\delta(F)$ of the rectangle $F=\textsc{Rect}(\mathbf{I},\mathbf{c},\mathbf{d})$ is defined as follows.*

If $\mathbf{c_i}>\delta$, then

$$Ext_\delta(F)=\{y\in[m]^n:\langle y,\mathbf{i}\rangle\pmod M\in[\mathbf{c_i}-\delta,\mathbf{d_i}+\delta)\cdot M\},$$

and

$$Ext_\delta(F)=\{y\in[m]^n:\langle y,\mathbf{i}\rangle\pmod M\in[0,\mathbf{d_i}+\delta)\cdot M\cup[1-\delta+\mathbf{c_i},1)\cdot M\}$$

otherwise.

The interior (resp. exterior) of a rectangle is quite close to the rectangle itself in terms of size, i.e. there are few points on the boundary (under appropriate conditions):

Lemma 106 *For every $\mathbf{I}\subseteq\mathcal{F}$, $|\mathbf{I}|\le K^2$, for every $\mathbf{c},\mathbf{d}\in(\Delta\cdot\mathbb{Z}\cap[0,1])^{\mathbf{I}}$, $\mathbf{c}<\mathbf{d}$, if $R=\textsc{Rect}(\mathbf{I},\mathbf{c},\mathbf{d})$, one has*

$$|R\setminus Int_\delta(R)|\le\sqrt{\delta}|R|$$

and

$$|Ext_\delta(R)\setminus R|\le\sqrt{\delta}|R|$$

Proof: We start by proving **(1)**. We have

$$\begin{aligned}|R\setminus\mathrm{Int}_\delta(R)|&=|\{x\in R:\langle x,\mathbf{i}\rangle\pmod M\in([\mathbf{c_i},\mathbf{c_i}+\delta)\cup[\mathbf{d_i}-\delta,\mathbf{d_i}))\cdot M\text{ for some }\mathbf{i}\in\mathbf{I}\}|\\&\le\sum_{\mathbf{i}\in\mathbf{I}}|\{x\in R:\langle x,\mathbf{i}\rangle\pmod M\in([\mathbf{c_i},\mathbf{c_i}+\delta)\cup[\mathbf{d_i}-\delta,\mathbf{d_i}))\cdot M\}|\\&\le\sum_{\mathbf{i}\in\mathbf{I}}|R_\mathbf{i}\setminus\mathrm{Int}_\delta(R_\mathbf{i})|,\end{aligned}\tag{115}$$

where we let $R_\mathbf{i}:=\textsc{Rect}(\{\mathbf{i}\},\mathbf{c_i},\mathbf{d_i})$ to simplify notation.

We now fix $\mathbf{i}\in\mathbf{I}$ and upper bound $|R_\mathbf{i}\setminus\mathrm{Int}_\delta(R_\mathbf{i})|$. Let $C\subset[m]^n$ be a minimal $\{\mathbf{i}\}$-subspace cover (see Definition 112). Fix $x\in C$. Recall that

$$\mathrm{line}_\mathbf{i}(x)=\left\{x'\in[m]^n:x'=x+\lambda\cdot\mathbf{i}\text{ for some integer }\lambda\text{ s.t. }\lfloor\langle x',\mathbf{i}\rangle/M\rfloor=\lfloor\langle x,\mathbf{i}\rangle/M\rfloor\right\}.$$

By Claim 92, **(2)** and **(3)**, we have for $x\in C\setminus B$

$$\begin{aligned}|\mathrm{line}_\mathbf{i}(x)\cap(R_\mathbf{i}\setminus\mathrm{Int}_\delta(R_\mathbf{i}))|&=|\{y\in\mathrm{line}_\mathbf{i}(x):\langle y,\mathbf{i}\rangle\pmod M\in[\mathbf{c_i},\mathbf{c_i}+\delta)\cdot M\}|\\&\quad+|\{y\in\mathrm{line}_\mathbf{i}(x):\langle y,\mathbf{i}\rangle\pmod M\in[\mathbf{d_i}-\delta,\mathbf{d_i})\cdot M\}|\\&=2\delta\cdot M/w,\end{aligned}\tag{116}$$

where we used the fact that $\text{line}_{\mathbf{i}}(x) \subset [m]^n$ for all $x \in [m]^n \setminus B$.

Summing over all $x \in C$, we thus get

$$\begin{aligned}
|R_{\mathbf{i}} \setminus \text{Int}_\delta(R_{\mathbf{i}})| &= \sum_{x \in C} |\text{line}_{\mathbf{i}}(x) \cap (R_{\mathbf{i}} \setminus \text{Int}_\delta(R_{\mathbf{i}}))| \\
&= \sum_{x \in C \setminus B} |\text{line}_{\mathbf{i}}(x) \cap (R_{\mathbf{i}} \setminus \text{Int}_\delta(R_{\mathbf{i}}))| + \sum_{x \in B} |\text{line}_{\mathbf{i}}(x) \cap (R_{\mathbf{i}} \setminus \text{Int}_\delta(R_{\mathbf{i}}))| \qquad (117) \\
&\leq 2\delta(M/w) \cdot |C \setminus B| + \sum_{x \in B} |\text{line}_{\mathbf{i}}(x) \cap (R_{\mathbf{i}} \setminus \text{Int}_\delta(R_{\mathbf{i}}))|.
\end{aligned}$$

We now note that since $|\text{line}_{\mathbf{i}}(x)| = M/w$ for every $x \in [m]^n \setminus B$ by Claim 92, **(1)**, we have

$$\begin{aligned}
|C \setminus B| &= (M/w)^{-1} \sum_{x \in C \setminus B} |\text{line}_{\mathbf{i}}(x)| \\
&\leq (M/w)^{-1} \sum_{x \in C} |\text{line}_{\mathbf{i}}(x)| \\
&\leq (M/w)^{-1} m^n.
\end{aligned}$$

Substituting this into (117), we get

$$\begin{aligned}
|R_{\mathbf{i}} \setminus \text{Int}_\delta(R_{\mathbf{i}})| &\leq 2\delta(M/w) \cdot |C \setminus B| + \sum_{x \in B} |\text{line}_{\mathbf{i}}(x) \cap (R_{\mathbf{i}} \setminus \text{Int}_\delta(R_{\mathbf{i}}))| \\
&\leq 2\delta(M/w) \cdot |C \setminus B| + \sum_{x \in B} |\text{line}_{\mathbf{i}}(x)| \\
&\leq 2\delta m^n + (M/w) \cdot \frac{1}{n^{10}} \cdot m^n \\
&\leq 3\delta m^n,
\end{aligned}$$

where the third transition uses the fact that $|\text{line}_{\mathbf{i}}(x)| \leq M/w$ for every $x \in [m]^n \setminus B$ by Claim 92, **(1)**.

Combining the above with (115), we get

$$\begin{aligned}
|R \setminus \text{Int}_\delta(R)| &\leq \sum_{\mathbf{i} \in \mathbf{I}} |R_{\mathbf{i}} \setminus \text{Int}_\delta(R_{\mathbf{i}})| \\
&\leq 3\delta \cdot |\mathbf{I}| \cdot m^n \\
&\leq 3\delta \cdot |\mathbf{I}| \cdot 2\Delta^{-|\mathbf{I}|}|R| \\
&\leq \sqrt{\delta}|R|,
\end{aligned}$$

as required. The third transition use the fact that by Lemma 102, **(1)** one has $(1-\sqrt{\epsilon})\Delta^{|\mathbf{I}|} \leq |R|/m^n \leq (1+\sqrt{\epsilon})\Delta^{|\mathbf{I}|}$ as well as the assumption that ϵ is smaller than an absolute constant (smaller than $1/4$ suffices here). The forth transition uses the assumption that $|\mathbf{I}| \leq K^2$ together with the assumption that $\delta < \Delta^{100K^2}$ by (p5).

The proof of **(2)** is similar and we omit the details. ■

5.7 Subspaces and their properties

We now introduce the notion of subspaces, our main tool in defining the local permutation map Π, and ultimately the map τ glueing together two basic gadgets (see Section 5.10.2 and Section 5.10.3 below). We first introduce

Definition 107 (Block of x with respect to a sequence of vectors J) *For a subset* $\mathbf{J} \subset \mathcal{F}$ *we let* $block_{\mathbf{J}}(x) := (\lfloor \langle x, \mathbf{j} \rangle / M \rfloor)_{\mathbf{j} \in \mathbf{J}}$.

Definition 108 (Subspace of x) *For every subset* $\mathbf{I} \subseteq \mathcal{F}$ *for every* $x \in [m]^n$ *define*

$$\begin{aligned} \mathit{subspace}_{\mathbf{I}}(x) := \Big\{ & x' \in [m]^n : x' = x + \sum_{\mathbf{i} \in \mathbf{I}} t_{\mathbf{i}} \cdot \mathbf{i} \text{ for } t \in \mathbb{Z}^{\mathbf{I}} \\ & \text{s.t. } \mathit{block}_{\mathbf{I}}(x) = \mathit{block}_{\mathbf{I}}(x') \text{ and } ||t||_\infty \leq 2M/w \Big\} . \end{aligned}$$

The more lightweight definition of lines used in Section 5.3 to define the edge set E^ℓ of our basic gadget G in fact coincides with a one-dimensional subspace as per Definition 108, as we show below. This lets us reuse claims about subspaces:

Claim 109 *For every* $\mathbf{j} \in \mathcal{F}$*, then for every* $x \in [m]^n$ *one has* $\mathit{line}_{\mathbf{j}}(x) = \mathit{subspace}_{\{\mathbf{j}\}}(x)$*, where* $\mathit{line}_{\mathbf{j}}(x)$ *is as per Definition 91.*

Proof: We have by Definition 91

$$\text{line}_{\mathbf{j}}(x) = \left\{ x' \in [m]^n : x' = x + \lambda \cdot \mathbf{j} \text{ for some integer } \lambda \text{ s.t. } \lfloor \langle x', \mathbf{j} \rangle / M \rfloor = \lfloor \langle x, \mathbf{j} \rangle / M \rfloor \right\} .$$

and by Definition 108

$$\begin{aligned} \text{subspace}_{\{\mathbf{j}\}}(x) := \Big\{ & x' \in [m]^n : x' = x + \lambda \cdot \mathbf{j} \ \text{ for } \lambda \in \mathbb{Z} \\ & \text{s.t. block}_{\{\mathbf{j}\}}(x) = \text{block}_{\{\mathbf{j}\}}(x') \text{ and } |\lambda| \leq 2M/w \Big\} . \end{aligned}$$

At the same time if $x' = x + \lambda \cdot \mathbf{j}$ for an integer λ, one has

$$\langle x', \mathbf{j} \rangle = \langle x + \lambda \cdot \mathbf{j}, \mathbf{j} \rangle = \langle x, \mathbf{j} \rangle + \lambda \cdot w,$$

so if $|\lambda| > 2M/w$ (for example, when $\lambda > 2M/w$; the other case is similar), one has

$$\text{block}_{\{\mathbf{j}\}}(x') = \lfloor \langle x', \mathbf{j} \rangle / M \rfloor = \lfloor (\langle x, \mathbf{j} \rangle + 2M)/M \rfloor = \lfloor \langle x, \mathbf{j} \rangle / M + 2 \rfloor \geq \lfloor \langle x, \mathbf{j} \rangle / M \rfloor + 1 = \text{block}_{\{\mathbf{j}\}}(x) + 1.$$

Thus, the constraint $|\lambda| \leq 2M/w$ is implied by the constraint $\text{block}_{\{\mathbf{j}\}}(x') = \text{block}_{\{\mathbf{j}\}}(x)$, and thus $\text{line}_{\mathbf{j}}(x) = \text{block}_{\{\mathbf{j}\}}(x)$, as required. ■

Remark 110 *We note that while Claim 109 shows that the* ℓ_∞ *constraint in Definition 108 is redundant when* $|\mathbf{I}| = 1$*, it is not redundant for general* $\mathbf{I}$*, since the vectors in* $\mathcal{F}$ *are only nearly orthogonal.*

We show that subspaces partition $[m]^n$. This fact is key, and lets us define various maps (e.g., the local permutation map Π, see Section 5.10.2), locally on subspaces, and then naturally extend them to the full space.

Lemma 111 (Subspaces form a partition) *For every* $\mathbf{I} \subset \mathcal{F}$*, every* $\epsilon \in (0, 1/(10|\mathbf{I}|))$*, every* $x, x' \in [m]^n$ *one has either* $\mathit{subspace}_{\mathbf{I}}(x) = \mathit{subspace}_{\mathbf{I}}(x')$ *or* $\mathit{subspace}_{\mathbf{I}}(x) \cap \mathit{subspace}_{\mathbf{I}}(x') = \emptyset$.

Proof: Consider an element $y \in \text{subspace}_{\mathbf{I}}(x) \cap \text{subspace}_{\mathbf{I}}(x')$. There exist integer coefficients $(t_{\mathbf{i}})_{\mathbf{i} \in \mathbf{I}}$ and $(t'_{\mathbf{i}})_{\mathbf{i} \in \mathbf{I}}$ such that

$$x + \sum_{\mathbf{i} \in \mathbf{I}} t_{\mathbf{i}} \cdot \mathbf{i} = y = x' + \sum_{\mathbf{i} \in \mathbf{I}} t'_{\mathbf{i}} \cdot \mathbf{i},$$

so that

$$x' - x = \sum_{\mathbf{i}\in\mathbf{I}} (t'_{\mathbf{i}} - t_{\mathbf{i}}) \cdot \mathbf{i}.$$

At the same time for every $z \in \text{subspace}_{\mathbf{I}}(x)$ one has $\text{block}_{\mathbf{I}}(z) = \text{block}_{\mathbf{I}}(x)$, and there exists integer coefficients $(s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}$ such that $z = x + \sum_{\mathbf{i}\in\mathbf{I}} s_{\mathbf{i}} \cdot \mathbf{i}$. Combining this with the equation above, we get

$$z = x + \sum_{\mathbf{i}\in\mathbf{I}} s_{\mathbf{i}} \cdot \mathbf{i} = x' + \sum_{\mathbf{i}\in\mathbf{I}} (s_{\mathbf{i}} + t'_{\mathbf{i}} - t_{\mathbf{i}}) \cdot \mathbf{i}.$$

The existence of $y \in \text{subspace}_{\mathbf{I}}(x) \cap \text{subspace}_{\mathbf{I}}(x')$ also implies that $\text{block}_{\mathbf{I}}(x) = \text{block}_{\mathbf{I}}(y) = \text{block}_{\mathbf{I}}(x')$, and hence $\text{block}_{\mathbf{I}}(z) = \text{block}_{\mathbf{I}}(x) = \text{block}_{\mathbf{I}}(x')$. Thus, in order to show that $z \in \text{subspace}_{\mathbf{I}}(x')$, it suffices to prove that $|s_{\mathbf{i}} + t'_{\mathbf{i}} - t_{\mathbf{i}}| \le 2M/w$ for all $\mathbf{i} \in \mathbf{I}$, i.e. $||s + t' - t||_\infty \le 2M/w$. Suppose not, and let $\mathbf{j} \in \mathbf{I}$ be such that $|s_{\mathbf{j}} + t'_{\mathbf{j}} - t_{\mathbf{j}}| > 2M/w$. Then we have, recalling that $\langle \mathbf{i}, \mathbf{i} \rangle = w$ for all $\mathbf{i} \in \mathcal{F}$ and $\langle \mathbf{i}, \mathbf{i}' \rangle \le \epsilon w$ for $\mathbf{i}, \mathbf{i}' \in \mathcal{F}$, $\mathbf{i} \neq \mathbf{i}'$,

$$\langle z, \mathbf{j} \rangle = \langle x, \mathbf{j} \rangle + (s_{\mathbf{j}} + t'_{\mathbf{j}} - t_{\mathbf{j}}) \cdot w + \sum_{\mathbf{i}\in\mathbf{I}\setminus\{\mathbf{j}\}} (s_{\mathbf{i}} + t'_{\mathbf{i}} - t_{\mathbf{i}}) \cdot \langle \mathbf{i}, \mathbf{j} \rangle,$$

so

$$\begin{aligned} \left| \langle z, \mathbf{j} \rangle - \langle x, \mathbf{j} \rangle - (s_{\mathbf{j}} + t'_{\mathbf{j}} - t_{\mathbf{j}}) \cdot w \right| &\le \epsilon |\mathbf{I}| \cdot ||s + t' - t||_\infty \cdot w \\ &\le \epsilon |\mathbf{I}| (||s||_\infty + ||t'||_\infty + ||t||_\infty) \cdot w \\ &\le 6\epsilon |\mathbf{I}| \cdot M, \end{aligned}$$

where in the last transition we used the fact that $||s||_\infty \le 2M/w$, $||t||_\infty \le 2M/w$ and $||t'||_\infty \le 2M/w$. We thus have, since $\epsilon < 1/(10|\mathbf{I}|)$ by assumption of the lemma,

$$|\langle z, \mathbf{j} \rangle - \langle x, \mathbf{j} \rangle| \ge |s_{\mathbf{j}} + t'_{\mathbf{j}} - t_{\mathbf{j}}| \cdot w - 6\epsilon |\mathbf{I}| \cdot M > (2M/w) \cdot w - 6\epsilon |\mathbf{I}| \cdot M > M.$$

This means that $\lfloor \langle z, \mathbf{j} \rangle / M \rfloor \neq \lfloor \langle x, \mathbf{j} \rangle / M \rfloor$, and hence $\text{block}_{\mathbf{I}}(z) \neq \text{block}_{\mathbf{I}}(x)$, which is a contradiction. We thus get that $||s + t' - t||_\infty \le 2M/w$, and hence $z \in \text{subspace}_{\mathbf{I}}(x')$, as required.

■

Since subspaces partition $[m]^n$, we often select a minimal number of representative points subspaces through which cover the entire space, and define, e.g., the local permutation map Π (see Section 5.10.2), on subspaces through these representative points.

Definition 112 (Minimal I-subspace cover) *We say that a set $C \subset [m]^n$ is a minimal $\mathbf{I}$-subspace cover if*

$$\bigcup_{x\in C} \textit{subspace}_{\mathbf{I}}(x) = [m]^n$$

and $\textit{subspace}_{\mathbf{I}}(x) \cap \textit{subspace}_{\mathbf{I}}(x') = \emptyset$ for $x, x' \in C$, $x \neq x'$.

It follows from Lemma 111 that for every $\mathbf{I} \subseteq \mathcal{F}$ there exists a minimal $\mathbf{I}$-subspace cover C: start with C being the empty set and iteratively add $x \in [m]^n$ to C if $\text{subspace}_{\mathbf{I}}(x) \cap \text{subspace}_{\mathbf{I}}(x') = \emptyset$ for every $x' \in C$.

Lemma 113 (Intersection of a rectangle with a subspace) *For every $\mathbf{I}, \mathbf{J} \subset \mathcal{F}$, $|\mathbf{I}|, |\mathbf{J}| \le K^2$, every $\mathbf{a}, \mathbf{b} \in \Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{J}}$, $\mathbf{a} < \mathbf{b}$, if*

$$\gamma = \prod_{\mathbf{i}\in\mathbf{I}\cap\mathbf{J}} (\mathbf{b}_{\mathbf{i}} - \mathbf{a}_{\mathbf{i}})$$

and

$$R = \textsc{Rect}(\mathbf{J}, \mathbf{a}, \mathbf{b}),$$

the following conditions hold.

(1) *For every $x \in [m]^n \setminus B$ one has*

$$(1-\epsilon^{2/3}) \cdot \gamma \cdot G \leq |\mathit{subspace}_{\mathbf{I}}(x) \cap R| \leq (1+\epsilon^{2/3}) \cdot \gamma \cdot G,$$

where $G = (M/w)^{|\mathbf{I}|}$.

(2) *For every positive integer $\lambda \leq K$ such that $\lambda \mid W/w$, if*

$$R' = \{x \in R : \mathit{wt}(x) \pmod W \in [0, 1/\lambda) \cdot W\},$$

one has for every $x \in [m]^n \setminus B$

$$(1-\epsilon^{2/3}) \cdot \frac{1}{\lambda} \cdot \gamma \cdot G \leq \left|\mathit{subspace}_{\mathbf{I}}(x) \cap R'\right| \leq (1+\epsilon^{2/3}) \cdot \frac{1}{\lambda} \cdot \gamma \cdot G,$$

where $G = (M/w)^{|\mathbf{I}|}$.

5.8 Large matchings in individual gadgets

We prove that the basic gadget $G = (S, T)$ contains a matching of most of S to $T \setminus T_*$:

Lemma 114 *There exists a matching of a $(1 - O(1/K))$ fraction of vertices in S to $T \setminus T_*$.*

Proof: The proof proceeds in two steps. In **step 1** we show that for every $k \in [K/2]$, every $x \in [m]^n \setminus B$ one has

$$\left|\mathrm{line}_{\mathbf{j}}(x) \cap S_k^{\mathbf{j}}\right| = (1 \pm O(1/K)) \left|\mathrm{line}_{\mathbf{j}}(x) \cap (T_k \setminus T_k^{\mathbf{j}})\right|,$$

which in particular implies that a complete bipartite graph between these two sets of vertices contains a matching of required size. In **step 2** we use this fact to conclude the result of the lemma, in particular taking care of the fact that the actual edge set of G^ℓ only contains a complete graph between $\mathrm{line}_{\mathbf{j}}(x) \cap \mathrm{Int}_\delta(S_k^{\mathbf{j}})$ and $\mathrm{line}_{\mathbf{j}}(x) \cap (T_k \setminus T_k^{\mathbf{j}})$.

Step 1: defining the matching on lines. Fix $k \in [K/2]$. Let $\mathbf{j} = \mathbf{J}_k$, and recall that for every $x \in [m]^n$ one has $\mathrm{line}_{\mathbf{j}}(x) = \mathrm{subspace}_{\{\mathbf{j}\}}(x)$ by Claim 109. Let $R = T_k = \textsc{Rect}(\mathbf{J}, \mathbf{c}, \mathbf{d})$, where $\mathbf{J} = \mathbf{J}_{<k}$ and for every $s = 0, \ldots, k-1$ one has $\mathbf{c}_{\mathbf{j}_s} = 0$ and $\mathbf{d}_{\mathbf{j}_s} = 1 - \frac{1}{K-s}$. For every $x \in [m]^n \setminus B$ by Lemma 113, **(1)**, one has

$$(1-\sqrt{\epsilon}) \cdot (M/w) \leq |\mathrm{line}_{\mathbf{j}}(x) \cap T_k| \leq (1+\sqrt{\epsilon}) \cdot (M/w), \tag{118}$$

where $G = M/w$. Note that the error term in the lemma is $\epsilon^{2/3} < \sqrt{\epsilon}$ since $\epsilon \in (0,1)$. Also note that in the application of the lemma we have $\gamma = 1$, since $\mathbf{j} \notin \mathbf{J}_{<k}$.

Now let $R = T_k^{\mathbf{j}} = T_{k+1} = \textsc{Rect}(\mathbf{J}, \mathbf{c}, \mathbf{d})$(since $\mathbf{j} = \mathbf{J}_k$), where $\mathbf{J} = \mathbf{J}_{\leq k}$ and for every $s = 0, \ldots, k$ one has $\mathbf{c}_{\mathbf{j}_s} = 0$ and $\mathbf{d}_{\mathbf{j}_s} = 1 - \frac{1}{K-s}$. For every $x \in [m]^n \setminus B$ by Lemma 113, **(1)**, one has

$$(1-\sqrt{\epsilon}) \cdot \left(1 - \frac{1}{K-k}\right) \cdot (M/w) \leq \left|\mathrm{line}_{\mathbf{j}}(x) \cap T_k^{\mathbf{j}}\right| \leq (1+\sqrt{\epsilon}) \cdot \left(1 - \frac{1}{K-k}\right) \cdot (M/w) \tag{119}$$

Note that in the application of the lemma we have $\gamma = \mathbf{d}_{\mathbf{j}} - \mathbf{c}_{\mathbf{j}} = 1 - \frac{1}{K-k}$, since $\{\mathbf{j}\} \cap \mathbf{J}_{\leq k} = \{\mathbf{j}\}$. Putting (118), (119) together, we get

$$|\mathrm{line}_{\mathbf{j}}(x) \cap (T_k \setminus T_k^{\mathbf{j}})| = (1 + O(K\sqrt{\epsilon})) \cdot \frac{1}{K-k} \cdot (M/w) \tag{120}$$

We now bound $|\text{line}_{\mathbf{j}}(x) \cap S_k^{\mathbf{j}}|$. To that effect let

$$R' := \left\{ x \in R : \text{wt}(x) \pmod{W} \in \left[0, \frac{1}{K-k}\right) \cdot W \right\},$$

and note that $R' = S_k^{\mathbf{j}}$ by (102). For every $x \in [m]^n \setminus B$ by Lemma 113, **(2)**, one has

$$(1-\sqrt{\epsilon})\frac{1}{K-k}\left(1-\frac{1}{K-k}\right)\cdot(M/w) \le |\text{line}_{\mathbf{j}}(x)\cap S_k^{\mathbf{j}}| \le (1+\sqrt{\epsilon})\frac{1}{K-k}\left(1-\frac{1}{K-k}\right)\cdot(M/w). \quad (121)$$

Now recall that by (108) for every $\mathbf{j} \in \mathbf{B}_k$ and every $y \in C_{\mathbf{j}}$ (for a minimal $\mathbf{j}$-line cover $C_{\mathbf{j}}$) the edge set E_k contains all edges in the set

$$(\text{line}_{\mathbf{j}}(x) \cap \text{Int}_\delta(S_k^{\mathbf{j}})) \times (\text{line}_{\mathbf{j}}(x) \cap (T_k \setminus T_k^{\mathbf{j}})). \quad (122)$$

Putting (120) together with (121), using the fact that $O(K\sqrt{\epsilon}) = O(1/K)$ by (p3),(p5) and (p6), and recalling that $0 \le k \le K/2-1$, we get that for every $x \in [m]^n \setminus B$ there exists a matching of a $1-O(1/K)$ fraction of $\text{line}_{\mathbf{j}}(x) \cap S_k^{\mathbf{j}}$ to $\text{line}_{\mathbf{j}}(x) \cap (T_k \setminus T_k^{\mathbf{j}})$ using edges in

$$(\text{line}_{\mathbf{j}}(x) \cap S_k^{\mathbf{j}}) \times (\text{line}_{\mathbf{j}}(x) \cap (T_k \setminus T_k^{\mathbf{j}})).$$

We show in **step 2** below that taking the union of these matchings over $y \in C_{\mathbf{j}}$ and restricting the resulting matching to edges that do not touch $S_k^{\mathbf{j}} \setminus \text{Int}_\delta(S_k^{\mathbf{j}})$ reduces the size of the matching only slightly, and ensures that the matching uses only the edges that are present in the graph, i.e. edges in (122), as required.

Step 2: defining the global matching. Let $C_{\mathbf{j}} \subseteq [m]^n$ denote a minimal $\mathbf{j}$-line cover (one can think of this cover as the one used to defined the corresponding edge set of G; however, one notes that the actual edge set does not depend on the specific choice of a cover). In **step 1** we showed the existence of a matching of a $1-O(1/K)$ fraction of $\text{line}_{\mathbf{j}}(x) \cap S_k^{\mathbf{j}}$ to $\text{line}_{\mathbf{j}}(x) \cap (T_k \setminus T_k^{\mathbf{j}})$ for every $k \in [K/2]$ and every $x \in [m]^n \setminus B$ using edges in (122).

We now note that for every $k \in [K/2]$

$$\begin{aligned}\left| S_k \setminus \bigcup_{x \in C \cap B} (\text{line}_{\mathbf{j}}(x) \cap S_k^{\mathbf{j}}) \right| &\le \left| S_k^{\mathbf{j}} \setminus \bigcup_{x \in C \cap B} (\text{line}_{\mathbf{j}}(x) \cap S_k^{\mathbf{j}}) \right| + |S_k \setminus S_k^{\mathbf{j}}| \\ &\le |B| \cdot (M/w) + |S_k \setminus S_k^{\mathbf{j}}|,\end{aligned} \quad (123)$$

where we used the fact that $|\text{line}_{\mathbf{j}}(x)| \le M/w$ by Claim 92, **(1)**, for all $x \in [m]^n$ and all $\mathbf{j} \in \mathcal{F}$.

We now bound the second term in (123). By Lemma 85, **(2)** and Lemma 85, **(3)**, one has

$$|S_k|/m^n = (1 \pm \sqrt{\epsilon}) \cdot |T_0|/K$$

and

$$|S_k^{\mathbf{j}}|/m^n = (1 \pm \sqrt{\epsilon})\left(1 - \frac{1}{K-k}\right) \cdot |T_0|/K.$$

This means that the second term in (123) is upper bounded by

$$\frac{1}{K}\left(2\sqrt{\epsilon} + \frac{1}{K-k}\right)|T_0| = O(1/K^2) \cdot |T_0|,$$

where we used the fact that

$$\begin{aligned}
\sqrt{\epsilon} &\leq \delta && \text{(by (p6))}\\
&\leq \Delta^{100K^2} && \text{(by (p5))}\\
&\leq K^{-100K^2} && \text{(by (p3))}\\
&\leq K^{-4}.
\end{aligned}$$

We now bound the first term in (123) by noting that by Claim 79

$$|B| \cdot (M/w) \leq n^{-9} \cdot m^n = O(1/K^2)|T_0| = O(1/K)|S_k|$$

for every $k \in [K/2]$.

Putting the above bounds together, we get that for every $k \in [K/2]$ there exists a matching of all but a $O(1/K)$ fraction of S_k to $T_k \setminus T_k^{\mathbf{j}}$, where $\mathbf{j} = \mathbf{J}_k$, using edges in (122). It remains to remove from this matching edges incident on vertices in $S_k^{\mathbf{j}} \setminus \text{Int}_\delta(S_k^{\mathbf{j}})$. The matching is reduced by at most

$$\begin{aligned}
|S_k^{\mathbf{j}} \setminus \text{Int}_\delta(S_k^{\mathbf{j}})| &\leq |T_k^{\mathbf{j}} \setminus \text{Int}_\delta(T_k^{\mathbf{j}})|\\
&\leq \sqrt{\delta}|T_k^{\mathbf{j}}|\\
&\leq 2K\sqrt{\delta}|S_k^{\mathbf{j}}|\\
&= O(1/K)|S_k^{\mathbf{j}}|.
\end{aligned}$$

The first transition above is by definition of $S_k^{\mathbf{j}}$ and S_k (see 102 and 101). The second transition is by Lemma 106. The third transition is due to the fact that by Lemma 85, **(3)** and **(4)**, one has $|S_k^{\mathbf{j}}| \geq (1/K)|T_k^{\mathbf{j}}|$. The forth transition is by (p3) and (p5).

In other words, for every $k \in [K/2]$ there exists a matching of all but $O(1/K)$ fraction of S_k to $T_k \setminus T_{k+1}$. Since the sets T_k form a nested sequence, the sets $T_k \setminus T_{k+1}$ are disjoint, similarly to the sets S_k. Thus, the matchings extend to a matching of a $1 - O(1/K)$ fraction of

$$S = S_0 \uplus S_1 \uplus \ldots \uplus S_{K/2-1}$$

to

$$\bigcup_{k \in [K/2]} T_k \setminus T_{k+1} = T_0 \setminus T_{K/2} = T \setminus T_*.$$

Since $\sum_{k \in [K/2]} |S_k| = \frac{1}{2}(1 + O(1/K)) \cdot |T_0| = (1 + O(1/K))|T \setminus T_*|$ by Lemma 85, **(1)** and **(2)** together with the choice of ϵ (as per (p3), (p5) and (p6)), the result of the lemma follows. ■

5.9 $1 - e^{-1}$ hardness using basic gadgets

We show how the $1 - e^{-1}$ hardness from [Kap13] follows using our basic gadgets in Appendix D.

5.10 Maps τ^ℓ identifying the basic gadgets

The main result of this section is the definition of maps

$$\tau^\ell : S^\ell \to T_*^{\ell-1}$$

mapping the S side of the bipartition (the 'arriving vertices') of the ℓ-th gadget G^ℓ to the terminal subcube $T_*^{\ell-1}$ of the previous gadget $G^{\ell-1}$.

Fix $\ell \in [L], \ell > 0$. To simplify notation, let $\mathbf{B} = \mathbf{B}^{\ell-1}, \mathbf{B}' = \mathbf{B}^{\ell}$, and recall that both sets are partitioned into $K/2$ disjoint equal size sets

$$\begin{aligned}\mathbf{B} &= \mathbf{B}_0 \cup \mathbf{B}_1 \cup \ldots \cup \mathbf{B}_{K/2}\\ \mathbf{B}' &= \mathbf{B}'_0 \cup \mathbf{B}'_1 \cup \ldots \mathbf{B}'_{K/2}.\end{aligned}$$

Let $G = (S, T, E) = G^{\ell-1}, G' = (S', T', E') = G^{\ell}$. Let $\mathbf{J} = \mathbf{J}^{\ell-1}$, $\mathbf{J}' = \mathbf{J}^{\ell}$, $\mathbf{r} = \mathbf{r}^{\ell-1}, \mathbf{r}' = \mathbf{r}^{\ell}$, and recall that

$$\begin{aligned}\mathbf{J} &\in \mathbf{B}_0 \times \mathbf{B}_1 \times \ldots \times \mathbf{B}_{K/2}\\ \mathbf{J}' &\in \mathbf{B}'_0 \times \mathbf{B}'_1 \times \ldots \times \mathbf{B}'_{K/2}.\end{aligned}$$

With this notation in place, we will define the map

$$\tau : S' \to T^* \cup \{\perp\},$$

where for a vertex $x \in S'$ we write $\tau(x) = \perp$ to denote the fact that τ is not defined on x. Thus, in essence τ is a partial map. We later use τ to identify basic gadgets $G^{\ell}, \ell \in [L]$, arriving in the stream. We start by defining an auxiliary map ρ that we refer to as the *densifying map* (see Section 5.10.1 below). The map ρ maps a subsampled rectangle such as a set $S_k, k \in [K/2]$, to a regular rectangle. The map τ is then defined by composing ρ with another auxiliary transformation that we refer to as the *local permutation map* defined in Section 5.10.2. The map τ is then defined in Section 5.10.3.

5.10.1 Densifying map ρ

The densifying map is defined as follows:

Definition 115 ($(\alpha, \mathbf{r})$-densifying map) *For a positive integer α and $\mathbf{r} \in \mathcal{F}$ the $(\alpha, \mathbf{r})$-densifying map $\rho : [m]^n \setminus B \to [m]^n$ is defined as follows. For $x \in [m]^n$ and $\mathbf{r} \in \mathcal{F}$ we first let*

$$\langle x, \mathbf{r}\rangle \pmod M = aW + b(W/\alpha) + c,$$

where $a \in [M/W]$, $b \in [\alpha]$ and $c \in [W/\alpha]$. Then define

$$\rho(x) := x - \mathbf{r} \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right).$$

We note that the map ρ is well defined since for every $i \in [n]$ one has $(\rho(x))_i \le x_i < m$ and

$$\begin{aligned}(\rho(x))_i &= x_i - \mathbf{r}_i \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right)\\ &\ge x_i - \left(\frac{W}{w}(1 - 1/\alpha) \cdot (M/W - 1) + \frac{W}{\alpha w}(\alpha - 1)\right)\\ &= x_i - \left(\frac{W}{w}(1 - 1/\alpha) \cdot (M/W - 1) + \frac{W}{w}(1 - 1/\alpha)\right)\\ &= x_i - \left(\frac{W}{w} \cdot (M/W - 1) + \frac{W}{w}\right)(1 - 1/\alpha)\\ &= x_i - \frac{M}{w}(1 - 1/\alpha)\\ &\ge 0\end{aligned}$$

for all $x \in [m]^n \setminus B$ since n is sufficiently large as a function of M/w, W/w, K, Δ, δ, and L, and in particular $n > M/w$.

The next lemma summarizes the relevant properties of the map ρ:

Lemma 116 (Densification of a subsampled set) *For every integer $\alpha \geq 2$, every $\mathbf{r} \in \mathcal{F}$, every rectangle $U \subseteq [m]^n$, $U = (\mathbf{I}, \mathbf{a}, \mathbf{b})$, $\mathbf{a}, \mathbf{b} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}}, \mathbf{a} < \mathbf{b}$, such that $\mathbf{r} \notin \mathbf{I}$, the following conditions hold for the $(\alpha, \mathbf{r})$-densifying map ρ (see Definition 115):*

(1) *ρ is injective;*

(2) *ρ maps*

$$\{x \in \mathit{Int}_\delta(U) : \mathit{wt}(x) \in [0, 1/\alpha) \cdot W \pmod W\}$$

to

$$\{x \in U : \langle x, \mathbf{r}\rangle \pmod M \in [0, 1/\alpha) \cdot M\}$$

(3) *for every $x \in [m]^n$ one has $\rho(x) = x + \lambda \cdot \mathbf{r}$ for an integer λ satisfying $|\lambda| \leq M/w$.*

Proof: We start by proving the **(3)**. One has by Definition 115 $\rho(x) = x + \lambda \cdot \mathbf{r}$, where $\lambda = -\left(\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right)$ for $a \in [M/W]$ and $b \in [\alpha]$. We thus have

$$\begin{aligned}
|\lambda| &= \left|\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right| \\
&\leq \left|\frac{W}{w}(1 - 1/\alpha) \cdot (M/W - 1) + \frac{W}{\alpha w}(\alpha - 1)\right| \\
&\leq \left|\frac{W}{w}(1 - 1/\alpha) \cdot (M/W - 1) + \frac{W}{w} \cdot (1 - 1/\alpha)\right| \\
&\leq \left|(1 - 1/\alpha)\left(\frac{W}{w} \cdot (M/W - 1) + \frac{W}{w}\right)\right| \\
&\leq |(1 - 1/\alpha) \cdot M/w| \\
&\leq M/w
\end{aligned}$$

as required.

We now prove **(2)**. By Definition 115 one has, letting

$$\langle x, \mathbf{r}\rangle \pmod M = aW + b(W/\alpha) + c,$$

where $a \in [M/W]$, $b \in [\alpha]$ and $c \in [W/\alpha]$,

$$\rho(x) := x - \mathbf{r} \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right). \tag{124}$$

We have by (124),

$$\begin{aligned}
\langle \rho(x), \mathbf{r}\rangle \pmod M &= \left[\langle x, \mathbf{r}\rangle \pmod M - \langle \mathbf{r}, \mathbf{r}\rangle \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right)\right] \pmod M \\
&= \left[(aW + b(W/\alpha) + c) - \langle \mathbf{r}, \mathbf{r}\rangle \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right)\right] \pmod M \\
&= \left[(aW + b(W/\alpha) + c) - W(1 - 1/\alpha) \cdot a - \frac{W}{\alpha} b\right] \pmod M \\
&= (W/\alpha)a + c \in [M/\alpha],
\end{aligned} \tag{125}$$

as required. In the last transition we used the fact that $a \in [M/W]$ and $c \in [W/\alpha]$ by definition of a and b.

We now argue injectivity, i.e., prove **(1)**. Suppose that $\rho(x) = \rho(y)$ for some $y \neq x$. Specifically, let

$$\begin{aligned}\langle x, \mathbf{r}\rangle \pmod{M} &= aW + b(W/\alpha) + c\\ \langle y, \mathbf{r}\rangle \pmod{M} &= a'W + b'(W/\alpha) + c'\end{aligned}$$

with $a, a' \in [M/W]$, $b, b' \in [\alpha]$ and $c, c' \in [W/\alpha]$. Then $\rho(x) = \rho(y)$ means that

$$x - \mathbf{r} \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right) = y - \mathbf{r} \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a' + \frac{W}{\alpha w} b'\right). \tag{126}$$

First note that that by (125)

$$\left\langle x - \mathbf{r} \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a + \frac{W}{\alpha w} b\right), \mathbf{r}\right\rangle \pmod{M} = a(W/\alpha) + c$$

and similarly

$$\left\langle y - \mathbf{r} \cdot \left(\frac{W}{w}(1 - 1/\alpha) \cdot a' + \frac{W}{\alpha w} b'\right), \mathbf{r}\right\rangle \pmod{M} = a'(W/\alpha) + c'.$$

Combining the two equations above with (126), we get $a = a'$ and $c = c'$, and it remains to show that $b = b'$. To that effect recall that

$$\begin{aligned}\text{wt}(x) &= \sum_{i \in [n]} x_i \in [0, 1/\alpha) \cdot W \pmod{W}\\ \text{wt}(y) &= \sum_{i \in [n]} y_i \in [0, 1/\alpha) \cdot W \pmod{W}.\end{aligned}$$

Applying the wt$(\cdot)$ function to both sides of (126), using the fact that $|\mathbf{r}| = w$ and rearranging terms, we get

$$\begin{aligned}\text{wt}(x) - \text{wt}(y) &= \left(W(1 - 1/\alpha) \cdot a + \frac{W}{\alpha} b\right) - \left(W(1 - 1/\alpha) \cdot a' + \frac{W}{\alpha} b'\right)\\ &= \frac{W}{\alpha}(b - b'),\end{aligned} \tag{127}$$

where in the last transition we used the fact that $a = a'$, as established above. Now recalling that wt$(x) \pmod{W} \in [0, 1/\alpha) \cdot W$ and wt$(y) \pmod{W} \in [0, 1/\alpha) \cdot W$ by assumption, we get that

$$(\text{wt}(x) \pmod{W}) - (\text{wt}(y) \pmod{W}) \in (-1/\alpha, 1/\alpha) \cdot W,$$

and hence $b = b'$, which implies that $x = y$. This establishes injectivity of ρ, proving **(1)**.

We now prove **(2)**. For every $x \in \text{Int}_\delta(U)$ we have by (124) that $\rho(x) := x - \lambda \cdot \mathbf{r}$, where λ is an integer satisfying $|\lambda| \leq M/w$, as established above. We thus have $\rho(x) \in U$ by Lemma 104. ■

5.10.2 Local permutation map Π

We now define our local permutation map Π.

Definition 117 (Local permutation map Π) *For two cubes $R = (\mathbf{I}, \mathbf{a})$, $R' = (\mathbf{I}', \mathbf{a}')$ such that $\mathbf{I}, \mathbf{I}' \subset \mathcal{F}$, $\mathbf{I} \cap \mathbf{I}' = \emptyset$, the (partial) map*

$$\Pi_{R' \to R} : [m]^n \to [m]^n$$

is defined as follows. Let $C \subseteq [m]^n$ denote a minimal $\mathbf{I} \cup \mathbf{I}'$-subspace cover (Definition (112)*).*

For every $x \in C$ we define the mapping as follows. Let

$$s = |\mathit{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R|$$
$$s' = |\mathit{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R'|.$$

Define $\Pi_{R' \to R}$ on subspace$_{\mathbf{I} \cup \mathbf{I}'}(x)$ as an arbitrary bijective mapping from a subset of subspace$_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R'$ of size $\min\{s, s'\}$ to a subset of subspace$_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R$ of size $\min\{s, s'\}$.

Remark 118 *We show later (see Lemma 120 below) that s is quite close to s' for $x \in C \setminus B$. Thus the map Π is defined on almost all of $|\mathit{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R|$ and almost all of $|\mathit{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R'|$ for most choices of $x \in C$.*

The next lemma shows that the permutation map $\Pi_{R' \to R}$ performs sparse bounded shifts, i.e. that $\Pi_{R' \to R}(x)$ can be expresses as the sum of x with a small number of vectors in $\mathcal{F}$, each with rather small coefficients:

Lemma 119 (Local permutation map performs sparse bounded shifts) *For two cubes $R = (\mathbf{I}, \mathbf{a})$, $R' = (\mathbf{I}', \mathbf{a}')$, $\mathbf{a} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}}, \mathbf{a}' \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'}$, such that $\mathbf{I}, \mathbf{I}' \subset \mathcal{F}$, $\mathbf{I} \cap \mathbf{I}' = \emptyset$, the following is true for the (partial) map*

$$\Pi_{R' \to R} : [m]^n \to [m]^n.$$

For every $z \in [m]^n$ such that $\Pi := \Pi_{R' \to R}$ is defined on z one has $\Pi(z) = z + \sum_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'} t_{\mathbf{i}} \cdot \mathbf{i}$ with $||t||_\infty \leq 4M/w$.

Proof: This follows by Definition 108 and Definition 117. Indeed, recall that for a minimal $\mathbf{I} \cup \mathbf{I}'$-subspace cover C and $x \in C$ the map Π maps points $a \in \text{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R'$ to points $b \in \text{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R$. By definition of subspace$_{\mathbf{I} \cup \mathbf{I}'}(x)$ (Definition 108) there exist coefficients $\{t^a_{\mathbf{i}}\}_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'}$ and $\{t^b_{\mathbf{i}}\}_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'}$ such that

$$a = x + \sum_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'} t^a_{\mathbf{i}} \cdot \mathbf{i} \quad \text{and} \quad b = x + \sum_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'} t^b_{\mathbf{i}} \cdot \mathbf{i}$$

with $||t^a||_\infty \leq 2M/w$ and $||t^b||_\infty \leq 2M/w$. Putting the above bounds together, we get

$$b = a + \sum_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'} (t^b_{\mathbf{i}} - t^a_{\mathbf{i}}) \cdot \mathbf{i}$$

with $||t^b - t^a||_\infty \leq 4M/w$ for every $b \in \text{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R$, as required. ■

While $\Pi_{R' \to R}$ is defined with respect to two cubes R' and R, we often need to know where Π maps an extended rectangle, namely a rectangle that beyond constraints imposed by R' has further constraints – see R'_{ext} below. We show that if the additional constraints inherent in R'_{ext} are nearly orthogonal (which they are since all our vectors come from the family $\mathcal{F}$), then at least the interior of an extended rectangle R'_{ext} is mapped to an appropriate extended rectangle R_{ext}:

Lemma 120 (Action of permutation map on extended rectangles) *For every pair of cubes $R = (\mathbf{I}, \mathbf{a})$, $R' = (\mathbf{I}', \mathbf{a}')$, $\mathbf{a} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}}, \mathbf{a}' \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'}$, such that $\mathbf{I}, \mathbf{I}' \subset \mathcal{F}$, $|\mathbf{I}| = |\mathbf{I}'|$, $\mathbf{I} \cap \mathbf{I}' = \emptyset$, $|\mathbf{I} \cup \mathbf{I}'| \leq K^2$, if $\epsilon < \delta/(4|\mathbf{I} \cup \mathbf{I}'|)$, the following conditions hold for the corresponding (partial) map $\Pi := \Pi_{R' \to R} : [m]^n \setminus B \to [m]^n$ (see Definition 117).*

For every $\mathbf{J} \subset \mathcal{F} \setminus (\mathbf{I} \cup \mathbf{I}')$ and every $\mathbf{c}, \mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{J}}, \mathbf{c} < \mathbf{d}$, if

$$R_{ext} = (\mathbf{I} \cup \mathbf{J}, (\mathbf{a}, \mathbf{c}), (\mathbf{a} + \Delta \cdot \mathbf{1}, \mathbf{d})) \text{ and } R'_{ext} = (\mathbf{I}' \cup \mathbf{J}, (\mathbf{a}', \mathbf{c}), (\mathbf{a}' + \Delta \cdot \mathbf{1}, \mathbf{d})),$$

then

(1) Π *maps the interior of* R'_{ext} *to* R_{ext}*, i.e.*

$$\Pi(\mathit{Int}_\delta(R'_{ext})) \subseteq R_{ext}.$$

(2) *the number of points in* R' *that* Π *is not defined on is bounded by* $8\sqrt{\epsilon}|R'|$.

Proof: We start by proving **(1)**. Pick $x \in \text{Int}_\delta(R'_{ext})$ such that $\Pi(x)$ is defined. We need to verify that **(a)** for every $\mathbf{i} \in \mathbf{I}$ one has $\langle \Pi(x), \mathbf{i}\rangle \pmod M \in [\mathbf{a_i}, \mathbf{a_i} + \Delta \cdot \mathbf{1}) \cdot M$ and **(b)** for every $\mathbf{k} \in \mathbf{J}$ one has $\langle \Pi(x), \mathbf{k}\rangle \pmod M \in [\mathbf{c_k}, \mathbf{d_k}) \cdot M$.

Condition **(a)** is satisfied by construction of Π since Π maps points in $R' = (\mathbf{I}, \mathbf{a}')$ to points in $R = (\mathbf{I}, \mathbf{a})$ and $R'_{ext} \subseteq R'$. We now establish **(b)**. By Lemma 119 one has $\Pi(x) = x + \sum_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'} t_\mathbf{i} \cdot \mathbf{i}$, where $||t||_\infty \leq 4M/w$. We thus have that for every $\mathbf{k} \in \mathbf{J}$

$$|\langle \Pi(x), \mathbf{k}\rangle - \langle x, \mathbf{k}\rangle| \leq \left|\sum_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'} t_\mathbf{i} \cdot \langle \mathbf{i}, \mathbf{k}\rangle\right| \leq 4\epsilon|\mathbf{I} \cup \mathbf{I}'| \cdot M < \delta M, \tag{128}$$

where we used the fact that $\langle \mathbf{i}, \mathbf{k}\rangle \leq \epsilon w$ for all $\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'$ as $\mathbf{J} \subset \mathcal{F} \setminus (\mathbf{I} \cup \mathbf{I}')$ by assumption, as well as the fact that

$$\begin{aligned} \epsilon &< \delta^2 && \text{(by (p6))} \\ &\leq \delta \cdot \Delta^{200K^2} && \text{(by (p5))} \\ &\leq \delta \cdot K^{-200K^2} && \text{(by (p3))} \\ &\leq \delta/(4|\mathbf{I} \cup \mathbf{I}'), \end{aligned}$$

where the last transition is due to the fact that $|\mathbf{I} \cup \mathbf{I}'| \leq K^2$ by assumption, and K is larger than an absolute constant. Since $x \in \text{Int}_\delta(R_{ext})$ by assumption, we have

$$\langle x, \mathbf{k}\rangle \pmod M \in [\mathbf{c_k} + \delta, \mathbf{d_k} - \delta) \cdot M$$

for every $\mathbf{k} \in \mathbf{J}$. Putting this together with (128) gives

$$\langle \Pi(x), \mathbf{k}\rangle \pmod M \in [\mathbf{c_k}, \mathbf{d_k}) \cdot M,$$

as required.

We now prove **(2)**. Let $C \subseteq [m]^n$ be the minimal $\mathbf{I} \cup \mathbf{I}'$-subspace cover used in the definition of Π. Recall that for every $x \in C \setminus B$ one has by Lemma 159, **(1)**,

$$(1 - \sqrt{\epsilon})\Delta^{|\mathbf{I}|} \cdot G \leq |\text{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R| \leq (1 + \sqrt{\epsilon})\Delta^{|\mathbf{I}|} \cdot G,$$

where $G = (M/w)^{|\mathbf{I}|}$. Similarly, one has

$$(1 - \sqrt{\epsilon})\Delta^{|\mathbf{I}'|} \cdot G \leq \left|\text{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R'\right| \leq (1 + \sqrt{\epsilon})\Delta^{|\mathbf{I}'|} \cdot G,$$

since $|\mathbf{I}| = |\mathbf{I}'|$. We thus get for every $x \in [m]^n \setminus B$, letting $s = |\text{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R|$ and $s' = |\text{subspace}_{\mathbf{I} \cup \mathbf{I}'}(x) \cap R'|$,

$$\max\{s, s'\} - \min\{s, s'\} \leq 4\sqrt{\epsilon} \cdot s'$$

as long as ϵ is smaller than a constant. Thus, the number of points in subspace$_{\mathbf{I}\cup\mathbf{I}'}(x)\cap R'$ that Π is not defined on is bounded by $4\sqrt{\epsilon}|\text{subspace}_{\mathbf{I}\cup\mathbf{I}'}(x)\cap R'|$. The number of points that Π is not defined on is bounded by

$$\begin{aligned}
&4\sqrt{\epsilon}\cdot\sum_{x\in C\setminus B}|\text{subspace}_{\mathbf{I}\cup\mathbf{I}'}(x)\cap R'|+|B|\cdot(5M/w)^{|\mathbf{I}\cup\mathbf{I}'|}\\
&\leq 4\sqrt{\epsilon}\cdot\sum_{x\in C\setminus B}|\text{subspace}_{\mathbf{I}\cup\mathbf{I}'}(x)\cap R'|+\frac{1}{n}|R'|\cdot(5M/w)^{|\mathbf{I}\cup\mathbf{I}'|}\\
&\leq 8\sqrt{\epsilon}\cdot\sum_{x\in C}|\text{subspace}_{\mathbf{I}\cup\mathbf{I}'}(x)\cap R'|\\
&=8\sqrt{\epsilon}\cdot|R'|,
\end{aligned}$$

where the first transition uses the fact that for every $x\in[m]^n$ one has $|\text{subspace}_{\mathbf{I}\cup\mathbf{I}'}(x)|\leq(5M/w)^{|\mathbf{I}\cup\mathbf{I}'|}$ (since coordinates of t are bounded by $2M/w$ in absolute value in Definition 108) and the second transition uses the fact that $|R'|\geq\Delta^{|\mathbf{I}\cup\mathbf{I}'|}\geq\Delta^{K^2}$, and the third transition uses the assumption that n is sufficiently large as a function of $M/w, W/w, K, L, \Delta, \delta$. ■

5.10.3 Defining the glueing map τ

We define the glueing map τ in this section. To do that, first for every $k\in[K/2]$ we define a map

$$\tau_k:S'_k\to T_*\cup\{\perp\},$$

where for a vertex $x\in S'_k$ we write $\tau(x)=\perp$ to denote the fact that τ is not defined on x. Thus, in essence τ is a partial map. We ensure that

1. τ_k is injective on elements of S'_k that it does not map to $\perp$, i.e., if $\tau_k(x)\neq\perp$ and $\tau_k(y)\neq\perp$, then $\tau_k(x)\neq\tau_k(y)$ for $x\neq y$.
2. the images of τ_k are disjoint for different k, i.e. these maps extend naturally to an injective partial map from the union of S'_k over all $k\in[K/2]$ to T_* that is defined on almost all of S'.

Then the map τ is defined as mapping an element in $x\in S_k$ to $\tau_k(x)$ for every $k\in[K/2]$.

The map τ_k is parameterized by the compression vector $\mathbf{r}\in\mathbf{B}_{K/2},\mathbf{r}\notin\mathbf{J}_k$, for the terminal subcube T_*, as well as the extension and compression vectors for every $k\in[K/2]$ (see Definition 81) Ext$_k\subseteq\mathbf{B}'_k$ and $\mathbf{q}_k\in\mathbf{B}'_k$. Define sets

$$\mathbf{I}=\mathbf{J}\cup\{\mathbf{r}\}\subset\mathcal{F}\tag{129}$$

and

$$\mathbf{I}'_k=\mathbf{J}'_{<k}\cup\text{Ext}_k\cup\{\mathbf{q}_k\}\subset\mathcal{F}\tag{130}$$

We sometimes write $\mathbf{I}'$ when k is fixed and clear from context. Let ρ_k be the $(K-k,\mathbf{q}_k)$-densifying map as per Definition 115. By Lemma 116 we have

$$\rho_k(\text{Int}_\delta(S'_k))\subseteq\left\{x\in T'_k:\langle x,\mathbf{q}_k\rangle\pmod M\in\left[0,\frac{1}{K-k}\right)\cdot M\right\},\tag{131}$$

Indeed, we invoke the lemma with $U=T'_k$, since $S'_k=\textsc{DownSet}_k(T'_k)$ so that

$$\begin{aligned}
\text{Int}_\delta(S'_k)&=\textsc{DownSet}_k(\text{Int}_\delta(T'_k))\\
&=\left\{x\in\text{Int}_\delta(T'_k):\text{wt}(x)\in\left[0,\frac{1}{K-k}\right)\cdot W\pmod W\right\},
\end{aligned}$$

by definition of a δ-interior (see Definition 103). Recall that T'_k is indeed a rectangle, as required by Lemma 116, since $T'_k = \textsc{Rect}(\mathbf{J}'_{<k}, \mathbf{c}, \mathbf{d})$ with $\mathbf{c}_{\mathbf{j}'_s} = 0$, $\mathbf{d}_{\mathbf{j}'_s} = 1 - \frac{1}{K-s}$ for all $s \in [k]$. Note that the preconditions of Lemma 116 are satisfied since T'_k is indeed a rectangle (see (100)) and $\mathbf{q}_k \notin \mathbf{J}'_{<k}$ (note that $\Delta \mid \frac{1}{K-s}$ for all $s \in [k]$ by (p3), so rectangle boundaries are indeed in $\Delta \cdot \mathbb{Z} \cap [0,1]$, as required by Lemma 116).

Definition 121 *For $k \in [K/2]$ let $\mathbb{D}_k \subseteq (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}'_k}$ be such that*

$$\left\{x \in T'_k : \langle x, \mathbf{q}_k \rangle \pmod{M} \in \left[0, \frac{1}{K-k}\right) \cdot M\right\} = \bigcup_{\mathbf{d} \in \mathbb{D}_k} \textsc{Rect}(\mathbf{I}'_k, \mathbf{d}).$$

Note that such a set $\mathbb{D}_k$ exists since T'_k is a rectangle in $\mathbf{I}'_k$. Indeed, let $\mathbf{c}_{\mathbf{j}'_s} = 0, \mathbf{d}_{\mathbf{j}'_s} = 1 - \frac{1}{K-s}$ for $s \in [k]$, let $\mathbf{c}_{\mathbf{q}_k} = 0, \mathbf{d}_{\mathbf{q}_k} = \frac{1}{K-k}$, and $\mathbf{c}_\mathbf{i} = 0, \mathbf{d}_\mathbf{i} = 1$ for $\mathbf{i} \in \mathrm{Ext}_k$. Then

$$\left\{x \in T'_k : \langle x, \mathbf{q}_k \rangle \pmod{M} \in \left[0, \frac{1}{K-k}\right) \cdot M\right\} = \textsc{Rect}(\mathbf{I}'_k, \mathbf{c}, \mathbf{d}),$$

and by Claim 101, we get that the set $\mathbb{D}_k$ from Definition 121 exists and satisfies

$$\mathbb{D}_k = (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}'_k} \cap \prod_{\mathbf{i} \in \mathbf{I}'_k} [\mathbf{c}_\mathbf{i}, \mathbf{d}_\mathbf{i}). \tag{132}$$

Combining the definition above with (131), we get

$$\rho_k(\mathrm{Int}_\delta(S'_k)) \subseteq \bigcup_{\mathbf{d} \in \mathbb{D}_k} \textsc{Rect}(\mathbf{I}'_k, \mathbf{d}). \tag{133}$$

Similarly let $\mathbb{A} \subseteq \Delta \cdot \mathbb{Z} \cap [0,1]^\mathbf{I}$ be such that

$$T_* = \bigcup_{\mathbf{a} \in \mathbb{A}} \textsc{Rect}(\mathbf{I}, \mathbf{a}). \tag{134}$$

Note that such $\mathbb{A}$ exists by Claim 101 since T^*_k is a rectangle in $\mathbf{I}$. The latter holds because $\mathbf{J} \subseteq \mathbf{I}$, $T^*_k = \textsc{Rect}(\mathbf{J}, \mathbf{c}, \mathbf{d})$ with $\mathbf{c}_{\mathbf{j}_s} = 0$, $\mathbf{d}_{\mathbf{j}_s} = 1 - \frac{1}{K-s}$ for all $s \in [K/2]$, and $\Delta \mid \frac{1}{K-s}$ for all $s \in [K/2]$. Now let

$$\mathsf{M} : \bigcup_{k \in [K/2]} \mathbb{D}_k \to \mathbb{A}. \tag{135}$$

be a bijective map. Such a map exists since $\left|\sum_{k \in [K/2]} \mathbb{D}_k\right| = \sum_{k \in [K/2]} |\mathbb{D}_k| = |\mathbb{A}|$. Indeed, by Definition 121 one has for every $k \in [K/2]$

$$|\mathbb{D}_k| = \frac{1}{\Delta^{|\mathbf{I}'_k|}} \cdot \frac{1}{K-k} \cdot \prod_{s=0}^{k-1} \left(1 - \frac{1}{K-s}\right) = \frac{1}{\Delta^{|\mathbf{I}'_k|}} \cdot \frac{1}{K}$$

and by (134) one has

$$|\mathbb{A}| = \frac{1}{\Delta^{|\mathbf{I}|}} \cdot \prod_{s=0}^{K/2} \left(1 - \frac{1}{K-s}\right) = \frac{1}{\Delta^{|\mathbf{I}|}} \cdot \frac{1}{2},$$

and therefore

$$\sum_{k \in [K/2]} |\mathbb{D}_k| = \frac{1}{\Delta^{|\mathbf{I}'_k|}} \cdot \frac{1}{K} \cdot (K/2) = \frac{1}{\Delta^{|\mathbf{I}'_k|}} \cdot \frac{1}{2} = |\mathbb{A}|,$$

as required (since $|\mathbf{I}| = |\mathbf{I}'_k|$ for every $k \in [K/2]$).

Remark 122 *Note that for every $k \in [K/2]$ the set $\mathbb{D}_k$ is determined by $\mathbf{I}$ and $\mathbf{I}'_k = \mathbf{J}'_{<k} \cup Ext_k \cup \{\mathbf{q}_k\}$, and $\mathbb{A}$ is determined by $\mathbf{I}$. Thus, we can construct the map M incrementally, by fixing $\mathsf{M}|_{\mathbb{D}_k} : \mathbb{D}_k \to \mathbb{A}$ as soon as $\mathbf{I}'_k$ becomes known. The latter in fact amounts to knowing $\mathbf{J}'_{<k}$, since we fix Ext_k and $\mathbf{q}_k$ for our hard input distribution.*

Remark 123 *We note that while the terminal subcube is defined as $T_* = T_{K/2}$, the parameter k ranges over $[K/2] = \{0, 1, 2 \ldots, K/2 - 1\}$, i.e. not including $k = K/2$. This is exactly in order to ensure that $\sum_{k\in[K/2]} |S'_k|$ equals $|T_*|$ up to lower order terms that can be made small as a function of ϵ, and in particular can be made arbitrarily smaller than K^K – this allows us to control the number of vertices left out by the glueing map τ in Lemma 128.*

For convenience of notation, we first define a map Π^*_k for each $k \in [K/2]$ that pieces together local permutation maps $\Pi_{R'\to R}$. We refer to these maps as *global permutation maps*:

Definition 124 (Global permutation maps Π^*_k) *For every $k \in [K/2]$ and every*

$$z \in \left\{ x \in T'_k : \langle x, \mathbf{q}_k \rangle \pmod M \in \left[0, \frac{1}{K-k}\right) \cdot M \right\}$$

we let $\mathbf{d} \in \mathbb{D}_k$ be such that $z \in Int_\delta(R')$, where $R' = \textsc{Rect}(\mathbf{I}'_k, \mathbf{d})$, if such $\mathbf{d}$ exists (otherwise leave Π^*_k undefined on z). Let $R = \textsc{Rect}(\mathbf{I}, \mathsf{M}(\mathbf{d}))$, where M is as per (135)*. We then define*

$$\Pi^*_k(z) := \Pi_{R'\to R}(z)$$

if $\Pi_{R'\to R}(z)$ is defined (otherwise leave Π^*_k undefined on z).

Finally, we define

Definition 125 (Glueing map τ) *For every $x \in S$, if $k \in [K/2]$ is such that $x \in S'_k$, we let*

$$\tau(x) := \Pi^*_k(\rho_k(x)) \in T_* \tag{136}$$

if $\Pi^*_k(\rho_k(x))$ is defined, and leave $\tau(x)$ undefined otherwise.

For a subset $U \subseteq S'$ we define

$$\tau(U) = \bigcup_{x\in U} \{\tau(x)\},$$

where we think of $\{\tau(x)\}$ as the empty set if $\tau(x)$ is not defined.

We gather some basic properties of the global permutation maps in

Claim 126 (Injectivity of Π^*_k and τ) *For every $k \in [K/2]$ the global permutation map Π^*_k is injective, and the ranges of Π^*_k are disjoint for $k \in [K/2]$. Furthermore, the map τ is injective.*

Proof: Fix $k \in [K/2]$, let $\mathbf{I} = \mathbf{I}_k$ and let

$$Q'_k = \left\{ x \in T'_k : \langle x, \mathbf{q}_k \rangle \pmod M \in \left[0, \frac{1}{K-k}\right) \cdot M \right\}$$

for convenience. We show that for every $z_0, z_1 \in Q'_k$ such that Π^* is defined on both one has $\Pi^*(z_0) \neq \Pi^*(z_1)$. For $z_0 \in Q'_k$ we let $\mathbf{d}_0 \in \mathbb{D}_k$ be such that $z_0 \in \text{Int}_\delta(R'_0)$, where $R'_0 = \textsc{Rect}(\mathbf{I}', \mathbf{d}_0)$, if such $\mathbf{d}_0$ exists (otherwise there is nothing to prove since Π^*_k undefined on z_0). Let $R_0 = \textsc{Rect}(\mathbf{I}, \mathsf{M}(\mathbf{d}_0))$. For $z_1 \in Q'_k$

we let $\mathbf{d}_1 \in \mathbb{D}_k$ be such that $z_1 \in \text{Int}_\delta(R'_1)$, where $R'_1 = \text{RECT}(\mathbf{I}', \mathbf{d}_1)$, if such $\mathbf{d}_1$ exists (otherwise there is nothing to prove since Π^*_k undefined on z_1). Let $R_1 = \text{RECT}(\mathbf{I}, \mathsf{M}(\mathbf{d}_1))$.

Recall that $\Pi^*_k(z_0) = \Pi_{R'_0 \to R_0}(z_0)$ and $\Pi^*_k(z_1) = \Pi_{R'_1 \to R_1}(z_1)$. If either of these maps is undefined on z_0 and z_1 respectively, there is nothing to prove. Now suppose that both of them are defined. By definition of Π^*_k one has

$$\Pi^*_k(z_0) \in R_0 \text{ and } \Pi^*_k(z_1) \in R_1.$$

We thus get that if $\mathbf{d}_0 \neq \mathbf{d}_1$, then $\Pi^*_k(z_0) \neq \Pi^*_k(z_1)$ since $R_0 \cap R_1 = \text{RECT}(\mathbf{I}, \mathsf{M}(\mathbf{d}_0)) \cap \text{RECT}(\mathbf{I}, \mathsf{M}(\mathbf{d}_1)) = \emptyset$ when $\mathbf{d}_0 \neq \mathbf{d}_1$. On the other hand, if $\mathbf{d}_0 = \mathbf{d}_1$, then $\Pi^*_k(z_0) \neq \Pi^*_k(z_1)$ because the map $\Pi_{R'_0 \to R_0} = \Pi_{R'_1 \to R_1}$ is injective by construction. This proves that Π^*_k is injective. Injectivity of Π^* follows from the fact that the map M (see (135)) is injective, as well as the fact that for every $\mathbf{a}_0, \mathbf{a}_1 \in \mathbb{A}$ one has $\text{RECT}(\mathbf{I}, \mathbf{a}_0) \cap \text{RECT}(\mathbf{I}, \mathbf{a}_1) = \emptyset$ when $\mathbf{a}_0 \neq \mathbf{a}_1$.

Finally, we prove injectivity of τ. Pick two distinct vertices $x, y \in S'$. Let $a, b \in [K/2]$ be such that $x \in S'_a$ and $y \in S'_b$. If $a \neq b$, then $\tau(x) \neq \tau(y)$ since the images of Π^*_k are disjoint by definition of M (see (135)), and the fact that for every $\mathbf{a}_0, \mathbf{a}_1 \in \mathbb{A}$ one has $\text{RECT}(\mathbf{I}, \mathbf{a}_0) \cap \text{RECT}(\mathbf{I}, \mathbf{a}_1) = \emptyset$ when $\mathbf{a}_0 \neq \mathbf{a}_1$. If $a = b$, then $\tau(x) = \Pi^*_a(\rho_a(x))$ and $\tau(y) = \Pi^*_a(\rho_a(y))$, where ρ_a is a $(K - a, \mathbf{r})$-densifying map, so the result follows by injectivity of Π^*_k, as well as the fact that ρ is injective by Lemma 116. ■

Similarly to the local (and therefore also global) permutation maps, τ performs sparse bounded shifts:

Lemma 127 (Glueing map τ performs sparse bounded shifts) *For every $x \in S'_k$ if $y = \tau(x)$, then there exist integer coefficients $\{t_\mathbf{i}\}_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'_k}$ such that*

$$y = x + \sum_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'_k} t_\mathbf{i} \cdot \mathbf{i}$$

such that $\|t\|_\infty \leq 5M/w$.

Proof: Let $z = \rho_k(x)$, and note that

$$z = x + \lambda \cdot \mathbf{q}_k$$

for some integer λ satisfying $|\lambda| \leq M/w$ by Lemma 116. Let $\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'_k}$ be such that $z \in R'$ with $R' = \text{RECT}(\mathbf{I}'_k, \mathbf{d})$. Let $R := \text{RECT}(\mathbf{I}, \mathsf{M}(\mathbf{d}))$. Note that $\Pi^*_k(z) = \Pi_{R' \to R}$, and one hence by Lemma 119 one has

$$\Pi^*_k(z) = z + \sum_{\mathbf{i} \in \mathbf{I} \cup \mathbf{I}'_k} s_\mathbf{i} \cdot \mathbf{i},$$

where s satisfies $\|s\|_\infty \leq 4M/w$. These two facts give the result. ■

Unlike the map τ defined in our toy construction from Section 3, the map τ is not quite a bijection. However, the range of τ covers almost all of T_*:

Lemma 128 (τ maps almost all of S' onto terminal subcube T_*) *We have $|T_* \setminus \tau(S')| \leq \delta^{1/4} \cdot |T_0|$. Furthermore, the map τ is defined on all but $\delta^{1/4}|S'|$ vertices in S'.*

Proof: We have

$$\begin{aligned} |T_* \setminus \tau(S')| &\leq |T_*| - |\tau(S')| && \text{(since } \tau(S') \subseteq T_*) \\ &\leq |T_*| - \sum_{k \in [K/2]} |\tau_k(S'_k)| && \text{(since the images of } \tau_k \text{ are disjoint)} \\ &\leq |T_*| - \sum_{k \in [K/2]} |\tau_k(\text{Int}_\delta(S'_k))|. \end{aligned} \tag{137}$$

The second transition used the fact that images of τ_k are disjoint for different k. This follows from the fact that $M : \bigcup_{k\in[K/2]} \mathbb{D}_k \to \mathbb{A}$ is a bijective mapping, together with the fact that by (136) for every $x \in S'_k$, if $\mathbf{d} \in \mathbb{D}_k$ is such that $\rho_k(x) \in R' := \textsc{Rect}(\mathbf{I}'_k, \mathbf{d})$, let $R := \textsc{Rect}(\mathbf{I}, \mathsf{M}(\mathbf{d}))$, then either $\tau(x) = \perp$ or $\tau(x) \in R$.

We let

$$Q'_k = \left\{ x \in T'_k : \langle x, \mathbf{q}_k\rangle \pmod M \in \left[0, \frac{1}{K-k}\right) \cdot M \right\}$$

for convenience, and note that Q'_k is exactly the rhs of (131). We have, using (131)

$$\begin{aligned} |\tau_k(\text{Int}_\delta(S'_k))| &\geq |\Pi^*_k(Q'_k)| - |Q'_k \setminus \text{Int}_\delta(S'_k)| \\ &\geq |\Pi^*_k(Q'_k)| - |Q'_k| + |\text{Int}_\delta(S'_k)| \\ &= |\Pi^*_k(Q'_k)| - |Q'_k| + |S'_k| - |S'_k \setminus \text{Int}_\delta(S'_k)| \\ &\geq |\Pi^*_k(Q'_k)| - |Q'_k| + (1-\sqrt{\delta})|S'_k|, \end{aligned} \tag{138}$$

where the second transition uses the fact that ρ_k is injective, and the last transition uses Lemma 106. We now lower bound the first term above. We have, letting $R'_{\mathbf{d}} := \textsc{Rect}(\mathbf{I}'_k, \mathbf{d})$ and $R_{\mathbf{d}} := \textsc{Rect}(\mathbf{I}, \mathsf{M}(\mathbf{d}))$ for every $\mathbf{d}$ to simplify notation and recalling that

$$Q'_k = \bigcup_{\mathbf{d}\in\mathbb{D}_k} \textsc{Rect}(\mathbf{I}'_k, \mathbf{d}) = \bigcup_{\mathbf{d}\in\mathbb{D}_k} R'_{\mathbf{d}}$$

by Definition 121,

$$|\Pi^*_k(Q'_k)| \geq \sum_{\mathbf{d}\in\mathbb{D}_k} |\Pi^*_k(R'_{\mathbf{d}})| \geq (1-8\sqrt{\epsilon}) \sum_{\mathbf{d}\in\mathbb{D}_k} |R'_{\mathbf{d}}| \geq (1-8\sqrt{\epsilon})|Q'_k| \tag{139}$$

In the equation above we used the fact that by Lemma 120, **(2)**, $\Pi^*_k(R'_{\mathbf{d}})$ is defined on all but a $8\sqrt{\epsilon}\cdot|R'_{\mathbf{d}}|$ vertices of $R'_{\mathbf{d}}$. This lower bounds the first term in (138). To upper bound the second term on the rhs of (138), we first note that by Lemma 102, **(1)**, with $\gamma = \frac{1}{K-k}\cdot\prod_{i=0}^{k-1}(1-\frac{i}{K}) = \frac{1}{K-K}(1-\frac{k}{K}) = \frac{1}{K}$ one has

$$(1-\sqrt{\epsilon})\frac{1}{K} \leq |Q'_k|/m^n \leq (1+\sqrt{\epsilon})\frac{1}{K}$$

and by Lemma 102, **(2)**, one has

$$(1-\sqrt{\epsilon})\frac{1}{K} \leq |S'_k|/m^n \leq (1+\sqrt{\epsilon})\frac{1}{K}, \tag{140}$$

so that

$$(1-3\sqrt{\epsilon})|Q'_k| \leq |S'_k| \leq (1+3\sqrt{\epsilon})|Q'_k|. \tag{141}$$

Substituting the above into (138), we get

$$\begin{aligned} |\tau_k(\text{Int}_\delta(S'_k))| &\geq |\Pi^*_k(Q'_k)| - |Q'_k| + (1-\sqrt{\delta})|S'_k| \\ &\geq |\Pi^*_k(Q'_k)| - |Q'_k| + (1-\sqrt{\delta})(1-3\sqrt{\epsilon})|Q'_k| \quad \text{(by (141))} \\ &\geq |\Pi^*_k(Q'_k)| - (\sqrt{\delta}+3\sqrt{\epsilon})|Q'_k| \\ &\geq (1-8\sqrt{\epsilon})|Q'_k| - (\sqrt{\delta}+3\sqrt{\epsilon})|Q'_k| \quad \text{(by (139))} \\ &\geq (1-11\sqrt{\epsilon}-\sqrt{\delta})|Q'_k| \\ &\geq (1-14\sqrt{\epsilon}-\sqrt{\delta})|S'_k| \\ &\geq (1-2\sqrt{\delta})|S'_k|. \end{aligned} \tag{142}$$

In the last two transitions we used (p6) and the assumption that K is larger than an absolute constant (so that ϵ is smaller than an absolute constant). .

Putting it together. Noting that

$$(1-\sqrt{\epsilon})\frac{1}{2} \le |T_*|/m^n \le (1+\sqrt{\epsilon})\frac{1}{2}$$

by Lemma 102, **(1)**, and substituting (142) into (137), we get

$$\begin{aligned}
|T_* \setminus \tau(S')| &\le |T_*| - \sum_{k\in[K/2]} |\tau_k(\mathrm{Int}_\delta(S'_k))| \\
&\le (1+\sqrt{\epsilon})\frac{1}{2}|T_0| - \sum_{k\in[K/2]} (1-2\sqrt{\delta})|S'_k| \qquad \text{(by (142))} \\
&\le (1+\sqrt{\epsilon})\frac{1}{2}|T_0| - (1-2\sqrt{\delta}) \sum_{k\in[K/2]} |S'_k| \\
&\le (1+\sqrt{\epsilon})\frac{1}{2}|T_0| - (1-4\sqrt{\delta})(1-\sqrt{\epsilon}) \sum_{k\in[K/2]} \frac{1}{K}|T_0| \quad \text{(by (140))} \\
&\le (1+\sqrt{\epsilon})\frac{1}{2}|T_0| - (1-4\sqrt{\delta}-\sqrt{\epsilon})\frac{1}{2}|T_0| \\
&\le (\sqrt{\epsilon}+4\sqrt{\delta}+\sqrt{\epsilon})\frac{1}{2}|T_0| \\
&\le \delta^{1/4}|T_0|
\end{aligned}$$

In the last two transitions we used (p6) and the assumption that K is larger than an absolute constant (so that ϵ and δ are smaller than an absolute constant). The second bound follows similarly. ■

The next lemma shows that the inverse of τ maps two points from the same cube to the same set S'_k for some $k \in [K/2]$.

Lemma 129 (Inverse of τ on a cube) *For every $x, y \in T_*$ such that $x \in \tau(S')$ and $y \in \tau(S')$, if there exists $\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}}$ such that $x, y \in \textsc{Rect}(\mathbf{I}, \mathbf{d})$, the following conditions hold:* **(1)** *there exists $k \in [K/2]$, $\widetilde{x}, \widetilde{y} \in S'_k$ such that $x \in \tau(\widetilde{x})$ and $y \in \tau(\widetilde{y})$,* **(2)** *there exists $\mathbf{d}' \in \mathbf{I}' = \mathbf{J}'_{<k} \cup Ext_k \cup \{\mathbf{q}_k\}$ such that $\rho_k(\widetilde{x}) \in \textsc{Rect}(\mathbf{I}', \mathbf{d}')$ and $\rho_k(\widetilde{y}) \in \textsc{Rect}(\mathbf{I}', \mathbf{d}')$.*

Proof: Let $\widetilde{x}, \widetilde{y} \in S'$ be such that $x \in \tau(\widetilde{x})$ and $y \in \tau(\widetilde{y})$ (such $\widetilde{x}$ and $\widetilde{y}$ exist by assumption of the lemma). Let $k_x, k_y \in [K/2]$ by such that $\widetilde{x} \in S'_{k_x}$ and $\widetilde{y} \in S'_{k_y}$. We will show that $k_x = k_y$. Recall that by Definition 124 we let $\mathbf{d}_x \in \mathbb{D}_{k_x}$ be such that $\rho_{k_x}(\widetilde{x}) \in \mathrm{Int}_\delta(\textsc{Rect}(\mathbf{I}'_{k_x}, \mathbf{d}_x))$, and let $\mathbf{d}_y \in \mathbb{D}_{k_y}$ be such that $\rho_{k_y}(\widetilde{y}) \in \mathrm{Int}_\delta(\textsc{Rect}(\mathbf{I}'_{k_y}, \mathbf{d}_y))$, where ρ_{k_x} and ρ_{k_y} are corresponding densification maps as per Definition 115 (along directions $\mathbf{q}_{k_x}$ and $\mathbf{q}_{k_y}$ respectively). Then

$$x = \Pi^*_{k_x}(\rho_{k_x}(\widetilde{x})) \in \textsc{Rect}(\mathbf{I}, \mathsf{M}(\mathbf{d}_x))$$

and

$$y = \Pi^*_{k_y}(\rho_{k_y}(\widetilde{y})) \in \textsc{Rect}(\mathbf{I}, \mathsf{M}(\mathbf{d}_y)).$$

Since $x, y \in \textsc{Rect}(\mathbf{I}, \mathbf{d})$ by assumption of the lemma, we get that $\mathsf{M}(\mathbf{d}_x) = \mathsf{M}(\mathbf{d}_y) = \mathbf{d}$. Since M is injective, this in particular implies that $k_x = k_y = k$ and $\mathbf{d}_x = \mathbf{d}_y$, as required. Letting $\mathbf{I}' = \mathbf{J}'_{<k} \cup \mathrm{Ext}_k \cup \{\mathbf{q}_k\}$, we thus get $\rho_k(\widetilde{x}) \in \textsc{Rect}(\mathbf{I}', \mathbf{d}')$ and $\rho_k(\widetilde{y}) \in \textsc{Rect}(\mathbf{I}', \mathbf{d}')$. ■

6 Predecessor map ν and its properties

In this section we define the predecessor map ν, which lets us define a good upper bound on the size of the maximum matching constructed by a low space algorithm later in Section 7 (specifically, see definition of the sets A_P, A_Q, B_P, B_Q in (245) and (247)). Intuitively, the predecessor map $\nu_{\ell,j}$ maps a subset of T^ℓ for some $\ell \in [L]$ through j repeated applications of the glueing map τ^ℓ interleaved with applications of the DOWNSET map. This is a natural object, since our construction is motivated by the fact that for appropriately defined 'nice' subsets $U \subseteq T^\ell$, namely for appropriately defined rectangles (see Lemma 10 in Section 2), the edge boundary of the set $U \cup \text{DOWNSET}^\ell(U)$ is very sparse, which is the basis of our hard input instance.

Definition 130 (Predecessor map ν) *We define the map $\nu_{\ell,j} : 2^{T^\ell} \to 2^{T^{\ell-j}}$ (mapping subsets of T^ℓ to subsets of $T^{\ell-j}$) as follows. For $U \subseteq T^\ell$ we let*

$$\nu_{\ell,0}(U) := U$$

and

$$\nu_{\ell,j}(U) := \tau^{\ell-(j-1)}(\text{DOWNSET}^{\ell-(j-1)}(\nu_{\ell,j-1}(U)))$$

for $j = 1, \ldots, \ell$. We define the closure *map $\nu_{\ell,*}$ by*

$$\nu_{\ell,*}(U) := \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \nu_{\ell,j}(U).$$

Similarly, we define

$$\mu_{\ell,j}(U) := \text{DOWNSET}^{\ell-j}(\nu_{\ell,j}(U))$$

for $j = 0, \ldots, \ell$, and let

$$\mu_{\ell,*}(U) := \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \mu_{\ell,j}(U).$$

Remark 131 *We note that $\nu_{\ell,j}$ can be viewed as mapping elements of T^ℓ to $T^{\ell-j}$: for $x \in T^\ell$ the image of x under $\nu_{\ell,j}$ is naturally defined as $\nu_{\ell,j}(\{x\})$, i.e. the image of a singleton set containing x. This map, however, is not a one-to-one map because* DOWNSET *is not (see Definition 87 and Remark 88). This in particular is the reason why we prefer to define $\nu_{\ell,j}$ as mapping sets to sets in Definition 130. On the other hand, $\nu_{\ell,j}$ maps every vertex to at most K^j vertices, since* DOWNSET *maps every vertex to at most $K/2$ vertices, and τ is a one to (at most) one map.*

The main results of this section are the following two lemmas. The first lemma bounds the size of the image of the non-terminal part of T^ℓ, namely $T^\ell \setminus T^\ell_*$, under the predecessor map μ:

Lemma 132 *For every $\ell \in [L]$, every $j = 0, \ldots, \ell$, one has*

$$(\ln 2 - C/K)^j \frac{1}{2}(1 - \ln 2)|T_0| \leq |\mu_{\ell,j}(T^\ell \setminus T^\ell_*)| \leq (\ln 2 + C/K)^j \frac{1}{2}(1 - \ln 2)|T_0|$$

for an absolute constant $C > 0$.

The second lemma is Lemma 143, which proves a key property (equivalent to Lemma 10 in Section 2) allowing us reason about the structure of the upper bounding vertex cover in Lemma 155 of Section 7.

6.1 Basic properties of ν and μ

Definition 133 (Injectivity for maps defined on sets) *A map $\nu : 2^A \to 2^B$ (mapping subsets of A to subsets of B) is called injective if for every $x, y \in A, x \neq y$ one has $\nu(\{x\}) \cap \nu(\{y\}) = \emptyset$.*

The following properties of ν and μ will be useful:

Claim 134 *For every $\ell \in [L]$, every $j \in 1, \ldots, \ell$ and every $U \subseteq T^\ell$ one has* **(1)** $\nu_{\ell,j}(U) = \nu_{\ell-1,j-1}(\tau^\ell(\textsc{DownSet}^\ell(U))$ *and* **(2)** $\mu_{\ell,j}(U) = \mu_{\ell-1,j-1}(\tau^\ell(\textsc{DownSet}^\ell(U)))$.

Proof: For **(1)** we have by Definition 130

$$\begin{aligned}\nu_{\ell,j}(U) &= \tau^{\ell-(j-1)}(\textsc{DownSet}^{\ell-(j-1)}(\nu_{\ell,j-1}(U)))\\ &= \tau^{\ell-(j-1)}(\textsc{DownSet}^{\ell-(j-1)}(\tau^{\ell-(j-2)}(\textsc{DownSet}^{\ell-(j-2)}(\nu_{\ell,j-2}(U)))))\\ &= \tau^{\ell-(j-1)}(\textsc{DownSet}^{\ell-(j-1)}(\tau^{\ell-(j-2)}(\textsc{DownSet}^{\ell-(j-2)}(\ldots\tau^{\ell}(\textsc{DownSet}^{\ell}(U))\ldots))))\\ &= \nu_{\ell-1,j-1}(\tau^\ell(\textsc{DownSet}^\ell(U)))\end{aligned}$$

For **(2)** we have by Definition 130 and using **(1)**

$$\begin{aligned}\mu_{\ell,j}(U) &= \textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(U))\\ &= \textsc{DownSet}^{\ell-j}(\nu_{\ell-1,j-1}(\tau^\ell(\textsc{DownSet}^\ell(U))))\\ &= \mu_{\ell-1,j-1}(\tau^\ell(\textsc{DownSet}^\ell(U))).\end{aligned}$$

■

We also need

Lemma 135 (Basic properties of the maps $\nu_{\ell,j}$ and $\mu_{\ell,j}$) *The following conditions hold for the maps ν and μ defined above:*

(1) *for every $\ell \in [L]$ and every $0 \leq j \leq \ell$ the maps $\nu_{\ell,j}$ and $\mu_{\ell,j}$ are injective;*

(2) *every $\ell, \ell' \in [L]$ every $0 \leq j \leq \ell$, $0 \leq j' \leq \ell'$, one has*

$$\nu_{\ell,j}(T^\ell \setminus T^\ell_*) \cap \nu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) = \emptyset$$

unless $\ell = \ell'$ and $j = j'$.

(3) *every $\ell, \ell' \in [L]$ every $0 \leq j \leq \ell$, $0 \leq j' \leq \ell'$, one has*

$$\mu_{\ell,j}(T^\ell \setminus T^\ell_*) \cap \mu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) = \emptyset$$

unless $\ell = \ell'$ and $j = j'$.

Proof: **(1)** follows since τ is injective by Claim 126 and $\textsc{DownSet}$ is injective by construction (Definition 87).

We now show **(2)**. First note that $\nu_{\ell,j}(T^\ell \setminus T^\ell_*) \subseteq T^{\ell-j}$ and $\nu_{\ell',j'}(T^{\ell'} \setminus T^{\ell'}_*) \subseteq T^{\ell'-j'}$, and hence the two sets are disjoint if $\ell - j \neq \ell' - j'$. Now suppose that $\ell - j = \ell' - j'$ and assume without loss of generality that $\ell \leq \ell'$. Furthermore, we can assume that $\ell < \ell'$, since if $\ell = \ell'$, one must have $j = j'$ as otherwise the sets are disjoint by the previous argument. Now note that

$$\nu_{\ell',\ell'-\ell}(T^{\ell'} \setminus T^{\ell'}_*) = \tau^{\ell+1}(\textsc{DownSet}^{\ell+1}(\nu_{\ell',\ell'-\ell-1}(T^{\ell'} \setminus T^{\ell'}_*)) \subseteq T^\ell_*,$$

since the range of $\tau^{\ell+1}$ is T_*^ℓ (see Definition 125). This means that

$$\begin{aligned}\nu_{\ell',j'}(T^{\ell'} \setminus T_*^{\ell'}) &= \nu_{\ell,j}(\nu_{\ell',\ell'-\ell}(T^{\ell'} \setminus T_*^{\ell'})) \\ &\subseteq \nu_{\ell,j}(T_*^\ell),\end{aligned}$$

and we get that

$$\nu_{\ell,j}(T^\ell \setminus T_*^\ell) \cap \nu_{\ell',j'}(T^{\ell'} \setminus T_*^{\ell'}) \subseteq \nu_{\ell,j}(T^\ell \setminus T_*^\ell) \cap \nu_{\ell,j}(T_*^\ell) = \emptyset$$

since $\nu_{\ell,j}$ is injective by **(1)**.

We now prove **(3)**. First note that by Definition 130

$$\mu_{\ell,j}(T^\ell \setminus T_*^\ell) \subseteq S^{\ell-j}$$

and

$$\mu_{\ell',j'}(T^{\ell'} \setminus T_*^{\ell'}) \subseteq S^{\ell'-j'},$$

and hence similarly to above the two sets are disjoint unless $\ell - j = \ell' - j'$. **(3)** now follows by noting that, again using Definition 130, we get, since $\ell - j = \ell' - j'$ and DOWNSET is injective,

$$\begin{aligned}\mu_{\ell,j}(T^\ell \setminus T_*^\ell) \cap \mu_{\ell',j'}(T^{\ell'} \setminus T_*^{\ell'}) &= \textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T_*^\ell)) \cap \textsc{DownSet}^{\ell'-j'}(\nu_{\ell',j'}(T^{\ell'} \setminus T_*^{\ell'})) \\ &= \textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T_*^\ell) \cap \nu_{\ell',j'}(T^{\ell'} \setminus T_*^{\ell'})) \\ &= \emptyset,\end{aligned}$$

where we used **(2)** in the last transition. ■

While for a given ℓ the terminal subcube T_*^ℓ is almost entirely covered by the range of $\tau^{\ell+1}$, it will be useful to know that almost all of T_*^ℓ can be covered by the image of the non-terminal part of $T^{\ell+j}$ under $\nu_{\ell+j,j}$:

Lemma 136 *For every $\ell \in [L]$ there exists $Z^\ell \subset T_*^\ell$ such that*

$$T_*^\ell = Z^\ell \cup \left(\nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j=1}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})\right)$$

and $|Z^\ell| \le K^L \delta^{1/4} \cdot |P|$.

Proof: We prove by induction on $\ell = L-1, \dots, 0$ that there exists sets $Z^\ell \subset T_*^\ell$ such that

$$T_*^\ell = Z^\ell \cup \left(\nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j=1}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})\right) \tag{143}$$

and $|Z^\ell| \le K^{L-\ell}\delta^{1/4}|P|$.

Base: $\ell = L-1$. One has $T_*^\ell = \nu_{L-1,0}(T_*^{L-1})$, since $\nu_{L-1,0}$ is the identity map by definition (see Definition 130). We let $Z^{L-1} = \emptyset$, so that $T_*^{L-1} = Z^\ell \cup \nu_{L-1,0}(T_*^{L-1})$.

Inductive step: $\ell \to \ell - 1$. Let

$$Z^\ell = T_*^\ell \setminus \left(\nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j\ge1} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})\right),$$

and note that

$$T_*^\ell = Z^\ell \cup \left(\nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j\geq 1} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})\right). \tag{144}$$

Applying $\tau^\ell(\textsc{DownSet}^\ell(\cdot))$ to both sides of (144), we get, letting $Q = \nu_{L-1,L-1-\ell}(T_*^{L-1})$ and

$$Z' = \tau^\ell(\textsc{DownSet}^\ell(Z)) \tag{145}$$

to simplify notation,

$$\begin{aligned}
\tau^\ell(\textsc{DownSet}^\ell(T_*^\ell)) &= Z' \cup \tau^\ell\left(\textsc{DownSet}^\ell\left(Q \cup \bigcup_{j\geq 1} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})\right)\right)\\
&= Z' \cup \tau^\ell\left(\textsc{DownSet}^\ell\left(Q\right)\right) \cup \bigcup_{j\geq 1} \tau^\ell\left(\textsc{DownSet}^\ell\left(\nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})\right)\right)\\
&= Z' \cup \nu_{L-1,L-\ell}(T_*^{L-1}) \cup \bigcup_{j\geq 1} \nu_{\ell+j,j+1}(T^{\ell+j} \setminus T_*^{\ell+j})\\
&= Z' \cup \nu_{L-1,L-\ell}(T_*^{L-1}) \cup \bigcup_{j\geq 1} \nu_{(\ell-1)+(j+1),j+1}(T^{(\ell-1)+(j+1)} \setminus T_*^{(\ell-1)+(j+1)})\\
&= Z' \cup \nu_{L-1,L-1-(\ell-1)}(T_*^{L-1}) \cup \bigcup_{j\geq 2} \nu_{(\ell-1)+j,j}(T^{(\ell-1)+j} \setminus T_*^{(\ell-1)+j}),
\end{aligned} \tag{146}$$

where the third transition is by Claim 134, **(1)**. At the same time we also have

$$\tau^\ell(\textsc{DownSet}^\ell(T^\ell \setminus T_*^\ell)) = \nu_{\ell,1}(T^\ell \setminus T_*^\ell) = \nu_{(\ell-1)+1,1}(T^\ell \setminus T_*^\ell). \tag{147}$$

Let $Z'' = T_*^{\ell-1} \setminus \tau^\ell(S^\ell)$. We have

$$\begin{aligned}
T_*^{\ell-1} &= Z'' \cup \tau^\ell(S^\ell)\\
&= Z'' \cup \tau^\ell(\textsc{DownSet}^\ell(T^\ell))\\
&= Z'' \cup \tau^\ell(\textsc{DownSet}^\ell(T^\ell \setminus T_*^\ell)) \cup \tau^\ell(\textsc{DownSet}^\ell(T_*^\ell))
\end{aligned} \tag{148}$$

Substituting (146) and (147) into (148), we get

$$T_*^{\ell-1} = Z^{\ell-1} \cup \nu_{L-1,L-\ell}(T_*^{L-1}) \cup \bigcup_{j\geq 1} \nu_{\ell-1+j,j}(T^{\ell-1+j} \setminus T_*^{\ell-1+j}), \tag{149}$$

where we let $Z^{\ell-1} := Z' \cup Z''$, so that by (145)

$$Z^{\ell-1} = Z' \cup Z'' = \tau^\ell(\textsc{DownSet}^\ell(Z^\ell)) \cup (T_*^{\ell-1} \setminus \tau^\ell(S^\ell)).$$

Thus, in order to complete the proof of the inductive claim, we need to show that $|Z^{\ell-1}| \leq K^{L-1-(\ell-1)}\delta^{1/4} \cdot |P|$.

We have $|Z''| \leq \delta^{1/4}|T_0|$ by Lemma 128, and hence

$$\begin{aligned}
|Z^\ell| &\leq |\tau^\ell(\textsc{DownSet}^\ell(Z^\ell))| + |Z''|\\
&\leq (K/2)|Z^\ell| + |Z''|\\
&\leq (K/2) \cdot K^{L-1-\ell}\delta^{1/4}|P| + \delta^{1/4}|P|\\
&\leq K^{L-1-(\ell-1)}\delta^{1/4}|P|,
\end{aligned} \tag{150}$$

The second inequality is due to the fact that $\textsc{DownSet}^\ell$ maps every vertex to at most $K/2$ vertices, and τ^ℓ is a one-to-one map. The third inequality uses the inductive hypothesis and the bound $|Z''| \leq \delta^{1/4}|T_0| \leq \delta^{1/4}|P|$. This completes the proof of the inductive step.

Finally, to obtain the result of the lemma, we extend the union on the right hand side of (149) to include $j = 0$, getting

$$T^\ell = Z^{\ell-1} \cup \nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j\geq 0} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}),$$

as required. This completes the proof of the inductive step. ■

6.2 Image of non-terminal subsets $T^\ell \setminus T_*^\ell$ under μ (proof of Lemma 132)

In this section we prove Lemma 132. We start with two auxiliary lemmas, and a definition:

Definition 137 (Vector consistent with the terminal subcube) *For every $\ell \in [L]$, if $\mathbf{J} = \Psi(\mathbf{B}^\ell)$, we say that a vector $\mathbf{f} \in \Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{J}}$ is* consistent with the terminal subcube T_*^ℓ *if for every $k \in [K/2]$ one has $\mathbf{f}_{\mathbf{j}_k} \in [0, 1 - \frac{1}{K-k})$.*

The first lemma bounds the size of the image of a rectangle F consistent with the terminal subcube under the predecessor map ν:

Lemma 138 *There exists an absolute constant $C > 0$ such that for every $\ell \in [L]$, every $j = 0, \ldots, \ell$, if $\mathbf{I} = \Psi(\mathbf{B}^\ell)$ and $\mathbf{H} \subseteq \Psi(\mathbf{B}^{>\ell})$, the following conditions hold.*

For every $\mathbf{f} \in \Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{I}}$ consistent with the terminal subcube T_*^ℓ (as per Definition 137) and every $\mathbf{c}, \mathbf{d} \in \Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{H}}, \mathbf{c} < \mathbf{d}$, if $F = \textsc{Rect}(\mathbf{I} \cup \mathbf{H}, (\mathbf{f}, \mathbf{c}), (\mathbf{f} + \Delta \cdot \mathbf{1}, \mathbf{d}))$, then

$$(\ln 2 - C/K)^j |F| \leq |\nu_{\ell,j}(F)| \leq (\ln 2 + C/K)^j |F|$$

for an absolute constant $C > 0$.

Proof: The proof is by induction on j. The inductive claim is that for every $\ell \in [L]$, if $\mathbf{I} = \Psi(\mathbf{B}^\ell)$ and $\mathbf{H} \subset \Psi(\mathbf{B}^{\geq \ell+1})$, the following conditions hold. For every $\mathbf{f} \in \Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{I}}$ and every $\mathbf{c}, \mathbf{d} \in \Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{H}}$, if $F = (\mathbf{I} \cup \mathbf{H}, (\mathbf{f}, \mathbf{c}), (\mathbf{f} + \Delta \cdot \mathbf{1}, \mathbf{d}))$, then

$$(\ln 2 - C/K)^j |F| \leq |\nu_{\ell,j}(F)| \leq (\ln 2 + C/K)^j |F|$$

where $C > 0$ is the absolute constant.
Base: $j = 0$. We have $|\nu_{\ell,j}(F)| = |F|$ since $\nu_{\ell,0}(F) = F$ for every F.
Inductive step: $j \to j + 1$. Fix $k \in [K/2]$, and let ρ_k be the $(K - k, \mathbf{q}_k)$-compressing map as per Definition 115, where $\mathbf{q}_k = \mathbf{q}_k^\ell \in \mathcal{F}$ is the compression vector for the k-th phase of the graph G^ℓ (see Definition 81). We let $\mathbf{J}' := \mathbf{J}^\ell$, $\mathbf{J} := \mathbf{J}^{\ell-1}$, $\mathbf{B}' := \mathbf{B}^\ell$, $\mathbf{B} := \mathbf{B}^{\ell-1}$ to simplify notation. Similarly define $T' := T^\ell$, $T := T^{\ell-1}$ and $S' := S^\ell$, $S := S^{\ell-1}$ to simplify notation. Let $\mathbf{r}' := \mathbf{r}^\ell$ and $\mathbf{r} := \mathbf{r}^{\ell-1}$ denote the ℓ-th and the $(\ell-1)$-th compression index respectively. We define

$$Z_k := \left\{ x \in [m]^n : \text{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \right\},$$

and let

$$Q_k^{ext} := \left\{ x \in F : \langle x, \mathbf{q}_k \rangle \pmod{M} \in \left[0, \frac{1}{K-k}\right) \cdot M \right\} \tag{151}$$

to simplify notation. The proof of the inductive step proceeds in several steps. In **Step 1** we show that for every $k \in [K/2]$ the image of the k-th downset of F under the compression map ρ_k is essentially the entire set

Q_k^{ext} (this is formally stated in (155) below). Then in **Step 2** we bound $|\nu_{\ell-1,j-1}(\Pi_k^*(Q_k^{ext}))|$ for $k \in [K/2]$ using the inductive hypothesis. Finally, in **Step 3** we put our bounds together to obtain the result of the lemma.

We start by establishing some basic bounds relating $|Q_k^{ext}|$ to $|F|$ that will be useful throughout the proof. We let $\gamma = \Delta^{|\mathbf{I}|} \cdot \prod_{\mathbf{i}\in\mathbf{H}}(\mathbf{d_i} - \mathbf{c_i})$ and invoke Lemma 102. By Lemma 102, **(1)**, we get

$$(1-\sqrt{\epsilon})\gamma \le |F|/m^n \le (1+\sqrt{\epsilon})\gamma, \tag{152}$$

and by Lemma 102, **(2)**,

$$(1-\sqrt{\epsilon})\frac{1}{K-k}\cdot\gamma \le |F\cap Z_k|/m^n \le (1+\sqrt{\epsilon})\frac{1}{K-k}\cdot\gamma. \tag{153}$$

Similarly, by Lemma 102, **(1)**, $\gamma' = \frac{1}{K-k}\cdot\Delta^{|\mathbf{I}|}\cdot\prod_{\mathbf{i}\in\mathbf{H}}(\mathbf{d_i}-\mathbf{c_i}) = \frac{1}{K-k}\cdot\gamma$ we get

$$(1-\sqrt{\epsilon})\frac{1}{K-k}\cdot\gamma \le \left|Q_k^{ext}\right|/m^n \le (1+\sqrt{\epsilon})\frac{1}{K-k}\cdot\gamma.$$

The bounds above imply

$$(1-3\sqrt{\epsilon})\frac{1}{K-k}|F| \le |Q_k^{ext}| \le (1+3\sqrt{\epsilon})\frac{1}{K-k}|F| \tag{154}$$

for every $k \in [K/2]$. Recalling that

$$\textsc{DownSet}_k(F) \asymp F \cap Z_k$$

and putting the above bounds together, we get $\rho_k\left(\textsc{DownSet}_k(\text{Int}_\delta(F))\right) \subseteq Q_k^{ext}$ and

$$\begin{aligned}\left|\rho_k\left(\textsc{DownSet}_k(F)\right)\cap Q_k^{ext}\right| &\ge \left|\rho_k\left(\textsc{DownSet}_k(\text{Int}_\delta(F))\right)\cap Q_k^{ext}\right| \\ &\ge |\textsc{DownSet}_k(\text{Int}_\delta(F))| \\ &\ge |\textsc{DownSet}_k(F)| - |F\setminus\text{Int}_\delta(F)| \\ &= |F\cap Z_k| - |F\setminus\text{Int}_\delta(F)| \\ &\ge (1-\sqrt{\epsilon})\frac{1}{K-k}\cdot\gamma\cdot m^n - \sqrt{\delta}|F| \\ &\ge (1-2K\sqrt{\delta}-3\sqrt{\epsilon})|Q_k^{ext}|.\end{aligned}$$

The first transition uses the fact that by Lemma 116 one has that

$$\rho_k\left(\text{Int}_\delta(F)\cap Z_k\right) \subseteq Q_k^{ext}$$

and ρ_k is injective on $\text{Int}_\delta(F)\cap Z_k$. The transition from line 4 to line 5 is by Lemma 106 and (153). The transition from line 5 to line 6 is by (154). Similarly, we get

$$\begin{aligned}|\rho_k\left(\textsc{DownSet}_k(F)\right)| &= \left|\rho_k\left(\textsc{DownSet}_k(F)\right)\cap Q_k^{ext}\right| + \left|\rho_k\left(\textsc{DownSet}_k(F)\right)\setminus Q_k^{ext}\right| \\ &\le \left|Q_k^{ext}\right| + |\rho_k\left(\textsc{DownSet}_k(F)\right)\setminus\rho_k\left(\textsc{DownSet}_k(\text{Int}_\delta(F))\right)| \\ &\le \left|Q_k^{ext}\right| + |F\setminus\text{Int}_\delta(F)| \\ &\le \left|Q_k^{ext}\right| + \sqrt{\delta}\,|F| \\ &\le (1-2K\sqrt{\delta})|Q_k^{ext}|.\end{aligned}$$

The second transition uses the fact that by Lemma 116, **(2)**, one has $\rho_k\left(\text{Int}_\delta(F)\cap Z_k\right) \subseteq Q_k^{ext}$ and ρ_k is injective by Lemma 116, **(1)**. The transition from line 3 to line 4 is by Lemma 106. The transition from line 4 to line 5 is by (154).

Noting that $2K\sqrt{\delta} + 2\sqrt{\epsilon} \leq \delta^{1/4}$ by (p4) and (p5), we record the above in the simpler form

$$(1-\delta^{1/4})|Q_k^{ext}| \leq \left|\rho_k\left(\textsc{DownSet}_k(F)\right) \cap Q_k^{ext}\right| \leq (1+\delta^{1/4})|Q_k^{ext}|. \tag{155}$$

Step 1. By Claim 134, **(1)**, we have

$$\begin{aligned}\nu_{\ell,j}(F) &= \nu_{\ell-1,j-1}(\tau^\ell(\textsc{DownSet}^\ell(F))\\ &= \bigcup_{k\in[K/2]} \nu_{\ell-1,j-1}(\tau_k^\ell(\textsc{DownSet}_k^\ell(F))\\ &= \bigcup_{k\in[K/2]} \nu_{\ell-1,j-1}(\tau_k(\textsc{DownSet}_k(F)),\end{aligned}$$

where we dropped the superscipt ℓ in the last line to simplify notation. For every $k \in [K/2]$ we have using (155) and the fact that $\tau_k = \Pi_k^* \circ \rho_k$

$$\begin{aligned}|\nu_{\ell-1,j-1}(\tau_k(\textsc{DownSet}_k(F)))| &= |\nu_{\ell-1,j-1}(\Pi_k^*(\rho_k(F\cap Z_k)))|\\ &\geq \left|\nu_{\ell-1,j-1}\left(\Pi_k^*(Q_k^{ext})\right)\right| - \max_{\substack{S\subseteq Q_k^{ext}\\ |S|\leq\delta^{1/4}|Q_k^{ext}|}} |\nu_{\ell-1,j-1}\left(\Pi_k^*(S)\right)|\\ &\geq \left|\nu_{\ell-1,j-1}\left(\Pi_k^*(Q_k^{ext})\right)\right| - K^{j-1}\delta^{1/4}\cdot|Q_k^{ext}|,\end{aligned} \tag{156}$$

since for every S one has $|\nu_{\ell-1,j-1}(S)| \leq K^{j-1}|S|$. For the upper bound we have for every $k \in [K/2]$

$$\begin{aligned}|\nu_{\ell-1,j-1}(\tau_k(\textsc{DownSet}_k(F)))| &= |\nu_{\ell-1,j-1}(\Pi_k^*(\rho_k(F\cap Z_k)))|\\ &\leq \left|\nu_{\ell-1,j-1}\left(\Pi_k^*(Q_k^{ext})\right)\right| + \left|\nu_{\ell-1,j-1}\left(\Pi_k^*(\rho_k(F\cap Z_k)\setminus Q_k^{ext})\right)\right|\\ &\leq \left|\nu_{\ell-1,j-1}\left(\Pi_k^*(Q_k^{ext})\right)\right| + K^{j-1}\delta^{1/4}\cdot|Q_k^{ext}|.\end{aligned} \tag{157}$$

We used the second inequality in (155) in the last transition, together with the fact that Π_k^* maps every vertex to at most one vertex.

Step 2. We now apply the inductive hypothesis to bound the first term in (156) (which coincides with the first term on the rhs of (157)). Define

$$\begin{aligned}\mathbf{I}'_0 &= \mathbf{J}'_{<k} \cup \mathrm{Ext}_k \cup \{\mathbf{q}_k\}\\ \mathbf{I}'_1 &= \mathbf{J}'_{\geq k} \cup \{\mathbf{r}'\} \cup \mathbf{H},\end{aligned} \tag{158}$$

where we let $\mathrm{Ext}_k := \mathrm{Ext}_k^\ell$ to simplify notation. Let $\mathbf{f}_0$ denote the restriction of $\mathbf{f}$ to coordinates in $\mathbf{J}'_{<k}$, and let $\mathbf{f}_1$ denote the restriction of $\mathbf{f}$ to coordinates in $\Psi(\mathbf{B}^\ell) \setminus \mathbf{J}'_{<k} = \mathbf{J}'_{\geq k} \cup \{\mathbf{r}'\}$. We also let

$$\begin{aligned}\mathbf{I}_0 &= \mathbf{J} \cup \{\mathbf{r}\}\\ \mathbf{I}_1 &= \mathbf{I}'_1.\end{aligned} \tag{159}$$

Now note that the definition of $\mathbf{I}'_0$ in (158) coincided with the definition of $\mathbf{I}'_k$ in (130), and the definition of $\mathbf{I}_0$ in (159) coincides with the definition of $\mathbf{I}$ in (129). Thus, by Definition 125 the map $\tau_k : S'_k \to T_*$ is defined by letting

$$\tau_k(x) = \Pi_k^*(\rho_k(x)),$$

where Π_k^* is defined as follows. For $z = \rho_k(x) \in [m]^n$ (leave τ_k undefined if $\rho_k(x)$ is not defined) one lets $\mathbf{a}_0 \in \mathbb{D}_k$, $R'(\mathbf{a}_0) := (\mathbf{I}'_0, \mathbf{a}_0, \mathbf{a}_0 + \Delta\cdot\mathbf{1})$ be such that

$$z \in \mathrm{Int}_\delta(R'(\mathbf{a}_0)) \tag{160}$$

if such an $\mathbf{a}_0 \in \mathbb{D}_k$ exists (otherwise $\Pi^*(z)$ is left undefined). Then one lets

$$R(\mathbf{a}_0) := (\mathbf{I}_0, \mathsf{M}(\mathbf{a}_0), \mathsf{M}(\mathbf{a}_0) + \Delta \cdot \mathbf{1}), \tag{161}$$

where M is as in (135), and sets, as per Definition 124,

$$\Pi_k^*(z) := \Pi_{R'(\mathbf{a}_0) \to R(\mathbf{a}_0)}(z). \tag{162}$$

We now show that $\tau_k(Q_k^{ext})$ can be approximated by a union of rectangles consistent with the terminal subcube T_*, to which we can apply the inductive hypothesis. Recall that by (151) one has

$$Q_k^{ext} := \left\{ x \in F : \langle x, \mathbf{q}_k \rangle \pmod{M} \in \left[0, \frac{1}{K-k}\right) \cdot M \right\}$$

where

$$F = \textsc{Rect}(\mathbf{I} \cup \mathbf{H}, (\mathbf{f}, \mathbf{c}), (\mathbf{f} + \Delta \cdot \mathbf{1}, \mathbf{d})).$$

For $\mathbf{a}_0 \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'_0}$ we define the extended rectangles

$$R'_{ext}(\mathbf{a}_0) = (\mathbf{I}'_0 \cup \mathbf{I}'_1, (\mathbf{a}_0, (\mathbf{f}_1, \mathbf{c})), (\mathbf{a}_0 + \Delta \cdot \mathbf{1}, (\mathbf{f}_1 + \Delta \cdot \mathbf{1}, \mathbf{d})))$$

and

$$R_{ext}(\mathbf{a}_0) = (\mathbf{I}_0 \cup \mathbf{I}_1, (\mathsf{M}(\mathbf{a}_0), (\mathbf{f}_1, \mathbf{c})), (\mathsf{M}(\mathbf{a}_0) + \Delta \cdot \mathbf{1}, (\mathbf{f}_1 + \Delta \cdot \mathbf{1}, \mathbf{d}))).$$

We now recall the definition of $\mathbb{D}_k$ (see Definition 121). Indeed, let $\mathbf{u}_{\mathbf{j}'_s} = 0, \mathbf{v}_{\mathbf{j}'_s} = 1 - \frac{1}{K-s}$ for $s \in [k]$, let $\mathbf{u}_{\mathbf{q}_k} = 0, \mathbf{v}_{\mathbf{q}_k} = \frac{1}{K-k}$, and $\mathbf{u}_{\mathbf{i}} = 0, \mathbf{v}_{\mathbf{i}} = 1$ for $\mathbf{i} \in \mathrm{Ext}_k$. Then, noting that $\mathbf{I}'_0$ as per (158) is equal to $\mathbf{I}'$ as per (130) one has as per (132)

$$\mathbb{D}_k = (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}'_0} \cap \prod_{\mathbf{i} \in \mathbf{I}'_0} [\mathbf{u}_{\mathbf{i}}, \mathbf{v}_{\mathbf{i}}). \tag{163}$$

We start by noting that Q_k^{ext} is a rectangle in $\mathbf{I}'_0 \cup \mathbf{I}'_1$. Indeed, let

$$\begin{aligned}
&\mathbf{u}^0_{\mathbf{j}'_s} = \mathbf{f}_{\mathbf{j}_s}, \mathbf{v}^0_{\mathbf{j}'_s} = \mathbf{f}_{\mathbf{j}_s} + \Delta \quad \text{ for } s \in [k] \\
&\mathbf{u}^0_{\mathbf{q}_k} = 0, \mathbf{v}^0_{\mathbf{q}_k} = \frac{1}{K-k} \\
&\text{and} \\
&\mathbf{u}^0_{\mathbf{i}} = 0, \mathbf{v}^0_{\mathbf{i}} = 1 \quad \text{ for } \mathbf{i} \in \mathrm{Ext}_k,
\end{aligned}$$

so that $\mathbf{u}^0, \mathbf{v}^0 \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'_0}$ (note that $\mathbf{u}^0 = \mathbf{f}_0$ and $\mathbf{v}^0 = \mathbf{f}_0 + \Delta \cdot \mathbf{1}$). Also let

$$\begin{aligned}
&\mathbf{u}^1_{\mathbf{j}'_s} = \mathbf{f}_{\mathbf{j}_s}, \mathbf{v}^1_{\mathbf{j}'_s} = \mathbf{f}_{\mathbf{j}_s} + \Delta \quad \text{ for } s \in \{k, k+1, \ldots, K/2 - 1\}, \\
&\mathbf{u}^1_{\mathbf{r}'_k} = 0, \mathbf{v}^1_{\mathbf{r}'_k} = 1, \\
&\text{and} \\
&\mathbf{u}^1_{\mathbf{i}} = \mathbf{c}_{\mathbf{i}}, \mathbf{v}^1_{\mathbf{i}} = \mathbf{d}_{\mathbf{i}} \quad \text{ for } \mathbf{i} \in \mathbf{H},
\end{aligned}$$

so that $\mathbf{u}^1, \mathbf{v}^1 \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'_1}$. We have $Q_k^{ext} = \textsc{Rect}(\mathbf{I}'_0 \cup \mathbf{I}'_1, (\mathbf{u}^0, \mathbf{u}^1), (\mathbf{v}^0, \mathbf{v}^1))$ by Claim 101

$$Q_k^{ext} = \bigcup_{\mathbf{a}_0 \in \mathbb{D}_k^{ext}} R'_{ext}(\mathbf{a}_0), \tag{164}$$

where

$$\begin{aligned}\mathbb{D}_k^{ext} &= (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}_0'} \cap \prod_{\mathbf{i} \in \mathbf{I}_0'} [\mathbf{u}_\mathbf{i}^0, \mathbf{v}_\mathbf{i}^0) \\ &\subseteq (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}_0'} \cap \prod_{\mathbf{i} \in \mathbf{I}_0'} [\mathbf{u}_\mathbf{i}, \mathbf{v}_\mathbf{i}) \\ &= \mathbb{D}_k,\end{aligned}$$

as required. The first transition is by Claim (101). The second transition is due to the fact that $Q_k^{ext} \subseteq T_*'$ since F is consistent with T_*' by assumption, and hence $Q_k^{ext} \subseteq T_k'$. The last transition is by definition of $\mathbb{D}_k$.

We let $\gamma = \Delta^{|\mathbf{I}_0'|} \cdot \prod_{\mathbf{i} \in \mathbf{I}_1'} (\mathbf{d}_\mathbf{i} - \mathbf{c}_\mathbf{i}) = \Delta^{|\mathbf{I}_0|} \cdot \prod_{\mathbf{i} \in \mathbf{I}_1} (\mathbf{d}_\mathbf{i} - \mathbf{c}_\mathbf{i})$ and invoke Lemma 102. By Lemma 102, **(1)**, we get

$$(1 - \sqrt{\epsilon})\gamma \leq \left| R'_{ext}(\mathbf{a}_0) \right| / m^n \leq (1 + \sqrt{\epsilon})\gamma, \tag{165}$$

and

$$(1 - \sqrt{\epsilon})\gamma \leq \left| R_{ext}(\mathbf{a}_0) \right| / m^n \leq (1 + \sqrt{\epsilon})\gamma. \tag{166}$$

Fix some $\mathbf{a}_0 \in \mathbb{D}_k$. We write R'_{ext} and R_{ext} to denote $R'_{ext}(\mathbf{a}_0)$ and $R_{ext}(\mathbf{a}_0)$, and write R' and R to denote $R'(\mathbf{a}_0)$ and $R(\mathbf{a}_0)$, omitting the dependence on $\mathbf{a}_0$ to simplify notation, when $\mathbf{a}_0$ is fixed. By Lemma 120, **(1)** we have

$$\Pi_k^*(\text{Int}_\delta(R'_{ext})) \subseteq R_{ext}. \tag{167}$$

At the same time by Lemma 106 we have

$$|\text{Int}_\delta(R'_{ext})| \geq (1 - \sqrt{\delta})|R'_{ext}|, \tag{168}$$

and by Lemma 102 one has $|R_{ext}| \leq (1 + 3\sqrt{\epsilon})|R'_{ext}|$. Putting these bounds together with (167) and using the fact that ϵ is smaller than δ by a large enough absolute constant by (p6), we get, writing $\text{Dom}(\Pi_k^*)$ to denote the domain of Π_k^*,

$$\begin{aligned}|R_{ext} \setminus \Pi_k^*(\text{Int}_\delta(R'_{ext}))| &\leq |R_{ext}| - |R'_{ext}| + |R'_{ext} \setminus \text{Int}_\delta(R'_{ext})| + |R'_{ext} \setminus \text{Dom}(\Pi_k^*)| \\ &\leq 3\sqrt{\epsilon}|R'_{ext}| + |R'_{ext} \setminus \text{Int}_\delta(R'_{ext})| + |R'_{ext} \setminus \text{Dom}(\Pi_k^*)| \\ &\leq (3\sqrt{\epsilon} + \sqrt{\delta})|R'_{ext}| + |R'_{ext} \setminus \text{Dom}(\Pi_k^*)|.\end{aligned} \tag{169}$$

We now bound $|R'_{ext} \setminus \text{Dom}(\Pi_k^*)|$. By Lemma 120, **(2)** we have

$$\begin{aligned}|R'_{ext} \setminus \text{Dom}(\Pi_k^*)| &\leq |R' \setminus \text{Dom}(\Pi_k^*)| \\ &\leq 8\sqrt{\epsilon}|R'| \\ &\leq 8\sqrt{\epsilon}\Delta^{-2K^2}|R'_{ext}|,\end{aligned}$$

where we used the fact that $|R'_{ext}| \geq \Delta^{2K^2} \cdot |R'|$ by Lemma 102, **(1)**, together with the fact that $|\Psi(\mathbf{B}^\ell)| \leq KL \leq K^2$. Substituting this into (169), we get

$$\begin{aligned}|R_{ext} \setminus \Pi_k^*(\text{Int}_\delta(R'_{ext}))| &\leq (3\sqrt{\epsilon} + \sqrt{\delta} + 8\sqrt{\epsilon}\Delta^{-2K^2})|R'_{ext}| \\ &\leq 2\sqrt{\delta}|R'_{ext}|\end{aligned} \tag{170}$$

by (p5) and (p6). At the same time, we have by Lemma 106 and (167)

$$|\Pi_k^*(R'_{ext}) \setminus R_{ext}| \leq |R'_{ext} \setminus \text{Int}_\delta(R'_{ext})| \leq \sqrt{\delta}|R'_{ext}|. \tag{171}$$

We now note that $\mathbf{I}_0 = \Psi(\mathbf{B}^\ell)$ as per (159) and $\mathsf{M}(\mathbf{a}_0)$ is consistent with T_* by definition of the map M (see (135) and (134)). Thus, the inductive hypothesis applies to the rectangle R_{ext} (the rhs of (167)), and we get

$$(\ln 2 - C/K)^{j-1}|R_{ext}| \leq |\nu_{\ell-1,j-1}(R_{ext})| \leq (\ln 2 + C/K)^{j-1}|R_{ext}|, \tag{172}$$

and hence, using the first inequality above together with (170),

$$\begin{aligned} |\nu_{\ell-1,j-1}(\Pi_k^*(R'_{ext}))| &\geq |\nu_{\ell-1,j-1}(R_{ext})| - |\nu_{\ell-1,j-1}(R_{ext} \setminus \Pi_k^*(\text{Int}_\delta(R'_{ext})))| \\ &\geq |\nu_{\ell-1,j-1}(R_{ext})| - K^{j-1} \cdot 2\sqrt{\delta} \cdot |R'_{ext}| \\ &\geq (\ln 2 - C/K)^{j-1} \cdot |R_{ext}| - \delta^{1/4} \cdot |R'_{ext}| \\ &\geq ((\ln 2 - C/K)^{j-1}(1 - 3\sqrt{\epsilon}) - \delta^{1/4}) \cdot |R'_{ext}|, \end{aligned} \tag{173}$$

where the transition from the first line to the second is because for every ℓ' the map $\tau^{\ell'}$ maps no vertex in S' to more than $K/2$ vertices in T_*, and in particular $\nu_{\ell-1,j-1}$ maps no vertex in $S^{\ell-1}$ to more than $(K/2)^{j-1}$ vertices in $T_*^{\ell-j}$ (note that we are using the looser bound of K^j on the product of these two bounds to simplify notation). The transition to the second to last line uses the fact that $K^{j-1}2\sqrt{\delta} \leq \delta^{1/4}$ by (p5). The transition to the last line uses (165) and (166). Using the second inequality in (172) together with (171), we similarly get

$$\begin{aligned} |\nu_{\ell-1,j-1}(\Pi_k^*(R'_{ext}))| &\leq |\nu_{\ell-1,j-1}(R_{ext})| + |\nu_{\ell-1,j-1}(\Pi_k^*(R'_{ext}) \setminus R_{ext})| \\ &\leq |\nu_{\ell-1,j-1}(R_{ext})| + K^{j-1} \cdot 2\sqrt{\delta} \cdot |R'_{ext}|, \\ &\leq (\ln 2 + C/K)^{j-1} \cdot |R_{ext}| + \delta^{1/4} \cdot |R'_{ext}| \\ &\leq ((\ln 2 + C/K)^{j-1} \cdot (1 + 3\sqrt{\epsilon}) + \delta^{1/4}) \cdot |R'_{ext}|, \end{aligned} \tag{174}$$

where the transition from the first line to the second is because for any ℓ' the map $\tau^{\ell'}$ maps no vertex in S' to more than $K/2$ vertices in T_*, and in particular $\nu_{\ell-1,j-1}$ maps no vertex in $S^{\ell-1}$ to more than $(K/2)^{j-1}$ vertices in $T_*^{\ell-j}$, as well as the fact that $\Pi_k^*(R'_{ext}) \setminus R_{ext} \subseteq \Pi_k^*(R'_{ext} \setminus \text{Int}_\delta(R'_{ext}))$ by (167). The transition to the second to last line uses the fact that $K^{j-1}2\sqrt{\delta} \leq \delta^{1/4}$ by (p5). The transition to the last line uses (165) and (166).

Putting (173) together with (164) and (155), and recalling that $R'_{ext} = R'_{ext}(\mathbf{a}_0)$, we get for the lower bound

$$\begin{aligned} |\nu_{\ell,j}(F))| &= \sum_{k \in [K/2]} |\nu_{\ell-1,j-1}(\tau(\text{DOWNSET}_k(F)))| \\ &= \sum_{k \in [K/2]} |\nu_{\ell-1,j-1}(\Pi_k^*(\rho_k(\text{DOWNSET}_k(F)))| \\ &\geq (1 - \delta^{1/4}) \sum_{k \in [K/2]} |\nu_{\ell-1,j-1}(\Pi_k^*(Q_k^{ext}))| \\ &= (1 - \delta^{1/4}) \sum_{k \in [K/2]} \sum_{\mathbf{a}_0 \in \mathbb{D}_k^{ext}} |\nu_{\ell-1,j-1}(\Pi_k^*(R'_{ext}(\mathbf{a}_0)))| \\ &\geq \sum_{k \in [K/2]} ((\ln 2 - C/K)^{j-1}(1 - 3\sqrt{\epsilon}) - \delta^{1/4}) \sum_{\mathbf{a}_0 \in \mathbb{D}_k^{ext}} |R'_{ext}(\mathbf{a}_0)| \\ &\geq ((\ln 2 - C/K)^{j-1}(1 - 3\sqrt{\epsilon}) - 3\delta^{1/4}) \sum_{k \in [K/2]} |Q_k^{ext}|. \end{aligned} \tag{175}$$

The first transition uses the fact that τ is injective by Claim 126, $\nu_{\ell-1,j-1}$ is injective by Lemma 135, **(1)**, and $\textsc{DownSet}_k(F) \cap \textsc{DownSet}_{k'}(F) = \emptyset$ for $k \neq k'$. The second transition uses the definition of τ (see Definition 125). The third transition uses (155) and the last transition uses (164). For the upper bound we get using (174)

$$\begin{aligned}
|\nu_{\ell,j}(F)| &= \sum_{k\in[K/2]} |\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_k(F)))| \\
&= \sum_{k\in[K/2]} |\nu_{\ell-1,j-1}(\Pi_k^*(\rho_k(\textsc{DownSet}_k(F)))| \\
&\leq (1+\delta^{1/4}) \sum_{k\in[K/2]} |\nu_{\ell-1,j-1}(\Pi_k^*(Q_k^{ext}))| \\
&= (1+\delta^{1/4}) \sum_{k\in[K/2]} \sum_{\mathbf{a}_0\in\mathbb{D}_k^{ext}} |\nu_{\ell-1,j-1}(\Pi_k^*(R'_{ext}(\mathbf{a}_0)))| \\
&\leq ((\ln 2 + C/K)^{j-1}(1+3\sqrt{\epsilon}) + 3\delta^{1/4}) \sum_{k\in[K/2]} \sum_{\mathbf{a}_0\in\mathbb{D}_k^{ext}} |R'_{ext}(\mathbf{a}_0)| \\
&= ((\ln 2 + C/K)^{j-1}(1+3\sqrt{\epsilon}) + 3\delta^{1/4}) \sum_{k\in[K/2]} |Q_k^{ext}|,
\end{aligned} \tag{176}$$

where the third transition uses (155) and the last transition uses (164).

Step 3: putting it together. For the lower bound we have by (175) and the fact that $|Q_k^{ext}| \geq (1 - 3\sqrt{\epsilon})\frac{1}{K-k}|F|$ by (154)

$$\begin{aligned}
|\nu_{\ell,j}(F))| &\geq ((\ln 2 - C/K)^{j-1}(1-3\sqrt{\epsilon}) - \delta^{1/4}) \sum_{k\in[K/2]} |Q_k^{ext}| \\
&\geq ((\ln 2 - C/K)^{j-1}(1-3\sqrt{\epsilon}) - \delta^{1/4}) \cdot \sum_{k\in[K/2]} (1-3\sqrt{\epsilon})\frac{1}{K-k} \cdot |F| \\
&= ((\ln 2 - C/K)^{j-1}(1-3\sqrt{\epsilon}) - \delta^{1/4}) \cdot (1-3\sqrt{\epsilon}) \cdot |F| \cdot \sum_{k\in[K/2]} \frac{1}{K-k} \\
&\geq ((\ln 2 - C/K)^{j-1}(1-3\sqrt{\epsilon}) - \delta^{1/4}) \cdot (1-3\sqrt{\epsilon})(\ln 2 - 1/K)|F| \\
&\geq (\ln 2 - C/K)^{j}|F|.
\end{aligned} \tag{177}$$

The second to last transition is by Claim 25. The last transition used the fact that $\sum_{k\in[K/2]} \frac{1}{K-k} \geq \ln 2 - 1/K$ by Claim 25 and our choice of C as a sufficiently large absolute constant, as well as the fact that $\delta < K^{-10}$ and $\epsilon < K^{-10}$ by (p4) and (p5) together with the fact that $\Delta \leq 1/K$ by (p3) and the fact that K is larger than an absolute constant.

For the upper bound we get using (174) and the fact that $|Q_k^{ext}| \leq (1+3\sqrt{\epsilon})\frac{1}{K-k}|F|$ by (154)

$$\begin{aligned}
|\nu_{\ell,j}(F)| &\leq ((\ln 2 + C/K)^{j-1}(1+3\sqrt{\epsilon}) + \delta^{1/4}) \sum_{k\in[K/2]} |Q_k^{ext}| \\
&\leq ((\ln 2 + C/K)^{j-1}(1+3\sqrt{\epsilon}) + \delta^{1/4}) \sum_{k\in[K/2]} (1+3\sqrt{\epsilon})\frac{1}{K-k}\cdot|F| \\
&= ((\ln 2 + C/K)^{j-1}(1+3\sqrt{\epsilon}) + \delta^{1/4})(1+3\sqrt{\epsilon})\cdot|F|\cdot \sum_{k\in[K/2]} \frac{1}{K-k} \\
&\leq ((\ln 2 + C/K)^{j-1}(1+3\sqrt{\epsilon}) + \delta^{1/4})(1+3\sqrt{\epsilon})(\ln 2)\cdot|F| \\
&= (\ln 2 + C/K)^{j}\cdot|F|
\end{aligned}$$

The second to last transition is by Claim 25. The last transition used the fact that $\sum_{k\in[K/2]}\frac{1}{K-k} \leq \ln 2$ by Claim 25 and our choice of C, as well as the fact that $\delta < K^{-10}$ and $\epsilon < K^{-10}$ by (p4) and (p5) together with the fact that $\Delta \leq 1/K$ by (p3) and the fact that K is larger than an absolute constant. This completes the proof of the inductive step, and establishes the claim of the lemma. ■

Corollary 139 *There exists an absolute constant $C > 0$ such that for every $\ell \in [L]$, every $j = 0,\ldots,\ell$, if $\mathbf{I} = \Psi(\mathbf{B}^{\ell})$ and $\mathbf{H} \subseteq \Psi(\mathbf{B}^{>\ell})$, the following conditions hold.*

For every $\mathbf{c},\mathbf{d} \in \Delta\cdot\mathbb{Z}\cap[0,1]^{\mathbf{I}\cup\mathbf{H}}, \mathbf{c} < \mathbf{d}$, such that $\textsc{Rect}(\mathbf{I},\mathbf{c}_{\mathbf{I}},\mathbf{d}_{\mathbf{I}}) \subseteq T_*^{\ell}$ the rectangle $F = \textsc{Rect}(\mathbf{I}\cup\mathbf{H},\mathbf{c},\mathbf{d})$ satisfies

$$(\ln 2 - C/K)^j|F| \leq |\nu_{\ell,j}(F)| \leq (\ln 2 + C/K)^j|F|$$

for an absolute constant $C > 0$.

Proof: One has by Claim 101

$$F = \textsc{Rect}(\mathbf{I}\cup\mathbf{H},\mathbf{c},\mathbf{d}) = \bigcup_{\mathbf{a}\in Q} F(\mathbf{a}), \tag{178}$$

where $Q = (\Delta\cdot\mathbb{Z}\cap[0,1])^{\mathbf{I}}\cap\textsc{Rect}(\mathbf{I},\mathbf{c}_{\mathbf{I}},\mathbf{d}_{\mathbf{I}})$ and

$$F(\mathbf{a}) = \textsc{Rect}(\mathbf{I}\cup\mathbf{H},(\mathbf{a},\mathbf{c}_{\mathbf{H}}),(\mathbf{a}+\Delta\cdot\mathbf{1},\mathbf{d}_{\mathbf{H}})).$$

Since $\textsc{Rect}(\mathbf{I},\mathbf{c}_{\mathbf{I}},\mathbf{d}_{\mathbf{I}}) \subseteq T_*^{\ell}$ by assumption, we get that every $\mathbf{f}\in Q$ is consistent with T_*^{ℓ}. Thus, Lemma 138 applies, and we get

$$(\ln 2 - C/K)^j|F(\mathbf{a})| \leq |\nu_{\ell,j}(F(\mathbf{a}))| \leq (\ln 2 + C/K)^j|F(\mathbf{a})|.$$

Substituting the above into (178), using the fact that $F(\mathbf{a})\cap F(\mathbf{a}') = \emptyset$ for $\mathbf{a}\neq\mathbf{a}'$ as well as the fact that $\nu_{\ell,j}$ is injective by Lemma 61, **(1)**, gives the result. ■

Finally, we give

Proof of Lemma 132: We start by noting that by Definition 130

$$\nu_{\ell,j+1}(T^{\ell}\setminus T_*^{\ell}) = \tau^{\ell-j}(\textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^{\ell}\setminus T_*^{\ell}))) = \tau^{\ell-j}(\mu_{\ell,j}(T^{\ell}\setminus T_*^{\ell})).$$

This means, using injectivity of $\tau^{\ell-j}$, that

$$\begin{aligned}
\Big||\mu_{\ell,j}(T^{\ell}\setminus T_*^{\ell})| - |\nu_{\ell,j+1}(T^{\ell}\setminus T_*^{\ell})|\Big| &\leq |\{y\in S^{\ell-j} : \tau^{\ell-j}(y) = \bot\}| \\
&\leq \delta^{1/4}|T|
\end{aligned}$$

by Lemma 128[6]. We have $\delta \leq K^{-100K^2}$ by (p3) and (p5), and therefore $\delta^{1/4} \leq K^{-25K^2} \leq K^{-100} \cdot (\ln 2)^L$, as $L \leq \sqrt{K}$ by (p4). This means that the above contributes a low order term to the final bound, and it suffices to prove that for every $\ell \in [L]$, every $j = 1, \ldots, \ell + 1$, one has

$$\frac{1}{2}(1 - \ln 2)(\ln 2 - C/K)^{j-1}|T_0| \leq |\nu_{\ell,j}(T^\ell \setminus T^\ell_*)| \leq \frac{1}{2}(1 - \ln 2)(\ln 2 + C/K)^{j-1}|T_0| \tag{179}$$

for an absolute constant $C > 0$. Note the power of $j - 1$ as opposed to j (this comes from the fact that we are using $\nu_{\ell,j}$ as a proxy for $\mu_{\ell,j-1}$, as per the argument above).

We let $\mathbf{J}' := \mathbf{J}^\ell$, $\mathbf{J} := \mathbf{J}^{\ell-1}$, $\mathbf{B}' := \mathbf{B}^\ell$, $\mathbf{B} := \mathbf{B}^{\ell-1}$ to simplify notation. Similarly define $T' := T^\ell$, $T := T^{\ell-1}$ and $S' := S^\ell$, $S := S^{\ell-1}$ to simplify notation. Let $\mathbf{r}' := \mathbf{r}^\ell, \mathbf{r} := \mathbf{r}^{\ell-1}$ denote the ℓ-th and the $(\ell-1)$-th compression indices respectively. We write

$$T' \setminus T'_* = \bigcup_{k=0}^{K/2-1} T'_k \setminus T'_{k+1},$$

and note that

$$\nu_{\ell,j}(T' \setminus T'_*) = \bigcup_{k=0}^{K/2-1} \nu_{\ell,j}(T'_k \setminus T'_{k+1}).$$

We now fix $k \in [K/2]$ and note that

$$\nu_{\ell,j}(T_k \setminus T_{k+1}) = \bigcup_{s=0}^{k} \nu_{\ell-1,j-1}(\tau^\ell(\textsc{DownSet}^\ell_s(T_k \setminus T_{k+1}))), \tag{180}$$

where we used Definition 87 and Remark 89. Also note that the sets on the rhs are disjoint since $\nu_{\ell-1,j-1}$ is injective by Lemma 135, **(1)**, τ^ℓ is injective by Claim 126 and $\textsc{DownSet}^\ell_s$ is injective by construction (Definition 87). In what follows we bound the cardinality of

$$\nu_{\ell-1,j-1}(\tau^\ell(\textsc{DownSet}^\ell_s(T \setminus T_*))$$

for fixed $k \in [K/2]$ and $s \in \{0, 1, \ldots, k\}$, and then put these bounds together to achieve the final result of the lemma.

Step 1. Define

$$Z_s := \left\{x \in [m]^n : \mathrm{wt}(x) \in \left[0, \frac{1}{K-s}\right) \cdot W \pmod{W}\right\}. \tag{181}$$

Also recall that by (99)

$$\begin{aligned} T'_k \setminus T'_{k+1} &= \left\{x \in T'_k : \langle x, \mathbf{j}'_k\rangle \pmod{M} \in \left[1 - \frac{1}{K-k}, 1\right) \cdot M\right\} \\ &= \left\{x \in [m]^n : \langle x, \mathbf{j}'_i\rangle \pmod{M} \in \left[0, 1 - \frac{1}{K-i}\right) \cdot M \text{ for all } i = 0, \ldots, k-1 \right. \\ &\qquad \left. \text{and } \langle x, \mathbf{j}'_k\rangle \pmod{M} \in \left[1 - \frac{1}{K-k}, 1\right) \cdot M\right\} \end{aligned} \tag{182}$$

We let

$$Q_k := T'_k \setminus T'_{k+1} \tag{183}$$

[6] Note that for convenience of notation in the corner case $j = \ell$ we imagine adding a pair of sets (T^{-1}, S^{-1}) and a corresponding map $\tau^0 : S^0 \to T^{-1}_*$ so that we can talk about $\nu_{\ell,j+1}$ for all $j = 0, \ldots, \ell$.

and, writing $\mathbf{q}'_s := \mathbf{q}^{\ell}_s$ for $s = 0, 1, \ldots, k$, to simplify notation, let

$$Q_{k,s} := \left\{ x \in Q_k : \langle x, \mathbf{q}'_s \rangle \pmod{M} \in \left[0, \frac{1}{K-s}\right) \cdot M \right\}. \tag{184}$$

Let ρ_s be the $(K - s, \mathbf{q}'_s)$-densifying map as per Definition 115. Now by Lemma 116 we have

$$\rho_s \left(\text{Int}_\delta \left(Q_k \cap Z_s \right) \right) \subseteq Q_{k,s}. \tag{185}$$

We start by noting that

$$\begin{aligned} |\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_s(Q_k)))| &= |\nu_{\ell-1,j-1}(\tau(Q_k \cap Z_s))| \\ &= |\nu_{\ell-1,j-1}(\Pi^*_s(\rho_s(Q_k \cap Z_s)))| \\ &\geq |\nu_{\ell-1,j-1}(\Pi^*_s(Q_{k,s}))| - |\nu_{\ell-1,j-1}(\Pi^*_s(Q_{k,s} \setminus \rho_s(Q_k \cap Z_s)))| \\ &\geq |\nu_{\ell-1,j-1}(\Pi^*_s(Q_{k,s}))| - K^{j-1}|Q_{k,s} \setminus \rho_s(Q_k \cap Z_s)|. \end{aligned} \tag{186}$$

The first transition above is by Definition 87, the second transition is by Definition 125, and the forth transition uses the fact that Π^*_s maps every vertex to at most one vertex, as well as the fact that $\nu_{\ell-1,j-1}$ maps every vertex to at most K^{j-1} vertices. Similarly,

$$\begin{aligned} |\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_s(Q_k)))| &= |\nu_{\ell-1,j-1}(\tau(Q_k \cap Z_s))| \\ &= |\nu_{\ell-1,j-1}(\Pi^*_s(\rho_s(Q_k \cap Z_s)))| \\ &\leq |\nu_{\ell-1,j-1}(\Pi^*_s(Q_{k,s}))| + |\nu_{\ell-1,j-1}(\Pi^*_s(\rho_s(Q_k \cap Z_s) \setminus Q_{k,s}))| \\ &\leq |\nu_{\ell-1,j-1}(\Pi^*_s(Q_{k,s}))| + K^{j-1}|\rho_s(Q_k \cap Z_s) \setminus Q_{k,s}|. \end{aligned} \tag{187}$$

The first transition above is by Definition 87, the second transition is by Definition 125, and the forth transition uses the fact that Π^*_s maps every vertex to at most one vertex, as well as the fact that $\nu_{\ell-1,j-1}$ maps every vertex to at most K^{j-1} vertices.

Step 1. We now upper bound $Q_{k,s} \setminus \rho_s(Q_k \cap Z_s)$ and $\rho_s(Q_k \cap Z_s) \setminus Q_{k,s}$, which allows us to upper bound the error terms in (186) and (187) respectively. We first apply Lemma 102, **(1)**, to Q_k and $Q_{k,s}$, and Lemma 102, **(2)**, to $Q_k \cap Z_k$ with

$$\gamma := \left(\prod_{i=0}^{k-1} \left(1 - \frac{1}{K-i} \right) \right) \frac{1}{K-k} = \frac{1}{K}.$$

The resulting bounds are

$$\begin{aligned} |Q_k|/m^n &= (1 \pm \sqrt{\epsilon})\gamma = (1 \pm \sqrt{\epsilon})\frac{1}{K} \\ |Q_{k,s}|/m^n &= (1 \pm \sqrt{\epsilon})\frac{1}{K-s}\gamma = (1 \pm \sqrt{\epsilon})\frac{1}{K-s} \cdot \frac{1}{K} \\ |Q_k \cap Z_s|/m^n &= (1 \pm \sqrt{\epsilon})\frac{1}{K-s} \cdot \gamma = (1 \pm \sqrt{\epsilon})\frac{1}{K-s} \cdot \frac{1}{K}. \end{aligned} \tag{188}$$

We thus get, using (185) together with the fact that ρ_s is injective,

$$\begin{aligned} |Q_{k,s} \setminus \rho_s(Q_k \cap Z_s)| &\leq |Q_{k,s}| - |\text{Int}_\delta(Q_k) \cap Z_s| \\ &\leq |Q_{k,s}| - |Q_k \cap Z_s| + |Q_k \setminus \text{Int}_\delta(Q_k)| \\ &\leq (1 + 3\sqrt{\epsilon})\frac{1}{K-s}|Q_k| - (1 - \sqrt{\epsilon})\frac{1}{K-s}|Q_k| + \sqrt{\delta}|Q_k| \\ &\leq (4\sqrt{\epsilon} + K\sqrt{\delta})|Q_{k,s}| \end{aligned} \tag{189}$$

Similarly, since ρ_s is injective,

$$\begin{aligned} |\rho_s(Q_k \cap Z_s) \setminus Q_{k,s}| &\leq |\rho_s(Q_k \setminus \mathrm{Int}_\delta(Q_k))| \\ &\leq \sqrt{\delta}|Q_k| \\ &\leq K\sqrt{\delta}|Q_{k,s}|, \end{aligned} \tag{190}$$

where we used Lemma 106 in the second transition.

Substituting the two bounds above into (186) and (187) respectively and noting that $K^j \cdot \sqrt{\delta} \leq \delta^{1/4}$ by (p5) together with (p3) and the fact that K is larger than an absolute constant, we get

$$|\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_s(Q_k))| \geq |\nu_{\ell-1,j-1}(\Pi^*_s(Q_{k,s}))| - \delta^{1/4}|Q_{k,s}| \tag{191}$$

and

$$|\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_s(Q_k))| \leq |\nu_{\ell-1,j-1}(\Pi^*_s(Q_{k,s}))| + \delta^{1/4}|Q_{k,s}|. \tag{192}$$

Step 2. Define

$$\begin{aligned} \mathbf{I}'_0 &= \mathbf{J}'_{<k} \cup \mathrm{Ext}'_k \cup \{\mathbf{q}'_k\} \\ \mathbf{I}'_1 &= \mathbf{J}'_{\geq k} \cup \{\mathbf{r}'\} \end{aligned}$$

and $\mathbf{I}' = \mathbf{I}'_0 \cup \mathbf{I}'_1$, as well as

$$\begin{aligned} \mathbf{I}_0 &= \mathbf{J} \cup \{\mathbf{r}\} \\ \mathbf{I}_1 &= \mathbf{I}'_1 \end{aligned} \tag{193}$$

and $\mathbf{I} = \mathbf{I}_0 \cup \mathbf{I}_1$. Recall that by Definition 121 together with (130) and Definition 121 for $k \in [K/2]$ the set $\mathbb{D}_k$ is a subset of $(\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'_0}$ such that

$$\left\{x \in T'_k : \langle x, \mathbf{q}_k\rangle \pmod{M} \in \left[0, \frac{1}{K-k}\right) \cdot M\right\} = \bigcup_{\mathbf{d} \in \mathbb{D}_k} \textsc{Rect}(\mathbf{I}'_0, \mathbf{d}).$$

We now recall the definition of $\mathbb{D}_k$ (see Definition 121). Indeed, let $\mathbf{u}_{\mathbf{j}'_s} = 0, \mathbf{v}_{\mathbf{j}'_s} = 1 - \frac{1}{K-s}$ for $s \in [k]$, let $\mathbf{u}_{\mathbf{q}_k} = 0, \mathbf{v}_{\mathbf{q}_k} = \frac{1}{K-k}$, and $\mathbf{u}_{\mathbf{i}} = 0, \mathbf{v}_{\mathbf{i}} = 1$ for $\mathbf{i} \in \mathrm{Ext}_k$. Then, noting that $\mathbf{I}'_0$ as per (158) is equal to $\mathbf{I}'$ as per (130) one has as per (132)

$$\mathbb{D}_k = (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}'_0} \cap \prod_{\mathbf{i} \in \mathbf{I}'_0} [\mathbf{u}_{\mathbf{i}}, \mathbf{v}_{\mathbf{i}}). \tag{194}$$

We now note that $Q_{k,s}$ is a rectangle in $\mathbf{I}'_0 \cup \mathbf{I}'_1$. Indeed, let

$$\begin{aligned} &\mathbf{u}^0_{\mathbf{j}'_i} = 0, \mathbf{v}^0_{\mathbf{j}'_i} = 1 - \frac{1}{K-i} \qquad \text{for } i \in [s] \\ &\mathbf{u}^0_{\mathbf{q}_s} = 0, \mathbf{v}^0_{\mathbf{q}_s} = \frac{1}{K-k} \\ &\text{and} \\ &\mathbf{u}^0_{\mathbf{i}} = 0, \mathbf{v}^0_{\mathbf{i}} = 1 \quad \text{for } \mathbf{i} \in \mathrm{Ext}'_s, \end{aligned}$$

so that $\mathbf{u}^0, \mathbf{v}^0 \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'_0}$. Also let

$$\begin{aligned} &\mathbf{u}^1_{\mathbf{j}'_i} = 0, \mathbf{v}^1_{\mathbf{j}'_i} = 1 - \frac{1}{K-i} \qquad \text{for } i \in \{s, s+1, \ldots, k-1\}, \\ &\mathbf{u}^1_{\mathbf{j}'_k} = 1 - \frac{1}{K-k}, \mathbf{v}^1_{\mathbf{j}'_k} = 1, \\ &\mathbf{u}^1_{\mathbf{j}'_i} = 0, \mathbf{v}^1_{\mathbf{j}'_i} = 1 \quad \text{for } i \in \{k, k+1, \ldots, K/2\} \\ &\mathbf{u}^1_{\mathbf{r}'_k} = 0, \mathbf{v}^1_{\mathbf{r}'_k} = 1, \end{aligned}$$

so that $\mathbf{u}^1, \mathbf{v}^1 \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'_1}$. We have $Q_{k,s} = \textsc{Rect}(\mathbf{I}'_0 \cup \mathbf{I}'_1, (\mathbf{u}^0, \mathbf{u}^1), (\mathbf{v}^0, \mathbf{v}^1))$, and hence using Claim 101 we get

$$Q_{k,s} = \bigcup_{\substack{\mathbf{a}=(\mathbf{a}_0,\mathbf{a}_1)\\ \mathbf{a}_0 \in \mathbb{D}_{k,s}, \mathbf{a}_1 \in \mathbb{D}^{ext}_{k,s}}} R'_{ext}(\mathbf{a}). \tag{195}$$

We have

$$\begin{aligned}\mathbb{D}_{k,s} &= (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}'_0} \cap \prod_{\mathbf{i} \in \mathbf{I}'_0} [\mathbf{u}^0_{\mathbf{i}}, \mathbf{v}^0_{\mathbf{i}}) \\ &\subseteq (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}'_0} \cap \prod_{\mathbf{i} \in \mathbf{I}'_0} [\mathbf{u}_{\mathbf{i}}, \mathbf{v}_{\mathbf{i}}) \\ &= \mathbb{D}_k,\end{aligned} \tag{196}$$

and

$$\mathbb{D}^{ext}_{k,s} = (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}'_0} \cap \prod_{\mathbf{i} \in \mathbf{I}'_1} [\mathbf{u}^1_{\mathbf{i}}, \mathbf{v}^1_{\mathbf{i}}).$$

The first transition in (196) is by Claim (101). The second transition is due to the fact that $Q_{k,s} \subseteq T'_k$ by (183) and (184). The last transition is by definition of $\mathbb{D}_k$.

For $\mathbf{a} \in Q_k$ we write $\mathbf{a}_0$ to denote the restriction of $\mathbf{a}$ to $\mathbf{I}'_0$, $\mathbf{a}_1$ to denote the restriction of $\mathbf{a}$ to $\mathbf{I}'_1$. Let $M : \mathbb{D}_k \to \mathbb{A}$ denote the map that defines τ (see Definition 125, Definition 124 and (135)). For $\mathbf{a}_0 \in \Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{I}'_0}$ let

$$\begin{gathered} R'(\mathbf{a}_0) = \textsc{Rect}(\mathbf{I}'_0, \mathbf{a}_0, \mathbf{a}_0 + \Delta \cdot \mathbf{1}) \\ \text{and} \\ R(\mathbf{a}_0) = \textsc{Rect}(\mathbf{I}_0, \mathsf{M}(\mathbf{a}_0), \mathsf{M}(\mathbf{a}_0) + \Delta \cdot \mathbf{1}).\end{gathered}$$

We also define extended rectangles by letting for $\mathbf{a} = (\mathbf{a}_0, \mathbf{a}_1) \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'} = (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}'_0 \cup \mathbf{I}'_1}$

$$\begin{gathered} R'_{ext}(\mathbf{a}) = \textsc{Rect}(\mathbf{I}'_0 \cup \mathbf{I}'_1, ((\mathbf{a}_0, \mathbf{a}_1), (\mathbf{a}_0 + \Delta \cdot \mathbf{1}, \mathbf{a}_1 + \Delta \cdot \mathbf{1}))) \\ \text{and} \\ R_{ext}(\mathbf{a}) = \textsc{Rect}(\mathbf{I}_0 \cup \mathbf{I}_1, ((\mathsf{M}(\mathbf{a}_0), \mathbf{a}_1), (\mathsf{M}(\mathbf{a}_0) + \Delta \cdot \mathbf{1}, \mathbf{a}_1 + \Delta \cdot \mathbf{1}))).\end{gathered} \tag{197}$$

By Lemma 120, **(1)** we have, omitting the dependence on $\mathbf{a}$ to simplify notation while $\mathbf{a}$ is fixed,

$$\Pi^*_s(\text{Int}_\delta(R'_{ext})) \subseteq R_{ext}. \tag{198}$$

At the same time by Lemma 106 we have

$$|\text{Int}_\delta(R'_{ext})| \geq (1 - \sqrt{\delta})|R'_{ext}|, \tag{199}$$

and by Lemma 102 one has $|R_{ext}| \leq (1 + 3\sqrt{\epsilon})|R'_{ext}|$.

$$\begin{aligned}|R_{ext} \setminus \Pi^*_s(\text{Int}_\delta(R'_{ext}))| &\leq |R_{ext}| - |R'_{ext}| + |R'_{ext} \setminus \text{Int}_\delta(R'_{ext})| + |R'_{ext} \setminus \text{Dom}(\Pi^*_s)| \\ &\leq 3\sqrt{\epsilon}|R'_{ext}| + |R'_{ext} \setminus \text{Int}_\delta(R'_{ext})| + |R'_{ext} \setminus \text{Dom}(\Pi^*_s)| \\ &\leq (3\sqrt{\epsilon} + \sqrt{\delta})|R'_{ext}| + |R'_{ext} \setminus \text{Dom}(\Pi^*_s)|\end{aligned} \tag{200}$$

We now bound $|R'_{ext} \setminus \text{Dom}(\Pi^*_s)|$. By Lemma 120, **(2)** we have

$$\begin{aligned}|R'_{ext} \setminus \text{Dom}(\Pi^*_k)| &\leq |R' \setminus \text{Dom}(\Pi^*_s)| \\ &\leq 8\sqrt{\epsilon}|R'| \\ &\leq 8\sqrt{\epsilon}\Delta^{-2K^2}|R'_{ext}|,\end{aligned}$$

where we used the fact that $|R'_{ext}| \geq \Delta^{2K^2} \cdot |R'|$ by Lemma 102, **(1)**. Substituting this into (200), we get

$$|R_{ext} \setminus \Pi^*_s(\text{Int}_\delta(R'_{ext}))| \leq (3\sqrt{\epsilon} + \sqrt{\delta} + 8\sqrt{\epsilon}\Delta^{-2K^2})|R'_{ext}| \leq 2\sqrt{\delta}|R'_{ext}|, \tag{201}$$

where we used the fact that

$$\begin{aligned}8\sqrt{\epsilon}\Delta^{-2K^2} &\leq 8\delta\Delta^{-2K^2} && \text{(by (p6))} \\ &\leq 8\delta\Delta^{-2K^2} && \text{(by (p5))} \\ &\leq 8\delta^{98/100} && \text{(by (p5)),}\end{aligned}$$

and therefore, since $\sqrt{\epsilon} \leq \delta$ by (p6),

$$3\sqrt{\epsilon} + \sqrt{\delta} + 8\sqrt{\epsilon}\Delta^{-2K^2} \leq 3\delta + \sqrt{\delta} + 8\delta^{98/100} \leq 2\sqrt{\delta}$$

since K is larger than an absolute constant and $\delta < \Delta^{100K^2} \leq K^{100K^2}$ by (p3) together with (p4).

At the same time, we have by Lemma 106

$$|\Pi^*_s(R'_{ext}) \setminus R_{ext}| \leq |R'_{ext} \setminus \text{Int}_\delta(R'_{ext})| \leq \sqrt{\delta}|R'_{ext}|. \tag{202}$$

We summarize these bounds in

$$\begin{gathered}|R_{ext} \setminus \Pi^*_s(R'_{ext})| \leq 2\sqrt{\delta}|R'_{ext}| \\ \text{and} \\ |\Pi^*_s(R'_{ext}) \setminus R_{ext}| \leq 2\sqrt{\delta}|R'_{ext}|\end{gathered} \tag{203}$$

We also note that

$$(1 - 3\sqrt{\epsilon})|R'_{ext}| \leq R_{ext} \leq (1 + 3\sqrt{\epsilon})|R'_{ext}|. \tag{204}$$

Indeed, to obtain the bound above we apply Lemma 102, **(1)** to R_{ext} and R'_{ext}. This gives

$$\begin{aligned}|R'_{ext}|/m^n &= (1 \pm \sqrt{\epsilon})\Delta^{|\mathbf{I}'|} \\ |R_{ext}|/m^n &= (1 \pm \sqrt{\epsilon})\Delta^{|\mathbf{I}|}.\end{aligned} \tag{205}$$

Taking the ratio of the two bounds above and using the fact that $|\mathbf{I}'| = |\mathbf{I}|$ yields (204), as required.

We now note that $\mathbf{I}_0 = \Psi(\mathbf{B})$ as per (193) and $\mathsf{M}(\mathbf{a}_0)$ is consistent with T_* by definition of the map M (see (135) and (134)). Thus, by Lemma 138 applied to the rectangle R_{ext} from (197) we get

$$(\ln 2 - C/K)^{j-1}|R_{ext}| \leq |\nu_{\ell-1,j-1}(R_{ext})| \leq (\ln 2 + C/K)^{j-1}|R_{ext}|. \tag{206}$$

Using the first inequality above together with the first bound in (203), we get

$$\begin{aligned}|\nu_{\ell-1,j-1}(\Pi^*_s(R'_{ext}))| &\geq |\nu_{\ell-1,j-1}(R_{ext})| - |\nu_{\ell-1,j-1}(R_{ext} \setminus \Pi^*_s(\text{Int}_\delta(R'_{ext})))| \\ &\geq |\nu_{\ell-1,j-1}(R_{ext})| - K^{j-1} \cdot 2\sqrt{\delta} \cdot |R'_{ext}| \\ &\geq (\ln 2 - C/K)^{j-1} \cdot |R_{ext}| - \delta^{1/4} \cdot |R'_{ext}| \\ &\geq ((\ln 2 - C/K)^{j-1}(1 - 3\sqrt{\epsilon}) - \delta^{1/4}) \cdot |R'_{ext}|,\end{aligned} \tag{207}$$

where the transition from the first line to the second is because for every ℓ' the map $\tau^{\ell'}$ maps no vertex in S' to more than $K/2$ vertices in T_*, and in particular $\nu_{\ell-1,j-1}$ maps no vertex in $S^{\ell-1}$ to more than $(K/2)^{j-1}$ vertices in $T_*^{\ell-j}$ (note that we are using the looser bound of K^j on the product of these two bounds to simplify notation). The penultimate transition uses the fact that $K^{j-1}2\sqrt{\delta} \leq \delta^{1/4}$ by (p5), and the transition to the last line uses (204). Using the second inequality in (206) together with the second bound in (203), we similarly get

$$\begin{aligned}
|\nu_{\ell-1,j-1}(\Pi_s^*(R'_{ext}))| &\leq |\nu_{\ell-1,j-1}(R_{ext})| + |\nu_{\ell-1,j-1}(\Pi_s^*(R'_{ext}) \setminus R_{ext})| \\
&\leq |\nu_{\ell-1,j-1}(R_{ext})| + K^{j-1} \cdot 2\sqrt{\delta} \cdot |R'_{ext}|, \\
&\leq (\ln 2 + C/K)^{j-1} \cdot |R_{ext}| + \delta^{1/4} \cdot |R'_{ext}| \\
&\leq ((\ln 2 + C/K)^{j-1}(1 + 3\sqrt{\epsilon}) + \delta^{1/4}) \cdot |R'_{ext}|
\end{aligned} \tag{208}$$

where the transition from the first line to the second is because for any ℓ' the map $\tau^{\ell'}$ maps no vertex in S' to more than $K/2$ vertices in T_*, and in particular $\nu_{\ell-1,j-1}$ maps no vertex in $S^{\ell-1}$ to more than $(K/2)^{j-1}$ vertices in $T_*^{\ell-j}$, as well as the fact that $\Pi_s^*(R'_{ext}) \setminus R_{ext} \subseteq \Pi_s^*(R'_{ext} \setminus \text{Int}_\delta(R'_{ext}))$ by (167). The transition to the last line uses the fact that $K^{j-1}2\sqrt{\delta} \leq \delta^{1/4}$ by (p5).

Substituting (207) and (208) respectively into (195), we get

$$\begin{aligned}
|\nu_{\ell-1,j-1}(\Pi_s^*(Q_{k,s}))| &= \sum_{\substack{\mathbf{a}=(\mathbf{a}_0,\mathbf{a}_1) \\ \mathbf{a}_0 \in \mathbb{D}_{k,s}, \mathbf{a}_1 \in \mathbb{D}_{k,s}^{ext}}} |\nu_{\ell-1,j-1}(\Pi_s^*(R'_{ext}(\mathbf{a})))| \\
&\geq \sum_{\substack{\mathbf{a}=(\mathbf{a}_0,\mathbf{a}_1) \\ \mathbf{a}_0 \in \mathbb{D}_{k,s}, \mathbf{a}_1 \in \mathbb{D}_{k,s}^{ext}}} ((\ln 2 - C/K)^{j-1}(1 - 3\sqrt{\epsilon}) - \delta^{1/4}) \cdot |R'_{ext}(\mathbf{a})| \\
&= ((\ln 2 - C/K)^{j-1} - 2\delta^{1/4}) \sum_{\substack{\mathbf{a}=(\mathbf{a}_0,\mathbf{a}_1) \\ \mathbf{a}_0 \in \mathbb{D}_{k,s}, \mathbf{a}_1 \in \mathbb{D}_{k,s}^{ext}}} |R'_{ext}(\mathbf{a})| \\
&= ((\ln 2 - C/K)^{j-1} - 2\delta^{1/4})|Q_{k,s}|.
\end{aligned} \tag{209}$$

and

$$\begin{aligned}
|\nu_{\ell-1,j-1}(\Pi_s^*(Q_{k,s}))| &= \sum_{\substack{\mathbf{a}=(\mathbf{a}_0,\mathbf{a}_1) \\ \mathbf{a}_0 \in \mathbb{D}_{k,s}, \mathbf{a}_1 \in \mathbb{D}_{k,s}^{ext}}} |R'_{ext}(\mathbf{a})| \\
&\leq \sum_{\substack{\mathbf{a}=(\mathbf{a}_0,\mathbf{a}_1) \\ \mathbf{a}_0 \in \mathbb{D}_{k,s}, \mathbf{a}_1 \in \mathbb{D}_{k,s}^{ext}}} ((\ln 2 - C/K)^{j-1}(1 + 3\sqrt{\epsilon}) + \delta^{1/4}) \cdot |R'_{ext}(\mathbf{a})| \\
&= ((\ln 2 + C/K)^{j-1} + 2\delta^{1/4}) \sum_{\substack{\mathbf{a}=(\mathbf{a}_0,\mathbf{a}_1) \\ \mathbf{a}_0 \in \mathbb{D}_{k,s}, \mathbf{a}_1 \in \mathbb{D}_{k,s}^{ext}}} |R'_{ext}(\mathbf{a})| \\
&= ((\ln 2 + C/K)^{j-1} + 2\delta^{1/4})|Q_{k,s}|.
\end{aligned} \tag{210}$$

Step 3. Substituting (209) and (210) into (191) and (211) respectively, and using (205), we get

$$\begin{aligned}
|\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_s(Q_k))| &\geq |\nu_{\ell-1,j-1}(\Pi_s^*(Q_{k,s}))| - \delta^{1/4}|Q_{k,s}| \\
&\geq ((\ln 2 - C/K)^{j-1} - 2\delta^{1/4})|Q_{k,s}| \\
&\geq ((\ln 2 - C/K)^{j-1} - 2\delta^{1/4} - 2\sqrt{\epsilon})\frac{1}{K-s}|Q_k| \\
&\geq ((\ln 2 - C/K)^{j-1} - 4\delta^{1/4})\frac{1}{K-s}|Q_k|
\end{aligned}$$

and

$$\begin{aligned}
|\nu_{\ell-1,j-1}(\tau(\textsc{DownSet}_s(Q_k))| &\leq |\nu_{\ell-1,j-1}(\Pi_s^*(Q_{k,s}))| + \delta^{1/4}|Q_{k,s}| \\
&\leq ((\ln 2 + C/K)^{j-1} + 2\delta^{1/4})|Q_{k,s}| \\
&\leq ((\ln 2 + C/K)^{j-1} + 2\delta^{1/4} + 2\sqrt{\epsilon})\frac{1}{K-s}|Q_k| \\
&\leq ((\ln 2 + C/K)^{j-1} + 4\delta^{1/4})\frac{1}{K-s}|Q_k|.
\end{aligned} \tag{211}$$

We now get by (180)

$$\begin{aligned}
|\nu_{\ell,j}(T_k \setminus T_{k+1})| &= |\nu_{\ell,j}(Q_k)| \\
&\geq \sum_{s=0}^{k} |\nu_{\ell-1,j-1}(\tau^{\ell}(\textsc{DownSet}_s^{\ell}(Q_k)))| \\
&\geq \sum_{s=0}^{k}((\ln 2 - C/K)^{j-1} - 4\delta^{1/4})\frac{1}{K-s}|Q_k| \\
&\geq ((\ln 2 - C/K)^{j-1} - 4\delta^{1/4})|Q_k| \left(\sum_{s=0}^{k} \frac{1}{K-s}\right)
\end{aligned} \tag{212}$$

and

$$\begin{aligned}
|\nu_{\ell,j}(T_k \setminus T_{k+1})| &= |\nu_{\ell,j}(Q_k)| \\
&\leq \sum_{s=0}^{k} |\nu_{\ell-1,j-1}(\tau^{\ell}(\textsc{DownSet}_s^{\ell}(Q_k)))| \\
&\leq \sum_{s=0}^{k}((\ln 2 + C/K)^{j-1} + 4\delta^{1/4})\frac{1}{K-s}|Q_k| \\
&\leq ((\ln 2 + C/K)^{j-1} + 4\delta^{1/4})|Q_k| \left(\sum_{s=0}^{k} \frac{1}{K-s}\right).
\end{aligned} \tag{213}$$

We now recall that by (205) one has $|Q_k|/m^n = (1 \pm \sqrt{\epsilon})\frac{1}{K}$. At the same time

$$\begin{aligned}
\frac{1}{K}\sum_{k\in[K/2]}\sum_{s=0}^{k}\frac{1}{K-s} &= \frac{1}{K}\sum_{k=0}^{K/2-1}\sum_{s=0}^{k}\frac{1}{K-s}\\
&= \frac{1}{K}\sum_{s=0}^{K/2-1}\frac{K/2-s}{K-s}\\
&= \frac{1}{K}\sum_{s=0}^{K/2-1}\frac{-K/2+K-s}{K-s}\\
&= \frac{1}{K}\sum_{s=0}^{K/2-1}\left(1-\frac{-K/2}{K-s}\right)\\
&= \frac{1}{2}-\frac{1}{2}\sum_{s=0}^{K/2-1}\frac{1}{K-s},
\end{aligned}$$

and hence by Claim 25

$$\frac{1}{2}-\frac{1}{2}\ln 2 \le \frac{1}{K}\sum_{k\in[K/2]}\sum_{s=0}^{k}\frac{1}{K-s} \le \frac{1}{2}-\frac{1}{2}(\ln 2 + 1/K).$$

Substituting these bounds into (212) and (213), we get

$$\begin{aligned}
|\nu_{\ell,j}(T_k\setminus T_{k+1})| &\ge ((\ln 2 - C/K)^{j-1} - 4\delta^{1/4})|Q_k|\left(\sum_{s=0}^{k}\frac{1}{K-s}\right)\\
&\ge ((\ln 2 - C/K)^{j-1} - 4\delta^{1/4})\left(\frac{1}{2}-\frac{1}{2}\ln 2\right)\cdot m^n\\
&\ge \frac{1}{2}(1-\ln 2)(\ln 2 - C/K)^{j-1}\cdot m^n
\end{aligned}$$

and

$$\begin{aligned}
|\nu_{\ell,j}(T_k\setminus T_{k+1})| &\le ((\ln 2 + C/K)^{j-1} + 4\delta^{1/4})|Q_k|\left(\sum_{s=0}^{k}\frac{1}{K-s}\right)\\
&\le ((\ln 2 + C/K)^{j-1} + 4\delta^{1/4})(1+3/K)\left(\frac{1}{2}-\frac{1}{2}\ln 2\right)\cdot m^n\\
&\le \frac{1}{2}(1-\ln 2)(\ln 2 + C/K)^{j-1}\cdot m^n
\end{aligned}$$

This establishes (179) and completes the proof of the lemma. ■

6.3 Key lemma: insensitivity of ν and μ to bounded near orthogonal shifts

Outlier vertices. We define sets of outlier vertices recursively for every $\ell \in [L]$. First define $\Xi^L = \emptyset$ for convenience. Then for every $\ell \in [L]$ we define Ξ^ℓ in terms of $\Xi^{\ell'}, \ell' > \ell$ as follows. First let

$$\mathbf{I}^\ell = \mathbf{J}^\ell \cup \{\mathbf{r}^\ell\} \text{ and } \mathbf{I}^\ell_k = \mathbf{J}^\ell_{<k} \cup \mathrm{Ext}^\ell_k \cup \{\mathbf{q}^\ell_k\} \tag{214}$$

for simplicity of notation. Intuitively, the outlier vertices are simply vertices that are too close to boundaries of cubes in coordinates $\mathbf{I}^\ell$ and $\mathbf{I}^\ell_k$ for all $k \in [K/2]$, or vertices in T^ℓ that are not in the range of $\tau^{\ell+1}$. It is convenient to define, for a $\mathbf{H} \subseteq \mathcal{F}$ and $\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{H}}$, the boundary of a cube as

$$\partial\textsc{Rect}(\mathbf{H}, \mathbf{d}) := \textsc{Rect}(\mathbf{H}, \mathbf{d}) \setminus \text{Int}_\delta(\textsc{Rect}(\mathbf{H}, \mathbf{d})).$$

First let, denoting $\mathbf{I} = \mathbf{I}^{L-1}$ and $\mathbf{I}_k = \mathbf{I}^{L-1}_k$ for convenience,

$$\Xi^{L-1} := \left(\bigcup_{\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}}} \partial\textsc{Rect}(\mathbf{I}, \mathbf{d}) \right) \cup \left(\bigcup_{k \in [K/2]} \bigcup_{\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}_k}} \partial\textsc{Rect}(\mathbf{I}_k, \mathbf{d}) \right), \tag{215}$$

and then for every $\ell \in [L], \ell < L-1$, let, denoting $\mathbf{I} = \mathbf{I}^\ell$ and $\mathbf{I}_k = \mathbf{I}^\ell_k$ for convenience,

$$\begin{aligned} \Xi^\ell := \nu_{\ell+1,1}(\Xi^{\ell+1}) \cup (T^\ell_* \setminus \tau^{\ell+1}(S^{\ell+1})) \cup &\left(\bigcup_{\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}}} \partial\textsc{Rect}(\mathbf{I}, \mathbf{d}) \right) \\ \cup &\left(\bigcup_{k \in [K/2]} \bigcup_{\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}_k}} \partial\textsc{Rect}(\mathbf{I}_k, \mathbf{d}) \right). \end{aligned} \tag{216}$$

Finally, let

$$\Xi = \bigcup_{\ell \in [L]} \Xi^\ell. \tag{217}$$

Remark 140 *Abusing notation somewhat, we will think of the set Ξ as the set of labels in $[m]^n$, and in particular will write $x \in \Xi$ for a vertex $x \in T^\ell$, as well as sometimes write $y \in \Xi$ for a vertex $y \in S^\ell$ for some $\ell \in [L]$.*

This set of outlier vertices is quite small, as the following claim shows:

Claim 141 $|\Xi| \leq \delta^{1/8}|T^0|$.

Proof: By Lemma 128 we have for every $\ell \in [L], \ell < L-1$, that $\left|T^\ell_* \setminus \tau^{\ell+1}(S^{\ell+1}))\right| \leq \delta^{1/4}\left|T^\ell\right|$, and therefore the total contribution of $T^\ell_* \setminus \tau^{\ell+1}(S^{\ell+1})$ due to recursive application of $\nu_{\ell+1,1}$ in the first line of (216) contributes a set of size at most $\sum_{i=0}^{\ell} K^i \delta^{1/4}\left|T^\ell\right|$, since $\nu_{\ell',1}$ maps every point to at most K points, for every $\ell' \in [L]$.

Now note that for every $\mathbf{H} \subset \mathcal{F}$ with $|\mathbf{H}| \leq K^2$ one has using Lemma 106

$$\begin{aligned} \left| \bigcup_{\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{H}}} \partial\textsc{Rect}(\mathbf{H}, \mathbf{d}) \cap T^\ell \right| &= \sum_{\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{H}}} |\partial\textsc{Rect}(\mathbf{H}, \mathbf{d}) \cap T^\ell| \\ &\leq \sum_{\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{H}}} \sqrt{\delta}|\textsc{Rect}(\mathbf{H}, \mathbf{d}) \cap T^\ell| \qquad \text{(by Lemma 106)} \\ &= \sqrt{\delta} \sum_{\mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{H}}} |\textsc{Rect}(\mathbf{H}, \mathbf{d}) \cap T^\ell| \\ &= \sqrt{\delta}|T^0|. \end{aligned} \tag{218}$$

Applying this to (216), and using the fact that for every ℓ and j the map $\nu_{\ell',1}$ does not map any point to more than K points, we get that the contribution of the set in (218) after all recursive applications of $\nu_{\ell,1}$ in the first line of (216) contributes at most $\sum_{i=0}^{\ell} K^i\sqrt{\delta}\,|T^\ell|$. Summing these contributions over $\mathbf{H}=\mathbf{I}$ and $\mathbf{H}=\mathbf{I}_k, k\in[K/2]$, we get for every $\ell\in[L]$

$$|\Xi^\ell|\leq 2K\cdot L\cdot K^L\cdot\delta^{1/4}|T^0| \tag{219}$$

and $|\Xi|\leq\sum_{\ell\in[L]}|\Xi^\ell|\leq 2K\cdot L^2\cdot K^L\cdot\delta^{1/4}|T^0|$. Finally, it remains to note that

$$\begin{aligned}2K\cdot L^2\cdot K^L\cdot\delta^{1/4}&\leq(K^{2K}\cdot\delta^{1/8})\cdot\delta^{1/8} &&\text{(since } L\leq K \text{ by (p4))}\\&\leq(K^{2K}\cdot K^{-(1/8)100K^2})\cdot\delta^{1/8} &&\text{(since } \delta\leq K^{-100K^2} \text{ by (p3) and (p5))}\\&\leq\delta^{1/8},\end{aligned}$$

where the last transition uses the fact that K is larger than an absolute constant. ■

Lemma 142 *For every $\ell\in[L]$, every $x\in T^\ell\setminus\Xi^\ell$ (where Ξ^ℓ is as in (216)) such that $x\in\nu_{\ell+z,z}(T^{\ell+z}\setminus T_*^{\ell+z})$ for some $z\in\{0,1,\ldots,L-1-\ell\}$ the following conditions hold for every $y\in T^\ell\setminus\Xi^\ell$ satisfying $y=x+\lambda\cdot\mathbf{u}$ for some $\mathbf{u}\in\mathbf{B}^\ell\setminus\widetilde{\Psi}(\mathbf{B}^\ell), |\lambda|\leq 2M/w$.*

For every $j=0,\ldots,z$ there exists $k\in[K/2]$ such that

(1) *there exist unique $\widetilde{x},\widetilde{y}\in T_k^{\ell+j}$ such that*

$$x\in\nu_{\ell+j,j}(\widetilde{x}) \text{ and } y\in\nu_{\ell+j,j}(\widetilde{y})$$

(2) *there exists a collection of vectors*

$$\mathbf{I}^{\ell+j}\subset\left(\mathbf{J}_{<k}^{\ell+j}\cup Ext_k^{\ell+j}\cup\{\mathbf{q}_k^{\ell+j}\}\right)\cup\bigcup_{s=0}^{j-1}\widetilde{\Psi}(\mathbf{B}^{\ell+s}). \tag{220}$$

with $|\mathbf{I}^{\ell+j}|=j(K+1)$ together with integer coefficients $t_\mathbf{i},\mathbf{i}\in\mathbf{I}^{\ell+j}$, satisfying $|t_\mathbf{i}|\leq 20M/w$ for $\mathbf{i}\in\mathbf{B}^{<\ell+j}$ and $|t_\mathbf{i}|\leq 10M/w$ for $\mathbf{i}\in\mathbf{B}^{\ell+j}$ such that

$$\widetilde{y}=\widetilde{x}+\lambda\cdot\mathbf{u}+\sum_{\mathbf{i}\in\mathbf{I}^{\ell+j}}t_\mathbf{i}\cdot\mathbf{i}. \tag{221}$$

(3) *for $\mathbf{I}=\mathbf{J}^{\ell+j}\cup\{\mathbf{r}^{\ell+j}\}$ there exists a rectangle $R=\textsc{Rect}(\mathbf{I},\mathbf{d})$, $\mathbf{d}\in(\Delta\cdot\mathbb{Z}\cap[0,1))^\mathbf{I}$, such that*

$$\widetilde{x}\in Int_\delta(R) \text{ and } \widetilde{y}\in Int_\delta(R).$$

Proof: We first note that the choice of z is unique by Lemma 135, **(2)**. We establish properties **(1)**, **(2)** and **(3)** above by induction on $j\in\{0,1,\ldots,z\}$.

Base: $j=0$**.** Note that $\nu_{\ell,0}$ is the identity map, so we can take $\widetilde{x}=x,\widetilde{y}=y$. Property **(1)** follows by construction. Property **(2)** follows taking $\mathbf{I}^\ell=\emptyset$. Property **(3)** follows since $y\in T^\ell\setminus\Xi^\ell$ by assumption and Ξ^ℓ includes all points that are too close to boundaries of rectangles in $\mathbf{J}^\ell\cup\{\mathbf{r}^\ell\}$ by construction (see (216)).

Inductive step: $j-1\to j$**.** We write $\mathbf{J}=\mathbf{J}^{\ell+j-1}$ and write $\mathbf{r}=\mathbf{r}^{\ell+j-1}$ to denote the $(\ell+j-1)$-th compression index. We write $\mathbf{J}'=\mathbf{J}^{\ell+j}$, and write $\text{Ext}_k=\text{Ext}_k^{\ell+j}$ and $\mathbf{q}_k=\mathbf{q}_k^{\ell+j}$ to denote the extension and compression indices of phase k at stage $\ell+j$. We let $\mathbf{r}'=\mathbf{r}^{\ell+j}$ denote the $(\ell+j)$-th compression index. We define

$$\mathbf{I}:=\mathbf{J}\cup\{\mathbf{r}\} \tag{222}$$

to simplify notation. By the inductive hypothesis for $x, y \in T^\ell \setminus \Xi^\ell$ there exist $u, v \in T^{\ell+j-1}$ such that

$$x \in \nu_{\ell+j-1,j-1}(u)$$

and

$$y \in \nu_{\ell+j-1,j-1}(v)$$

together with $\mathbf{d}' \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\mathbf{I}}$ such that

$$u \in \text{Int}_\delta(\textsc{Rect}(\mathbf{I}, \mathbf{d}')) \text{ and } v \in \text{Int}_\delta(\textsc{Rect}(\mathbf{I}, \mathbf{d}')), \tag{223}$$

and

$$v = u + \sum_{\mathbf{i} \in \mathbf{I}^{\ell+j-1}} t_{\mathbf{i}} \cdot \mathbf{i} \tag{224}$$

for integer coefficients t with $|t_{\mathbf{i}}| \leq 20M/w$ for $\mathbf{i} \in \mathbf{B}^{<\ell+j-1}$ and $|t_{\mathbf{i}}| \leq 10M/w$ for $\mathbf{i} \in \mathbf{B}^{\ell+j-1}$.

We assume that $j - 1 < z$, as otherwise there is nothing to prove. Otherwise, since $j - 1 < z$, we have $\textsc{Rect}(\mathbf{I}, \mathbf{d}) \subset T_*^{\ell+j-1}$, as $\textsc{Rect}(\mathbf{I}, \mathbf{d})$ cannot intersect both $T_*^{\ell+j-1}$ and $T^{\ell+j-1} \setminus T_*^{\ell+j-1}$ and the choice of z is unique (by Lemma 135, **(2)**, as noted above). Since

$$\Xi^\ell \supset \nu_{\ell+j-1,j-1}(T_*^{\ell+j-1} \setminus \tau^{\ell+j}(S^{\ell+j})),$$

there exist $x', y' \in S^{\ell+j}$ such that $\tau^{\ell+j}(x') = u$, $\tau^{\ell+j}(y') = v$. By (223) together with Lemma 129, **(1)** and **(2)**, there exists $k \in [K/2]$ such that $x', y' \in S_k^{\ell+j}$ and $\mathbf{d}' \in \mathbf{I}'$ such that

$$\rho_k(x') \in \textsc{Rect}(\mathbf{I}', \mathbf{d}') \text{ and } \rho_k(y') \in \textsc{Rect}(\mathbf{I}', \mathbf{d}'). \tag{225}$$

We will use the above fact shortly.

By Lemma 127 there exist integer coefficients $t_{\mathbf{i}}^x, t_{\mathbf{i}}^y$ such that

$$x' = u + \sum_{\mathbf{i} \in \mathbf{I}' \cup \mathbf{I}} t_{\mathbf{i}}^x \cdot \mathbf{i} \quad \text{with} \quad \|t^x\|_\infty \leq 5M/w$$

and

$$y' = v + \sum_{\mathbf{i} \in \mathbf{I}' \cup \mathbf{I}} t_{\mathbf{i}}^y \cdot \mathbf{i} \quad \text{with} \quad \|t^y\|_\infty \leq 5M/w,$$

where we define

$$\mathbf{I}' = \mathbf{J}'_{<k} \cup \text{Ext}_k \cup \{\mathbf{q}_k\} \tag{226}$$

to simplify notation. Combining this with (224), we get

$$y' = x' + \sum_{\mathbf{i} \in \mathbf{I}^{\ell+j}} s_{\mathbf{i}} \cdot \mathbf{i}, \tag{227}$$

where we let $\mathbf{I}^{\ell+j} := \mathbf{I}^{\ell+j-1} \cup \mathbf{I}' \cup \mathbf{I}$ and let

$$s_{\mathbf{i}} = t_{\mathbf{i}} + t_{\mathbf{i}}^y - t_{\mathbf{i}}^x,$$

extending $t_{\mathbf{i}}$ to be zero for $\mathbf{i} \notin \mathbf{I}^{\ell+j-1}$, $t_{\mathbf{i}}^x$ to be zero for $\mathbf{i} \notin \mathbf{I}' \cup \mathbf{I}$ and $t_{\mathbf{i}}^y$ to be zero for $\mathbf{i} \notin \mathbf{I}' \cup \mathbf{I}$. Note that

$$\begin{aligned}
\mathbf{I}^{\ell+j} &= \mathbf{I}^{\ell+j-1} \cup (\mathbf{I}' \cup \mathbf{I}) \\
&\subset \left(\left(\mathbf{J}_{<k}^{\ell+j-1} \cup \text{Ext}_k^{\ell+j-1} \cup \{\mathbf{q}_k^{\ell+j-1}\} \right) \cup \bigcup_{s=0}^{j-2} \widetilde{\Psi}(\mathbf{B}^{\ell+s}) \right) \cup (\mathbf{I}' \cup \mathbf{I}) \quad \text{(by the inductive hypothesis)} \\
&\subset \left(\mathbf{J}_{<k}^{\ell+j} \cup \text{Ext}_k^{\ell+j} \cup \{\mathbf{q}_k^{\ell+j}\} \right) \cup \bigcup_{s=0}^{j-1} \widetilde{\Psi}(\mathbf{B}^{\ell+s}).
\end{aligned}$$

The last transition uses the fact that

$$\mathbf{I}' = \mathbf{J}'_{<k} \cup \mathrm{Ext}_k \cup \{\mathbf{q}_k\} = \mathbf{J}^{\ell+j}_{<k} \cup \mathrm{Ext}^{\ell+j}_k \cup \{\mathbf{q}^{\ell+j}_k\}$$

by (226) and

$$\mathbf{I} = \mathbf{J} \cup \{\mathbf{r}\} \subset \widetilde{\Psi}(\mathbf{B}^{\ell+j-1})$$

by (222).

We now upper bound the magnitude of the coefficients $s_{\mathbf{i}}$. First, for $\mathbf{I}^{\ell+j} \backslash \mathbf{B}^{<\ell+j} \subseteq \mathbf{J}^{\ell+j}_{<k} \cup \mathrm{Ext}^{\ell+j}_k \cup \{\mathbf{q}^{\ell+j}_k\}$ one has

$$|s_{\mathbf{i}}| = |t^y_{\mathbf{i}} - t^x_{\mathbf{i}}| \leq |t^y_{\mathbf{i}}| + |t^x_{\mathbf{i}}| \leq 5M/w + 5M/w \leq 10M/w$$

as required. Now consider $\mathbf{i} \in \mathbf{I}^{\ell+j} \cap \mathbf{B}^{<\ell+j}$. First note that if $\mathbf{i} \in \mathbf{B}^{<\ell+j-1}$ then one has $t^x_{\mathbf{i}} = t^y_{\mathbf{i}} = 0$ since $\mathbf{B}^{<\ell+j-1} \cap (\mathbf{I} \cup \mathbf{I}') = \emptyset$, and thus one has $|s_{\mathbf{i}}| = |t_{\mathbf{i}}| \leq 20M/w$ by the inductive hypothesis. Now consider

$$\mathbf{i} \in \mathbf{I}^{\ell+j} \cap \mathbf{B}^{\ell+j-1}$$

In that case one has $|t_{\mathbf{i}}| \leq 10M/w$ by the inductive hypothesis, so

$$|s_{\mathbf{i}}| = |t_{\mathbf{i}} + t^y_{\mathbf{i}} - t^x_{\mathbf{i}}| \leq |t_{\mathbf{i}}| + |t^y_{\mathbf{i}}| + |t^x_{\mathbf{i}}| \leq 10M/w + 5M/w + 5M/w = 20M/w$$

as required, establishing properties **(1)** and **(2)**. We now turn to property **(3)**. Define

$$\widetilde{\mathbf{I}} = \mathbf{J}' \cup \{\mathbf{r}'\} \tag{228}$$

to simplify notation, and let $\mathbf{a}, \mathbf{b} \in (\Delta \cdot \mathbb{Z} \cap [0,1))^{\widetilde{\mathbf{I}}}$ be such that $x' \in \textsc{Rect}(\widetilde{\mathbf{I}}, \mathbf{a})$ and $y' \in \textsc{Rect}(\widetilde{\mathbf{I}}, \mathbf{b})$, i.e.

$$\langle x', \mathbf{i}\rangle \pmod M \in [\mathbf{a}_{\mathbf{i}}, \mathbf{a}_{\mathbf{i}} + \Delta) \cdot M \text{ and } \langle y', \mathbf{i}\rangle \pmod M \in [\mathbf{b}_{\mathbf{i}}, \mathbf{b}_{\mathbf{i}} + \Delta) \cdot M. \tag{229}$$

We now show that in fact $\mathbf{a} = \mathbf{b}$. We start by noting that

$$\begin{aligned} \widetilde{\mathbf{I}} \cap \mathbf{I}^{\ell+j} &= (\mathbf{J}' \cup \{\mathbf{r}'\}) \cap \mathbf{I}^{\ell+j} \\ &\subseteq (\mathbf{J}' \cup \{\mathbf{r}'\}) \cap (\mathbf{B}^{<\ell+j} \cup \mathbf{J}'_{<k} \cup \mathrm{Ext}_k \cup \{\mathbf{q}_k\}) \\ &\subseteq \mathbf{J}'_{<k} \end{aligned} \tag{230}$$

By (225) we have for every $\mathbf{i} \in \widetilde{\mathbf{I}} \cap \mathbf{I}^{\ell+j} \subseteq \mathbf{J}'$

$$\langle \rho_k(x'), \mathbf{i}\rangle \pmod M \in [\mathbf{d}'_{\mathbf{i}}, \mathbf{d}'_{\mathbf{i}} + \Delta) \cdot M \text{ and } \langle \rho_k(y'), \mathbf{i}\rangle \pmod M \in [\mathbf{d}'_{\mathbf{i}}, \mathbf{d}'_{\mathbf{i}} + \Delta) \cdot M. \tag{231}$$

At the same time by Lemma 116, **(3)**,

$$\rho_k(x') = x' + \lambda_x \cdot \mathbf{q}_k \text{ and } \rho_k(y') = y' + \lambda_y \cdot \mathbf{q}_k$$

for some integers λ_x, λ_y bounded by M/w in absolute value, which implies, since for every $\mathbf{i} \in \widetilde{\mathbf{I}} \cap \mathbf{I}^{\ell+j} \subseteq \mathbf{J}'$ one has $\langle \mathbf{q}_k, \mathbf{i}\rangle < \epsilon \cdot w$, that for every such $\mathbf{i}$

$$|\langle \rho_k(x'), \mathbf{i}\rangle - \langle x', \mathbf{i}\rangle| < \epsilon M \text{ and } |\langle \rho_k(y'), \mathbf{i}\rangle - \langle y', \mathbf{i}\rangle| < \epsilon M. \tag{232}$$

Finally, since $x, y \in T^\ell \setminus \Xi^\ell$ by assumption, we have $x' \notin \partial\textsc{Rect}(\mathbf{I}', \mathbf{c})$ and $y' \notin \partial\textsc{Rect}(\mathbf{I}', \mathbf{c})$ for any $\mathbf{c}$, (231) and (232) above, together with the fact that $\epsilon < \delta$ by (p6), imply that for every $\mathbf{i} \in \widetilde{\mathbf{I}} \cap \mathbf{I}^{\ell+j} \subseteq \mathbf{J}'$

$$\langle x', \mathbf{i}\rangle \pmod M \in [\mathbf{d}'_{\mathbf{i}}, \mathbf{d}'_{\mathbf{i}} + \Delta) \cdot M \text{ and } \langle y', \mathbf{i}\rangle \pmod M \in [\mathbf{d}'_{\mathbf{i}}, \mathbf{d}'_{\mathbf{i}} + \Delta) \cdot M.$$

Thus, for $\mathbf{a}$ and $\mathbf{b}$ from (229) we have $\mathbf{a}_\mathbf{i} = \mathbf{b}_\mathbf{i}$ for all $\mathbf{i} \in \widetilde{\mathbf{I}} \cap \mathbf{I}^{\ell+j}$. At the same time for every $\mathbf{i} \in \widetilde{\mathbf{I}} \setminus \mathbf{I}^{\ell+j}$ one has by (227)

$$\begin{aligned} \left|\langle x', \mathbf{i}\rangle - \langle y', \mathbf{i}\rangle\right| &= \left|\sum_{\mathbf{h}\in\mathbf{I}^{\ell+j}} s_\mathbf{h} \cdot \langle \mathbf{h}, \mathbf{i}\rangle\right| \\ &\leq |\mathbf{I}^{\ell+j}| \cdot (20M/w) \cdot \max_{\mathbf{h}\in\mathbf{I}^{\ell+j}} \langle \mathbf{h}, \mathbf{i}\rangle \\ &\leq |\mathbf{I}^{\ell+j}| \cdot (20M/w) \cdot \epsilon \cdot w \\ &\leq 40K^3\epsilon \cdot M \\ &< \delta \cdot M. \end{aligned} \tag{233}$$

The second transition above uses the fact that $\|s\|_\infty \leq 20M/w$, The forth transition uses the fact that

$$\left|\mathbf{I}^{\ell+j}\right| \leq 2K^2 \cdot L \leq 2K^3,$$

as

$$\mathbf{I}^{\ell+j} \subseteq \bigcup_{\ell\in[L]} \left(\mathbf{J}^\ell \cup \{\mathbf{r}^\ell\} \cup \bigcup_{k\in[K]} (\mathrm{Ext}_k^\ell \cup \{\mathbf{q}_k^\ell\})\right).$$

The fifth transition in (233) uses the fact

$$\begin{aligned} 40K^3\epsilon &\leq (40K^3\delta)\cdot\delta && \text{(by (p6))} \\ &\leq (40K^3 \cdot K^{-100K^2}) \cdot \delta && \text{(by (p3) and (p5))} \\ &< \delta \end{aligned}$$

since K is larger than a constant.

Now recall that $x, y \in T^\ell \setminus \Xi^\ell$, and in particular by (216)

$$x, y \notin \bigcup_{\mathbf{d}\in(\Delta\cdot\mathbb{Z}\cap[0,1])^{\widetilde{\mathbf{I}}}} \partial\textsc{Rect}(\widetilde{\mathbf{I}}, \mathbf{d}).$$

Combining this with (229) and (233) yields $\mathbf{a}_\mathbf{i} = \mathbf{b}_\mathbf{i}$, as required. Thus, we get

$$x', y' \in \textsc{Rect}(\widetilde{\mathbf{I}}, \mathbf{a}),$$

which establishes property **(3)** and completes the proof of the inductive step. ■

Lemma 143 *For every $\ell \in [L]$, every $x \in T^\ell \setminus \Xi^\ell$, $y \in T^\ell \setminus \Xi^\ell$ (where Ξ^ℓ is defined in* (216)*) the following conditions hold. If*

$$x \in \nu_{\ell+j,j}(T^{\ell+j} \setminus \mathit{Ext}_\delta(T_*^{\ell+j})),$$

and $y = x + \lambda \cdot \mathbf{u}$, $|\lambda| \leq 2M/w$, for some $\mathbf{u} \in \mathbf{B}^\ell \setminus \widetilde{\Psi}(\mathbf{B}^\ell)$, then

$$y \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}).$$

Proof: We invoke Lemma 142 with $z = j$, and let $\widetilde{x}$ and $\widetilde{y}$ denote the resulting points (we use $z = j$ in what follows), and let $k \in [K/2]$ be such that

$$\widetilde{x} \in (T^{\ell+z} \setminus \mathrm{Ext}_\delta(T_*^{\ell+z})) \cap T_k^{\ell+z} = T_k^{\ell+z} \setminus \mathrm{Ext}_\delta(T_*^{\ell+z}). \tag{234}$$

Also recall that

$$T^{\ell+z}\backslash\mathrm{Ext}_\delta(T_*^{\ell+z}) = \left\{y \in [m]^n : \langle y, \mathbf{j}_s\rangle \pmod M \in \left(1 - \frac{1}{K-s} + \delta, 1-\delta\right] \cdot M \text{ for some } s \in [K/2+1]\right\},$$

where we let $\mathbf{J} := \mathbf{J}^{\ell+z}$ to simplify notation. Since

$$T_k^{\ell+z} = \left\{y \in [m]^n : \langle y, \mathbf{j}_s\rangle \pmod M \in \left[0, 1 - \frac{1}{K-s}\right) \cdot M \text{ for all } s \in [k]\right\},$$

we have

$$\begin{aligned} T_k^{\ell+z} \setminus \mathrm{Ext}_\delta(T_*^{\ell+z}) = \Bigg\{y \in T_k^{\ell+z} : \langle y, \mathbf{j}_s\rangle \pmod M \in \left(1 - \frac{1}{K-s} + \delta, 1-\delta\right] \cdot M \\ \text{for some } s \in \{k, k+1, \ldots, K/2\}\Bigg\}. \end{aligned}$$

Since $\widetilde{x} \in T_k^{\ell+z} \setminus \mathrm{Ext}_\delta(T_*^{\ell+z})$ by (234), there exists $s \in \{k, k+1, \ldots, K/2\}$ such that

$$\langle \widetilde{x}, \mathbf{j}_s\rangle \pmod M \in \left(1 - \frac{1}{K-s} + \delta, 1-\delta\right] \cdot M.$$

At the same time using (220) and (221) we have for every $\mathbf{j} \in \mathbf{J}_{\geq k}^{\ell+z}$ and in particular for $\mathbf{j} = \mathbf{j}_s$

$$\begin{aligned} |\langle \widetilde{y}, \mathbf{j}\rangle - \langle \widetilde{x}, \mathbf{j}\rangle| &= \left|\lambda \cdot \langle \mathbf{u}, \mathbf{j}\rangle + \sum_{\mathbf{i} \in \mathbf{I}^{\ell+z}} t_{\mathbf{i}} \cdot \langle \mathbf{i}, \mathbf{j}\rangle\right| \\ &\leq \lambda \cdot \epsilon \cdot w + \sum_{\mathbf{i} \in \mathbf{I}^{\ell+z}} t_{\mathbf{i}} \cdot \epsilon \cdot w \\ &\leq \epsilon \cdot M + \epsilon \|t\|_\infty \cdot |\mathbf{I}| \cdot w \\ &\leq \epsilon(1 + L \cdot K) \cdot M \\ &< \delta M. \end{aligned} \tag{235}$$

In the derivation above we first used the fact that $\mathbf{u} \neq \mathbf{j}$ since $\mathbf{j} \in \mathbf{J}^{\ell+z} \subset \widetilde{\Psi}(\mathbf{B}^{\ell+z})$ and $\mathbf{u} \in \mathbf{B}^\ell \setminus \widetilde{\Psi}(\mathbf{B}^\ell)$ (note that the two sets are disjoint regardless of the value of z). We also used the fact that $\mathbf{j} \notin \mathbf{I}^{\ell+z}$, since $\mathbf{j} \in \mathbf{J}_{\geq k}^{\ell+z}$ (note the crucial subindex $\geq k$) and by Lemma 142, **(2)** one has

$$\begin{aligned} \mathbf{I}^{\ell+z} \cap \mathbf{J}_{\geq k}^{\ell+z} &\subset \left(\left(\mathbf{J}_{<k}^{\ell+z} \cup \mathrm{Ext}_k^{\ell+z} \cup \{\mathbf{q}_k^{\ell+z}\}\right) \cup \bigcup_{s=0}^{z-1} \widetilde{\Psi}(\mathbf{B}^{\ell+s})\right) \cap \mathbf{J}_{\geq k}^{\ell+z} \\ &\subseteq \left(\mathbf{J}_{<k}^{\ell+z} \cup \mathrm{Ext}_k^{\ell+z} \cup \{\mathbf{q}_k^{\ell+z}\}\right) \cap \mathbf{J}_{\geq k}^{\ell+z} \\ &= \emptyset. \end{aligned}$$

We then used the fact that

$$\begin{aligned} \epsilon(1 + L \cdot K) &\leq \epsilon(1 + K^2) && \text{(by (p4))} \\ &\leq \delta^2(1 + K^2) && \text{(by (p6))} \\ &\leq \delta\Delta^{100K^2}(1 + K^2) && \text{(by (p5))} \\ &\leq \delta K^{-100K^2}(1 + K^2) && \text{(by (p3))} \\ &\leq \delta, \end{aligned}$$

where the last transition is due to the fact that K is larger than a constant. Then we have by (235) that

$$\langle \widetilde{y}, \mathbf{j}_s \rangle \pmod{M} \in \left(1 - \frac{1}{K-s}, 1\right] \cdot M.$$

Thus, since $\widetilde{y} \in T_k^{\ell+z}$ by assumption, we have $\widetilde{y} \in T_k^{\ell+z} \setminus T_*^{\ell+z} \subseteq T^{\ell+z} \setminus T_*^{\ell+z}$ and therefore

$$y = \nu_{\ell+j,j}(\widetilde{y}) \in \nu_{\ell+j,j}(T^{\ell+z} \setminus T_*^{\ell+z}), \tag{236}$$

as required. [7] ■

Corollary 144 *For every $\ell \in [L]$, every $k \in [K/2]$, $x \in T_k^\ell \setminus \Xi^\ell$, $y \in S_k^\ell \setminus \Xi^\ell$ (where Ξ^ℓ is defined in* (216)*) the following conditions hold. If*

$$x \in \nu_{\ell+j,j}(T^{\ell+j} \setminus \mathit{Ext}_\delta(T_*^{\ell+j})),$$

and $y = x + \lambda \cdot \mathbf{u}, |\lambda| \leq 2M/w,$ for some $\mathbf{u} \in \mathbf{B}^\ell \setminus \widetilde{\Psi}(\mathbf{B}^\ell)$, then

$$y \in \mu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}).$$

Proof: Let $y' \in T_k^\ell$ be such that $y' \asymp y$ – such a y' exists by definition of S_k (see (101)).Then by Lemma 143 we have $y' \in \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})$. Since

$$\mu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}) = \text{DownSet}^\ell(\nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}))$$

by Definition 130, we get, again using the fact that $y' \asymp y$, that $y \in \mu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j})$, as required. ■

7 Proof of main theorem (Theorem 1)

We prove the main theorem (Theorem 1) in this section. First we define a hard distribution $\mathcal{D}$ on input graphs $\widehat{G}$ in Section 7.1. We then prove a lower bound on the size of the maximum matching in $\widehat{G}$ and design a good upper bound on the size of the matching constructed by a small space algorithm in Section 7.2. Finally, we prove the main theorem in Section 7.3.

7.1 Input distribution on graphs

We now define the hard distribution $\mathcal{D}$ on input graphs. First for $\ell \in [L]$ and $k \in [K/2]$ select the compression vector $\mathbf{q}_k^\ell$ arbitrarily from $\mathbf{B}_k^\ell$ and select the extension indices Ext_k^ℓ arbitrarily from $\mathbf{B}_k^\ell$. Recall that for $k \in [K/2]$ we define

$$\mathring{\mathbf{B}}_k^\ell = \mathbf{B}_k^\ell \setminus (\{\mathbf{q}_k^\ell\} \cup \text{Ext}_k^\ell)$$

and let

$$\mathring{\mathbf{B}}_{K/2}^\ell = \mathbf{B}_{K/2}^\ell \setminus \{\mathbf{r}^\ell\}.$$

Input distribution $\mathcal{D}$. For every $\ell \in [L]$ and every $k \in [K/2+1]$ sample

$$\mathbf{J}^\ell \sim \text{UNIF}\left(\mathring{\mathbf{B}}_0^\ell \times \mathring{\mathbf{B}}_1^\ell \times \ldots \times \mathring{\mathbf{B}}_{K/2}^\ell\right),$$

i.e. for each $k \in [K/2+1]$ sample $\mathbf{j}_k^\ell$ independently and uniformly at random from $\mathring{\mathbf{B}}_k^\ell$. Let $G^\ell = (S^\ell, T^\ell, E^\ell)$ be basic gadget graphs as defined in Section 5.3, and for every $\ell \in [L], \ell > 0$, let

$$\tau^\ell : S^\ell \to T_*^{\ell-1}$$

be the ℓ-th glueing map as defined in Section 5.10.

[7] We note that the stronger implication that $\widetilde{y} \in T_k^{\ell+z} \setminus T_*^{\ell+z}$ as opposed to just $\widetilde{y} \in T^{\ell+z} \setminus T_*^{\ell+z}$ is not needed to conclude (236).

Subsamplings $\widetilde{G}^\ell$ of individual gadgets G^ℓ. We now fix $\ell \in [L]$ and write $S = S^\ell$ and $T = T^\ell$ to simplify notation. For every $k \in [K/2]$, $\mathbf{j} \in \mathbf{B}^\ell_k$ and $y \in S_k$ let

$$X^\ell_{k,\mathbf{j}}(y) = \text{Bernoulli}(1 - 1/K) \tag{237}$$

denote independent Bernoulli random variables conditioned on $\sum_{y\in S_k} X^\ell_{k,\mathbf{j}}(y) = \lceil (1 - \frac{1}{K})|S_k| \rceil$ for all k and $\mathbf{j}$. We use these variables to sample edges of the graphs G^ℓ as follows. Define

$$\widetilde{E}^\ell_{k,\mathbf{j}} = \bigcup_{y\in C_\mathbf{j}} \left\{ u \in \text{line}_\mathbf{j}(y) \cap \text{Int}_\delta(S^\mathbf{j}_k) : X^\ell_{k,\mathbf{j}}(u) = 1 \right\} \times (\text{line}_\mathbf{j}(y) \cap (T_k \setminus T^\mathbf{j}_k)),$$

where $C_\mathbf{j}$ is a minimal $\mathbf{j}$-line cover, and let

$$\widetilde{E}^\ell_k = \bigcup_{\mathbf{j}\in \mathring{\mathbf{B}}^\ell_k} \widetilde{E}^\ell_{k,\mathbf{j}}.$$

Comparing this to the definition of the edge set of G^ℓ in (108), one observes that we subsample edges of G^ℓ in a somewhat dependent way – the set $\widetilde{E}^\ell_k$ contains, for every direction $\mathbf{j} \in \mathbf{B}^\ell_k$ and $y \in C_\mathbf{j}$, a complete bipartite graph between vertices u in $\text{line}_\mathbf{j}(y) \cap \text{Int}_\delta(S^\mathbf{j}_k)$ that were sampled by $X^\ell_{k,\mathbf{j}}(u)$ and $\text{line}_\mathbf{j}(y) \cap (T_k \setminus T^\mathbf{j}_k)$. The fact that randomness is provided by the vertices $u \in S_k$ as opposed to edges themselves will not be a problem since we are interested in concentration of matching size in G^ℓ and do not need to reason about arbitrary edge sets – see proof of Lemma 145 below. Let

$$\widetilde{G}^\ell = (S^\ell, T^\ell, \widetilde{E}^\ell).$$

As discussed above, $\widetilde{G}^\ell$ is a slightly subsampled version of G^ℓ. This operation has the desired effect of making it hard to store edges of $\widetilde{G}^\ell$ (since the algorithm intuitively must remember which edge of G^ℓ was included and which was not), but at the same time barely changes matching size in G^ℓ, as we now show.

Lemma 145 (Large matchings in subsampled gadgets $\widetilde{G}^\ell$) *With probability at least $1 - 1/N$ for every $\ell \in [L], \ell > 0$, there exists a matching of S^ℓ to $T^\ell \setminus T^\ell_*$ of size at least $(1 - O(1/K))|S^\ell|$.*

Proof: Fix $\ell \in [L]$ (we will apply a union bound over all $\ell \in [L]$ later). We write $G = G^\ell, S = S^\ell, T = T^\ell, E = E^\ell, \widetilde{G} = \widetilde{G}^\ell, \widetilde{E} = \widetilde{E}^\ell$ to simplify notation. For every edge $e \in E$ define the random variable

$$Z_e = \begin{cases} 1 & \text{if } e \in \widetilde{E} \\ 0 & \text{o.w.} \end{cases} \tag{238}$$

Note that for every matching $M \subseteq E$ random variables $\{Z_e\}_{e\in M}$ are negatively dependent, since a matching M touches every vertex at most once.

By Lemma 114 applied to $G = (S, T, E)$ there exists a matching of a $(1 - O(1/K))$ fraction of vertices in S to $T \setminus T_*$ – denote this matching by M. Let

$$\widetilde{M} := M \cap \widetilde{E} = \{e \in M : Z_e = 1\}$$

denote the subset of the edges of M that are included in $\widetilde{E}$. Note that $\widetilde{M}$ is a matching between a subset of S and a subset of $T \setminus T_*$, and we have

$$\mathbf{E}[|\widetilde{M}|] = \sum_{e\in M} \mathbf{Pr}[e \in \widetilde{E}] = \sum_{e\in M} \mathbf{E}[Z_e] = (1 - 1/K)|M|$$

by definition of Z_e in (238) and the fact that every edge in E is included in $\widetilde{E}$ with probability $1 - 1/K$ by (237). Since the random variables $\{Z_e\}_{e \in M}$ are negatively dependent, we have by an application to the Chernoff bound (for negatively associated random variables)

$$\mathbf{Pr}[|\widetilde{M}| < (1 - 2/K)|M|] \leq \exp(-\Omega(|M|/K)).$$

Since M matches at least a constant fraction of S, we get that $|M| = \Omega(N/(KL))$, and therefore

$$\mathbf{Pr}[|\widetilde{M}| < (1 - 2/K)|M|] \leq \exp(-\Omega(N/(KL))) \leq N^{-2},$$

where N is the number of vertices in our graph instance. Thus, for every fixed $\ell \in [L], \ell > 0$, with probability at least $1 - N^{-2}$ there exists a matching of at least a $1 - O(1/K)$ fraction of S^ℓ to $T^\ell \setminus T^\ell_*$ in $\widetilde{G}^\ell$. The result of the lemma follows by a union bound over ℓ. ■

Defining the input graph $\widehat{G}$. We now define the graph $\widehat{G} = (P, Q, \widehat{E})$ arriving in the stream and specify the order of arrival. We have

$$P = \left(\bigcup_{\text{even } \ell \in [L]} T^\ell \right) \cup \Upsilon_{odd} \tag{239}$$

and

$$Q = S^0 \cup \left(\bigcup_{\text{odd } \ell \in [L]} T^\ell \right) \cup \Upsilon_{even}, \tag{240}$$

where

$$\begin{aligned} \Upsilon_{even} &= \left(\bigcup_{\text{even } \ell \in [L], \ell > 0} \{s \in S^\ell : \tau^\ell(s) \text{ is not defined}\} \right) \\ &\text{and} \\ \Upsilon_{odd} &= \left(\bigcup_{\text{odd } \ell \in [L]} \{s \in S^\ell : \tau^\ell(s) \text{ is not defined}\} \right) \end{aligned} \tag{241}$$

We will show below that $|\Upsilon_{even} \cup \Upsilon_{odd}| = o(|P|)$.

Edge set $\widehat{E}$ of $\widehat{G}$. Before defining the edge set $\widehat{E}$, it is useful to define a natural extension of the glueing maps τ^ℓ, $\ell \in [L], \ell > 0$, from vertices in S^ℓ to edges in E^ℓ. For an edge $(s, t) \in E^\ell, s \in S^\ell, t \in T^\ell$ we define

$$\tau^\ell(e) = \begin{cases} (\tau^\ell(s), t) & \text{if } \tau^\ell(s) \neq \perp \\ (s, t) & \text{o.w.} \end{cases}$$

Note that τ^ℓ is injective on edges since it is injective on vertices in S^ℓ (by Claim 126). The edge set $\widehat{E}$ of $\widehat{G}$ is defined as

$$\widehat{E} = \bigcup_{\ell \in [L], \ell > 0} \bigcup_{k \in [K/2]} \bigcup_{\mathbf{j} \in \mathring{\mathbf{B}}^\ell_k} \widehat{E}^\ell_{k,\mathbf{j}}, \tag{242}$$

where

$$\widehat{E}^\ell_{k,\mathbf{j}} := \tau^\ell(\widetilde{E}^\ell_{k,\mathbf{j}}). \tag{243}$$

In other words, for every edge $(s, t) \in \widetilde{E}^\ell_{k,\mathbf{j}}$ where $s \in S^\ell$ and $t \in T^\ell$, $\ell > 0$:

1. if $\tau^\ell(s)$ is not defined, add the edge (s,t) to $\widehat{E}^\ell_{k,\mathbf{j}}$;

2. if $\tau^\ell(s)$ is defined, then add the edge $(\tau^\ell(s),t)$ to $\widehat{E}^\ell_{k,\mathbf{j}}$.

Note that we do not include the edges from S^0 to T^0 for convenience (since τ^0 is not defined, this would complicate notation somewhat).

Ordering of edges of $\widehat{G}$ in the stream. The graph $\widetilde{G}$ is presented in the stream over L *rounds* and $K/2$ *phases* as follows. For every $\ell \in \{0,1,\ldots,L-1\}$, for every $k \in [K/2]$, the edges in $\tau_*(E^\ell_k)$ are presented in the stream; the ordering within $\tau^\ell(E^\ell_k)$ is arbitrary.

Definition 146 (Ordering on (ℓ,k) pairs) *For $\ell \in [L]$ and $k \in [K/2+1]$ we write $(\ell',k') < (\ell,k)$ iff $\ell' < \ell$ or $\ell' = \ell$ but $k' < k$.*

Definition 147 *For $\ell \in [L]$ and $k \in [K/2]$ we write*

$$\widehat{G}_{(\ell,k)} = (P,Q,\widehat{E}^\ell_k),$$

and define $\widehat{G}_{(\ell,K/2)} = (P,Q,\emptyset)$, for convenience. We define

$$\widehat{G}_{<(\ell,k)} = \left(P,Q,\bigcup_{\substack{\ell'\in[L],k'\in[K/2]\\(\ell',k')<(\ell,k)}} \widehat{E}^{\ell'}_{k'}\right).$$

Definition 148 *For every $\ell \in [L], k \in [K/2]$ define $\Lambda_{\ell,k}$ as follows. For $k \in [K/2]$ let $\Lambda_{(\ell,k)} = (X^\ell_k, \mathbf{j}^\ell_k)$. For $k = K/2$ let $\Lambda_{\ell,K/2} := (\mathbf{j}^\ell_{K/2})$. We write $\Lambda_{<(\ell,k)} = \left(\Lambda_{\ell',k'}\right)_{(\ell',k')<(\ell,k)}$.*

Remark 149 *Note that $\widehat{G}_{\le(\ell,k)}$ is fully determined by $\Lambda_{<(\ell,k)}$ and X^ℓ_k, and $\mathbf{j}^\ell_k$ is uniformly random in $\mathring{\mathbf{B}}^\ell_k$ conditioned on $\Lambda_{<(\ell,k)}$ and X^ℓ_k. It is important to note here that the restriction of the glueing map τ^ℓ to $S^\ell_{\le k}$ (which we need to fully determine $\widehat{G}_{\le(\ell,k)}$) is, crucially, determined by $\mathbf{J}^\ell_{<k}$ – see Remark 122.*

7.2 Upper and lower bounds on matchings in $\widehat{G}$

We first prove

Lemma 150 (Large matching in $\widehat{G}$) *With probability at least $1-1/N$ there exists a matching in $\widehat{G}$ of size at least $(1-O(1/L))|P|$.*

Proof: By Lemma 145 with probability at least $1-N^{-1}$ for every $\ell \in [L], \ell > 0$, there exists a matching of a $1-O(1/K)$ fraction of S^ℓ to $T^\ell \setminus T^\ell_*$ in $\widetilde{G}^\ell$. We condition on this event.

Denote the corresponding matching in $\widetilde{G}^\ell$ by $\widetilde{M}^\ell$. Now recall that by construction of the graph $\widehat{G}$ for every $(s,t) \in \widetilde{M}^\ell, s \in S^\ell, t \in T^\ell \setminus T^\ell_*$ one of the following two cases holds:

1. if $\tau^\ell(s)$ is not defined, and $(s,t) \in \widehat{E}$;

2. if $\tau^\ell(s)$ is defined, and $(\tau^\ell(s),t) \in \widehat{E}$.

Since τ^ℓ is injective, $\tau^\ell(\widetilde{M}^\ell)$ is a matching for every $\ell \in [L], \ell > 0$. Now recall that $\widetilde{M}^\ell$ matches S^ℓ to $T^\ell \backslash T^\ell_*$. At the same time τ^ℓ and maps S^ℓ to $T^{\ell-1}_*$, and whenever $\tau^\ell(s)$ is not defined, an edge $(s,t) \in S^\ell \times T^\ell$ is mapped to a separate set of vertices (see Υ_{even} and Υ_{odd} in (239) and (240)) in $\widehat{G}$. so the union of these matchings still forms a matching in $\widehat{G}$.

We thus get that $\bigcup_{\ell\in[L],\ell>0} \tau^\ell(\widetilde{M}^\ell)$ is a matching of size at least

$$(1 - O(1/K)) \sum_{\ell\in[L],\ell>0} |S^\ell| = (1 - O(1/K))(L-1) \cdot (N/2) = (1 - O(1/L))(L/2) \cdot N.$$

In the above we used the fact that $|S^\ell| \geq \sum_{k\in[K/2]} (1-\sqrt{\epsilon})|T_0|/K \geq (1-\sqrt{\epsilon})N/2$ by Lemma 85, **(2)**, together with (p5) and (p6), as well as the fact that $L \leq K$ by (p4).

We now upper bound $|P|$. By (239)

$$\begin{aligned}
|P| &= \left| \left(\bigcup_{\text{even } \ell\in[L]} T^\ell \right) \cup \left(\bigcup_{\text{odd } \ell\in[L],\ell>0} \{s \in S^\ell : \tau^\ell(s) \text{ is not defined}\} \right) \right| \\
&= \sum_{\text{even } \ell\in[L]} |T^\ell| + \sum_{\text{odd } \ell\in[L],\ell>0} |\{s \in S^\ell : \tau^\ell(s) \text{ is not defined}\}| \\
&\leq (1+\epsilon^{1/2})(L/2)N + \sum_{\text{odd } \ell\in[L],\ell>0} |\{s \in S^\ell : \tau^\ell(s) \text{ is not defined}\}| \\
&\leq (1+\epsilon^{1/2})(L/2)N + \delta^{1/4}N \\
&\leq (1+O(1/K))(L/2)N.
\end{aligned}$$

The third transition is by Lemma 85 the forth transition is by Lemma 128 and the final transition is by (p5) and (p6). Putting the two bounds together, we get that there exists a matching of size at least $(1-O(1/L))(L/2)\cdot N \geq (1-O(1/L))|P|$ with probability at least $1 - N^{-1}$, as required. ■

We now turn to upper bounding the performance of a small space streaming algorithm on our input distribution $\mathcal{D}$. Since the input is sampled from a distribution, we may assume by Yao's minimax principle that the streaming algorithm ALG is deterministic. Let ALG denote a deterministic streaming algorithm that uses s bits of space and at the end of the stream outputs a matching M_{ALG} in $\widehat{G}$ such that

$$\mathbf{Pr}_{\widehat{G}\sim\mathcal{D}} \left[|M_{ALG}| \geq \left(\frac{1}{1+\ln 2} + \eta \right) |M_{OPT}| \right] \geq 3/4$$

for some positive $\eta \in (0,1)$, where M_{OPT} is a maximum matching in $\widehat{G}$. Note that we are assuming that with probability at least $3/4$ both M_{ALG} is a matching in $\widehat{G}$ (i.e., in particular, the algorithm does not output edges that are not in $\widehat{G}$) and the size of M_{ALG} is large as above. At the same time by Lemma 150 one has

$$\mathbf{Pr}_{\widehat{G}\sim\mathcal{D}} \left[|M_{OPT}| < (1 - O(1/L))|P| \right] \leq N^{-1}.$$

Putting the two bounds above together, we get

$$\mathbf{Pr}_{\widehat{G}\sim\mathcal{D}} \left[|M_{ALG}| \geq \left(\frac{1}{1+\ln 2} + \eta - O(1/L) \right) |P| \right] \geq 1/2. \tag{244}$$

In what follows we show that any algorithm that achieves (244) must essentially remember, for many edges of $G^\ell, \ell \in [L]$, whether they were included in $\widetilde{G}^\ell$ and therefore in $\widehat{G}$.

Upper bounding $|M_{ALG}|$. Let sets $\Xi^\ell \subset T^\ell$ of 'outlier' vertices as defined in (216), and let $\Xi = \bigcup_{\ell \in [L]} \Xi^\ell$ as in (217). Define

$$\begin{aligned} A_P &= \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \nu_{\ell,*}(T^\ell \setminus \text{Ext}_\delta(T^\ell_*)) \right) \setminus \Xi \\ A_Q &= \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ odd}}} \nu_{\ell,*}(T^\ell \setminus \text{Ext}_\delta(T^\ell_*)) \right) \setminus \Xi. \end{aligned} \tag{245}$$

We define intermediate sets

$$\begin{aligned} B'_Q &= \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \mu_{\ell,*}(T^\ell \setminus T^\ell_*) \right) \cup \Xi \\ B'_P &= \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ odd}}} \mu_{\ell,*}(T^\ell \setminus T^\ell_*) \right) \cup \Xi, \end{aligned} \tag{246}$$

and then let

$$\begin{aligned} B_Q &= \bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \tau^\ell(B'_Q \cap S^\ell) \\ B_P &= \bigcup_{\substack{\ell \in [L] \\ \ell \text{ odd}}} \tau^\ell(B'_P \cap S^\ell). \end{aligned} \tag{247}$$

We have

Claim 151 *$A_P \cap B_P = \emptyset$ and $A_Q \cap B_Q = \emptyset$.*

Proof: We prove the first claim (the proof of the second is analogous). One has by (245)

$$\begin{aligned} A_P &= \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \nu_{\ell,*}(T^\ell \setminus T^\ell_*) \right) \setminus \Xi \\ &= \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \nu_{\ell,j}(T^\ell \setminus T^\ell_*) \right) \setminus \Xi \end{aligned} \tag{248}$$

and by (247) and (246)

$$\begin{aligned}B_P &= \bigcup_{\substack{\ell\in[L]\\ \ell\text{ odd}}} \tau^\ell(B'_P \cap S^\ell)\\ &= \left(\bigcup_{\substack{\ell\in[L]\\ \ell\text{ odd}}} \bigcup_{\substack{j=0\\ j\text{ even}}}^{\ell} \tau^{\ell-j}(\mu_{\ell,j}(T^\ell \setminus T^\ell_*))\right) \cup \Xi\\ &\subseteq \left(\bigcup_{\substack{\ell\in[L]\\ \ell\text{ odd}}} \bigcup_{\substack{j=0\\ j\text{ even}}}^{\ell} \nu_{\ell,j+1}(T^\ell \setminus T^\ell_*)\right) \cup \Xi\end{aligned} \tag{249}$$

Disjointness now follows by Lemma 135, **(2)**, since the range of (ℓ, j) pairs in (86) is disjoint from the range in (87). ■

Lemma 152 (Almost partition of P and Q) *One has*

$$|P \setminus (A_P \cup B_P)| = O(N)$$

and

$$|Q \setminus (A_Q \cup B_Q)| = O(N)$$

for sets A_P, A_Q, B_P, B_Q defined in (245) *and* (247).

The proof of the lemma is given in Appendix C.3.

The following lemma is key to bounding the size of the vertex cover that we construct in Lemma 154 to upper bound the size of M_{ALG}.

Lemma 153 *One has*

$$|B_Q| \le \frac{L}{2} \cdot \frac{N}{2} \cdot \frac{1}{1+\ln 2}(1 + O(1/K))$$

and

$$|B_P| \le \frac{L}{2} \cdot \frac{N}{2} \cdot \frac{1}{1+\ln 2}(1 + O(1/K))$$

Proof: We prove the bound for B_Q (the proof for B_P is analogous). By (247) and (246) we have

$$\begin{aligned}
|B_Q| &= \left| \bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}} \tau^\ell(B'_P \cap S^\ell) \right| \\
&\le \left| \bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}} B'_P \cap S^\ell \right| \\
&= |B'_P| \\
&\le \left| \left(\bigcup_{\substack{\ell\in[L]\\ \ell \text{ even}}} \mu_{\ell,*}(T^\ell \setminus T^\ell_*) \right) \cup \Xi \right| \\
&\le |\Xi| + \sum_{\substack{\ell\in[L]\\ \ell \text{ even}}} |\mu_{\ell,*}(T^\ell \setminus T^\ell_*)| \\
&\le \delta^{1/8}|P| + \sum_{\substack{\ell\in[L]\\ \ell \text{ even}}} |\mu_{\ell,*}(T^\ell \setminus T^\ell_*)|,
\end{aligned}$$

where the last transition is by Claim 141. Thus, it suffices to upper bound $|\mu_{\ell,*}(T^\ell \setminus T^\ell_*)|$ for $\ell \in [L]$.

Using Lemma 132 one has for every $\ell \in [L]$

$$\begin{aligned}
\left|\mu_{\ell,*}(T^\ell \setminus T^\ell_*)\right| &= \left| \bigcup_{\substack{0\le j\le \ell\\ j\ even}} \mu_{\ell,j}(T^\ell \setminus T^\ell_*) \right| \\
&= \bigcup_{\substack{0\le j\le \ell\\ j\ even}} \left|\mu_{\ell,j}(T^\ell \setminus T^\ell_*)\right| && \text{(since } \mu_{\ell,j}(T^\ell \setminus T^\ell_*) \text{ are disjoint for different } j \text{ by Lemma 126, } \textbf{(3)}\text{)} \\
&\le \sum_{\substack{0\le j\le \ell\\ j\ even}} (\ln 2 + C/K)^j \frac{1}{2}(1-\ln 2)|T^\ell| && \text{(by Lemma 132)} \\
&\le \frac{1}{2}(1-\ln 2)|T^\ell| \sum_{j\ge 0} (\ln 2 + C/K)^{2j} \\
&= \frac{1-\ln 2}{2}|T^\ell| \cdot \frac{1}{1-(\ln 2 + C/K)^2} \\
&= \frac{1}{2(1+\ln 2)}(1+O(1/K))|T^\ell|
\end{aligned}$$

We now note that $|T^\ell| = N$ for all $\ell \in [L]$. Summing the above over all even ℓ between 0 and $L-1$ gives the required upper bound. ■

Lemma 154 *For every matching $M \subseteq \widehat{E}$ one has*

$$|M| \le |M \cap (A_P \times (Q \setminus B_Q))| + \frac{1}{1+\ln 2}|P| + O(|P|/L).$$

Proof: We exhibit a vertex cover of appropriate size for M. Specifically, we add to the vertex cover one endpoint of every edge in

$$M \cap (A_P \times (Q \setminus B_Q)),$$

as well as all vertices in $P \setminus A_P \approx B_P$ and B_Q. Note that this is indeed a vertex cover: every edge of M either has an endpoint in $P \setminus A_P$, or belongs to $A_P \times (Q \setminus B_Q)$, or belongs to $A_P \times B_Q$, in which case it has an endpoint in B_Q.

The size of the vertex cover is

$$\begin{aligned} &|M \cap (A_P \times (Q \setminus B_Q))| + |P \setminus A_P| + |B_Q| \\ \le &|M \cap (A_P \times (Q \setminus B_Q))| + |B_P| + |B_Q| + O(N), \end{aligned} \tag{250}$$

where we used Lemma 152 to conclude that

$$|P \setminus A_P| \le |B_P| + |P \setminus (A_P \cup B_P)| = |B_P| + O(N).$$

By Lemma 153 we have

$$|B_P| \le \frac{L}{2} \cdot \frac{N}{2} \frac{1}{1 + \ln 2}(1 + O(1/K))$$

and

$$|B_Q| \le \frac{L}{2} \cdot \frac{N}{2} \frac{1}{1 + \ln 2}(1 + O(1/K)).$$

Putting the above together with (250) and recalling that $L \le \sqrt{K}$ by (p4) and that

$$|P| = \left| \bigcup_{\text{even } \ell \in [L]} T^\ell \right| = L \cdot N/2$$

gives the result. ■

We now prove

Lemma 155 *For every matching $M \subseteq \widehat{E}$ one has*

$$M \cap (A_P \times (Q \setminus B_Q)) \subseteq \bigcup_{\ell \in [L], k \in [K/2]} \tau^\ell(E^\ell_{k, \mathbf{j}^\ell_k}).$$

Proof: Suppose that $u \in A_P, v \in Q \setminus B_Q$ and $(u, v) \in M$. Let $\ell \in [L]$ be an even integer such that $u \in T^\ell$. Such an ℓ exists because by (245) one has

$$A_P = \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \nu_{\ell,*}(T^\ell \setminus \mathrm{Ext}_\delta(T^\ell_*)) \right) \setminus \Xi$$

and by Definition 130 one has

$$\nu_{\ell,*}(T^\ell \setminus \mathrm{Ext}_\delta(T^\ell_*)) := \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \nu_{\ell,j}(T^\ell \setminus \mathrm{Ext}_\delta(T^\ell_*)),$$

so that

$$\nu_{\ell,*}(T^\ell \setminus \text{Ext}_\delta(T^\ell_*)) \subseteq \bigcup_{\text{even } \ell\in[L]} T^\ell.$$

Uniqueness of ℓ follows by Lemma 135, **(2)**. Furthermore, we get that

$$u \in \nu_{\ell+j,j}(T^{\ell+j} \setminus \text{Ext}_\delta(T^{\ell+j}_*)) \setminus \Xi \tag{251}$$

for some even $\ell \in [L]$ and even j.

We now consider two cases: depending on whether $v \in T^{\ell-1}$ (**case 1**) or $v \in T^{\ell+1}$ (**case 2**).

Case 1. In this case there exists a unique $y \in S^\ell$ such that $\tau^\ell(y) = v$. Indeed, otherwise the edge (u, v) would not be in the graph $\widehat{G}$ as per (242) and (243); uniqueness follows from injectivity of τ^ℓ. Letting $x = u$, we now show using Corollary 144 that $y \in \mu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*)$, which in turn by (247) together with the definition of $\mu_{\ell,*}$ (Definition 130) implies that $v = \tau^\ell(y) \in B_Q$, as required. We now provide the details.

Let $k \in [K/2]$ be the unique index such that $x \in T^\ell_k$ and $y \in S^\ell_k$. Uniqueness follows since the edge sets in (108) are disjoint by Lemma 98. Note that $x \notin \Xi$ since we excluded this set in (245). If $y \in \Xi$, we have $y \in B_Q$ and there is nothing to prove. Thus, it suffices to consider the case $y \notin \Xi$.

We thus have $x \in T^\ell_k \setminus \Xi$ and $y \in S^\ell_k \setminus \Xi$. Furthermore, since $(u, v) = \tau^\ell((y, x))$, the assumption that $(u, v) \in \widehat{E}$ implies that $(x, y) \in E^\ell$, and therefore

$$y = x + \lambda \cdot \mathbf{u}$$

for some $\mathbf{u} \in \mathring{\mathbf{B}}^\ell_k$. Furthermore, it follows by Lemma 92 that $|\lambda| \le 2M/w$. We assume towards a contradiction that $\mathbf{u} \neq \mathbf{j}^\ell_k$. Since

$$\widetilde{\Psi}(\mathbf{B}^\ell) \cap \mathring{\mathbf{B}}^\ell_k = \{\mathbf{j}^\ell_k\},$$

this means that $\mathbf{u} \notin \widetilde{\Psi}(\mathbf{B}^\ell)$ (see (96) for the definition of $\widetilde{\Psi}$). This means, since $\mathring{\mathbf{B}}^\ell \subset \mathbf{B}^\ell$, that the preconditions of Corollary 144 are satisfied and we get that

$$x \in \nu_{\ell+j,j}(T^{\ell+j} \setminus \text{Ext}_\delta(T^{\ell+j}_*)),$$

implies

$$y \in \mu_{\ell+j,j}(T^{\ell+j} \setminus T^{\ell+j}_*).$$

At the same time by Definition 130 for every $\ell \in [L]$

$$\mu_{\ell,*}(T^\ell \setminus T^\ell_*) := \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \mu_{\ell,j}(T^\ell \setminus T^\ell_*),$$

which means that $y \in \mu_{\ell,*}(T^\ell \setminus T^\ell_*) \subseteq B'_Q$ as per (246). Therefore, $v = \tau^\ell(y) \in B_Q$, as required.

Case 2. In this case there exists a unique $x' \in S^{\ell+1}$ such that $\tau^{\ell+1}(x') = u$. Indeed, otherwise the edge (u, v) would not be in the graph $\widehat{G}$ as per (242) and (243); uniqueness follows from injectivity of $\tau^{\ell+1}$. Let $x \in T^{\ell+1}$ be such that $x \asymp x'$. Let $y = v$. Let $k \in [K/2]$ be the unique index such that $y \in T^{\ell+1}_k$ and $x' \in S^{\ell+1}_k$. Uniqueness follows since the edge sets in (108) are disjoint by Lemma 98. Note that $x \notin \Xi$ since we excluded this set in (245). If $y \in \Xi$, we have $y \in B_Q$ and there is nothing to prove. Thus, it suffices to consider the case $y \notin \Xi$. We thus have $y \in T^{\ell+1}_k \setminus \Xi$ and $x' \in S^{\ell+1}_k \setminus \Xi$.

Since $(u, v) = \tau^{\ell+1}((x', y))$, the assumption that $(u, v) \in \widehat{E}$ implies that $(x', y) \in E^{\ell+1}$, and therefore, since $x \asymp x'$,

$$y = x + \lambda \cdot \mathbf{u}$$

for some $\mathbf{u} \in \mathring{\mathbf{B}}_k^{\ell+1}$. Furthermore, it follows by Lemma 92 that $|\lambda| \leq 2M/w$. We assume towards a contradiction that $\mathbf{u} \neq \mathbf{j}_k^{\ell+1}$. Since

$$\widetilde{\Psi}(\mathbf{B}^{\ell+1}) \cap \mathring{\mathbf{B}}_k^{\ell+1} = \{\mathbf{j}_k^{\ell+1}\},$$

this means that $\mathbf{u} \notin \widetilde{\Psi}(\mathbf{B}^{\ell+1})$, and therefore, since $\mathring{\mathbf{B}}^{\ell+1} \subseteq \mathbf{B}^{\ell+1}$, the preconditions of Lemma 143 are satisfied for x, y and $\ell + 1$. Furthermore, by (251) we have

$$\begin{aligned} u &= \tau^{\ell+1}(x') \\ &\in \nu_{\ell+j,j}(T^{\ell+j} \setminus \text{Ext}_\delta(T_*^{\ell+j})) \\ &\subseteq \tau^{\ell+1}\left(\mu_{\ell+j,j-1}(T^{\ell+j} \setminus \text{Ext}_\delta(T_*^{\ell+j}))\right), \end{aligned}$$

and therefore $x' \in \mu_{\ell+j,j-1}(T^{\ell+j} \setminus \text{Ext}_\delta(T_*^{\ell+j}))$. Since

$$\mu_{\ell+j,j-1}(T^{\ell+j} \setminus \text{Ext}_\delta(T_*^{\ell+j})) = \textsc{DownSet}^{\ell+1}(\nu_{\ell+j,j-1}(T^{\ell+j} \setminus \text{Ext}_\delta(T_*^{\ell+j}))),$$

we have, since $x \asymp x'$,

$$x \in \nu_{\ell+j,j-1}(T^{\ell+j} \setminus \text{Ext}_\delta(T_*^{\ell+j})) = \nu_{(\ell+1)+(j-1),j-1}(T^{(\ell+1)+(j-1)} \setminus \text{Ext}_\delta(T_*^{(\ell+1)+(j-1)})).$$

This means that the preconditions of Lemma 143 are satisfied, and we have [8]

$$\begin{aligned} y \in \nu_{(\ell+1)+(j-1),j-1}(T^{(\ell+1)+(j-1)} \setminus T_*^{(\ell-1)+(j-1)}) &= \nu_{\ell+j,j-1}(T^{\ell+j} \setminus T_*^{\ell+j}) \\ &= \tau^{\ell+2}(\mu_{\ell+j,j-2}(T^{\ell+j} \setminus T_*^{\ell+j})). \end{aligned}$$

At the same time by Definition 130 for every $\ell \in [L]$

$$\mu_{\ell,*}(T^\ell \setminus T_*^\ell) := \bigcup_{\substack{i=0 \\ i \text{ even}}}^{\ell} \mu_{\ell,i}(T^\ell \setminus T_*^\ell),$$

which means that $y \in \tau^{\ell+2}(\mu_{\ell+j,*}(T^{\ell+j} \setminus T_*^{\ell+j}) \cap S^{\ell+2}) \subseteq B_Q$ as per (246), as required. ■

7.3 Proof of Theorem 1

We now give

Proof of Theorem 1: Now putting (244) together with Lemma 154, we get

$$\begin{aligned} |M_{ALG} \cap (A_P \times (Q \setminus B_Q))| &\geq |M_{ALG}| - \left(\frac{1}{1+\ln 2}|P| + O(|P|/L)\right) \\ &\geq \left(\frac{1}{1+\ln 2} + \eta - O(1/K)\right)|P| - \left(\frac{1}{1+\ln 2}|P| + O(|P|/L)\right) \\ &\geq (\eta - O(1/L))|P| \\ &\geq (\eta/2)|P|, \end{aligned}$$

[8] When $\ell + 1 = L - 1$, we have $\ell + 2 = L$, which does not technically correspond to a gadget in our input graph. However, we think of artifically adding such a gadget here to handle this corner case for simplicity.

where we used (244) in the third transition and the fact that $L \leq \sqrt{K}$ by (p3) in the forth transition, and assumed that $L = \sqrt{K}$ is larger than an absolute constant that depends on η in the last transition. Thus,

$$\mathbf{Pr}_{\widehat{G}\sim\mathcal{D}}\left[|M_{ALG} \cap (A_P \times (Q \setminus B_Q))| \geq (\eta/4)|P| \text{ and } M_{ALG} \subseteq \widehat{E}\right] \geq 1/2. \tag{252}$$

Note that the second condition above, namely $M_{ALG} \subseteq \widehat{E}$ enforces the constraint that the algorithm does not output non-edges[9]. We do not add this condition explicitly in calculations below to simplify notation (one can think of $|M_{ALG}|$ as being defined as zero when M_{ALG} contains non-edges). Now recall that by Lemma 155 we have

$$M_{ALG} \cap (A_P \times (Q \setminus B_Q)) \subseteq \bigcup_{\ell\in[L],k\in[K/2]} \tau^\ell(E^\ell_{k,\mathbf{J}^\ell_k}) = \bigcup_{\ell\in[L],k\in[K/2]} \widehat{E}^\ell_{k,\mathbf{J}^\ell_k}.$$

Thus, there exist $\ell^* \in [L], k^* \in [K/2]$ such that

$$\mathbf{Pr}\left[|M_{ALG} \cap \widehat{E}^{\ell^*}_{k^*,\mathbf{j}^\ell_{k^*}}| \geq \frac{\eta}{2KL}|P|\right] \geq \frac{1}{KL}. \tag{253}$$

Indeed, otherwise one would have

$$\begin{aligned}
&\mathbf{Pr}[|M_{ALG} \cap (A_P \times (Q \setminus B_Q))| \geq (\eta/4)|P|] \\
&\qquad\leq \mathbf{Pr}\left[\text{exist } \ell \in [L] \text{ and } k \in [K/2] \text{ such that } |M_{ALG} \cap E^\ell_{k,\mathbf{j}^\ell_k}| \geq \frac{\eta}{2LK}|P|\right] \\
&\qquad\leq \sum_{\ell\in[L]} \sum_{k\in[K/2]} \mathbf{Pr}\left[|M_{ALG} \cap E^\ell_{k,\mathbf{j}^\ell_k}| \geq \frac{\eta}{2KL}|P|\right] \\
&\qquad< \sum_{\ell\in[L]} \sum_{k\in[K/2]} \frac{1}{KL} \\
&\qquad= (KL/2) \cdot \frac{1}{KL} \\
&\qquad= 1/2,
\end{aligned}$$

a contradiction with (252).

To simplify notation, we let $\ell = \ell^*, k = k^*$. Let that by Definition 147 we write $\widehat{G}_{<(\ell,k)}$ to denote the subgraph of $\widehat{G}$ that arrives up to the k-th phase of the ℓ-th round. Also recall that **(a)** $\widehat{G}_{\leq(\ell,k)}$ is fully determined by $\Lambda_{<(\ell,k)}$ and X^ℓ_k (see Definition 148) and **(b)** conditioned on $\Lambda_{<(\ell,k)}$ and X^ℓ_k one has $\mathbf{j}^\ell_k \sim UNIF(\mathring{\mathbf{B}}^\ell_k)$. For simplicity of notation we write

$$\mathbf{B} = \mathbf{B}^\ell_k,\ \mathring{\mathbf{B}} = \mathring{\mathbf{B}}^\ell_k \text{ and } \mathbf{j} = \mathbf{j}^\ell_k.$$

Recall that $\mathring{\mathbf{B}}^\ell_k = \mathbf{B}^\ell_k \setminus \text{Ext}^\ell_k \cup \{\mathbf{q}^\ell_k, \mathbf{r}^\ell\}$. We also let

$$S_k = S^\ell_k \text{ and } X := X^\ell_k.$$

[9] The analysis generalizes easily to the setting where the algorithm is allowed to output a small fraction of non-edges, but this is a rather non-standard assumption, and we prefer to operate under the more standard model where M_{ALG} must be a subset of $\widehat{E}$ with a good probability.

Lower bounding the space usage of ALG. In what follows we show that since M_{ALG} often returns many edges from $\widehat{G}_{(\ell,k)}$ as per (253), the conditional entropy of X_k^ℓ given Π and $\Lambda_{\leq(\ell,k)}$ is low, which gives the desired lower bound on s. Let $\Pi \in \{0,1\}^s$ denote the state of ALG after it has been presented with $\widehat{G}_{\leq(\ell,k)}$. Then finish running ALG on $\widehat{G}_{>(\ell,k)}$ starting with state Π. Let M_{ALG} denote the matching output by ALG. We have

$$\begin{aligned} s = |\Pi| &\geq H(\Pi) \\ &\geq H(\Pi|\Lambda_{<(\ell,k)}) \\ &\geq I(\Pi; X|\Lambda_{<(\ell,k)}) \\ &\geq \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} I(\Pi; X_{\mathbf{i}}|\Lambda_{<(\ell,k)}) \\ &= \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} I(\Pi; X_{\mathbf{i}}|\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}) \\ &\geq \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} I(M_{ALG}; X_{\mathbf{i}}|\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}) \end{aligned} \tag{254}$$

The second transition uses the fact that conditioning does not increase entropy, the forth transition uses the fact that $X_{\mathbf{i}}$'s are independent conditioned on $\Lambda_{<(\ell,k)}$, the forth transition uses the fact that $\mathbf{j}$ is independent of Π and $X_{\mathbf{i}}$ conditioned on $\Lambda_{<(\ell,k)}$. The final transition is by the data processing inequality:

Lemma 156 (Data Processing Inequality) *For any random variables (X, Y, Z) such that $X \to Y \to Z$ forms a Markov chain, we have $I(X;Z) \leq I(X;Y)$.*

Recall that we let $\ell = \ell^*$ and $k = k^*$, where ℓ^* and k^* satisfy (253), and let $\mathbf{j} = \mathbf{j}_k^\ell$, to simplify notation. We now lower bound

$$\begin{aligned} \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} I(M_{ALG}; X_{\mathbf{i}}|\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}) &= \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} H(X_{\mathbf{i}}|\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}) - H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}) \\ &= \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} H(X_{\mathbf{i}}) - H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}). \end{aligned} \tag{255}$$

We now upper bound $H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\})$ on the rhs of (255). Let

$$\mathcal{E} := \left\{|M_{ALG} \cap E_{k,\mathbf{j}}^\ell| \geq \frac{\eta}{2KL}|P| \text{ and } M_{ALG} \subseteq \widehat{E}\right\} \tag{256}$$

and let Z denote the indicator of $\mathcal{E}$. Note that $\mathbf{E}[Z] = \mathbf{Pr}[\mathcal{E}] \geq \frac{1}{KL}$ by (253). We have

$$\begin{aligned} H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}) &\leq H(X_{\mathbf{i}}, Z|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}) \\ &\leq H(Z) + H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}, Z) \\ &\leq 1 + H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}, Z), \end{aligned} \tag{257}$$

where we used the fact that $H(Z) \leq 1$, as Z is a binary variable. At the same time, since $\mathbf{E}[Z] = \mathbf{E}_{\mathbf{i}\sim UNIF(\mathring{\mathbf{B}})}[Z|\{\mathbf{j}=\mathbf{i}\}] \geq \frac{1}{KL}$ by (253), and $\mathbf{j} \sim UNIF(\mathring{\mathbf{B}})$, there exists a subset $\mathcal{J} \subseteq \mathring{\mathbf{B}}$ such that $|\mathcal{J}| \geq \frac{1}{KL}|\mathring{\mathbf{B}}|$ and for every $\mathbf{i} \in \mathcal{J}$ one has $\mathbf{E}[Z|\{\mathbf{j}=\mathbf{i}\}] \geq \frac{1}{KL}$. For every $\mathbf{i} \in \mathcal{J}$ one has

$$\begin{aligned} H(X_{\mathbf{i}}|M_{ALG}, &\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}, Z) \\ &= H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i} \wedge Z=1\}) \cdot \mathbf{Pr}[Z=1|\{\mathbf{j}=\mathbf{i}\}] \\ &+ H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i} \wedge Z=0\}) \cdot \mathbf{Pr}[Z=0|\{\mathbf{j}=\mathbf{i}\}] \end{aligned} \tag{258}$$

We now bound both terms on the rhs in (258). For the second term we have

$$\begin{aligned} H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i} \wedge Z=0\}) &\leq \mathbf{E}_{\Lambda_{<(\ell,k)}}[|S_k|] \cdot H_2(1-1/K) \\ &\leq (1+\sqrt{\epsilon})\frac{1}{K}|T| \cdot H_2(1-1/K) \end{aligned} \tag{259}$$

where the first transition is because $\sum_{y \in S_k} X_{\mathbf{i}}(y) = \lceil (1-\frac{1}{K})|S_k| \rceil$ by definition of $X_{\mathbf{i}}$ and the second transition is by Lemma 85, **(2)**.

For the first term on the rhs in (258) we note that since $M_{ALG} \subseteq \widehat{E}$ as we are conditioning on the event $\mathcal{E}$ (by conditioning on $\{Z=1\}$) for every $y \in S_k$ that is matched by M_{ALG} one has $X_{\mathbf{i}}(y)=1$. By conditioning on $\{Z=1 \wedge \mathbf{j}=\mathbf{i}\}$, we get by (256) $|M_{ALG} \cap E^{\ell}_{k,\mathbf{i}}| \geq \frac{\eta|P|}{2KL}$, and hence

$$\gamma := \frac{|M_{ALG} \cap E^{\ell}_{k,\mathbf{i}}|}{|S_k|} \geq \frac{\eta|P|}{2KL|S_k|} \geq \frac{\eta|T|}{4K|S_k|} \geq \eta/8.$$

For every fixing λ of $\Lambda_{<(\ell,k)}$ one has,

$$H(X_{\mathbf{i}}|M_{ALG}, \{\Lambda_{<(\ell,k)}=\lambda \wedge \mathbf{j}=\mathbf{i} \wedge Z=1\}) \leq (1-\gamma)|S_k| H_2\left(1-\frac{1}{K(1-\gamma)}\right),$$

since conditioned on M_{ALG}, $\lambda, \mathbf{j}=\mathbf{i}$ and the success event $Z=1$ there are exactly $(1-\gamma)|S_k|$ values of $y \in S_k \setminus M_{ALG}$ such that $X_{\mathbf{i}}(y)=1$, and hence the conditional entropy of $X_{\mathbf{i}}$ is bounded by

$$\begin{aligned} \log_2 \binom{|S_k \setminus M_{ALG}|}{(1-\frac{1}{K}-\gamma)|S_k|} &= \log_2 \binom{(1-\gamma)|S_k|}{(1-\frac{1}{K}-\gamma)|S_k|} \\ &= \log_2 \binom{(1-\gamma)|S_k|}{(1-\frac{1}{K(1-\gamma)})(1-\gamma)|S_k|} \\ &\leq (1-\gamma)|S_k| H_2\left(1-\frac{1}{K(1-\gamma)}\right), \end{aligned}$$

where the last transition is by subadditivity of entropy. Recalling that $\gamma \geq \eta/8$ and $\eta > 0$ is a small constant we bound the rhs above by

$$\begin{aligned} (1-\gamma)|S_k| H_2\left(1-\frac{1}{K(1-\gamma)}\right) &\leq (1-\eta/8)|S_k| H_2\left(1-\frac{1}{K(1-\eta/8)}\right) \\ &\leq (1+\sqrt{\epsilon})\frac{1}{K}|T| \cdot (1-\eta/8) H_2\left(1-\frac{1}{K(1-\eta/8)}\right), \end{aligned} \tag{260}$$

where in the second transition we also used the fact that by Lemma 85, **(2)**, we have $|S_k| \leq (1+\sqrt{\epsilon})\frac{1}{K}|T|$. At this point we also note that

$$\begin{aligned} (1-\eta/8) H_2\left(1-\frac{1}{K(1-\eta/8)}\right) &= \frac{1}{K}\log_2 K + \frac{1}{K \ln 2} - \frac{1}{K}\log\frac{1}{1-8/\eta} + O(1/K^2) \\ &\leq H_2(1-1/K) - \frac{1}{K}\log\frac{1}{1-\eta/8} + O(1/K^2). \end{aligned}$$

since $H_2(1-1/K) = \frac{1}{K}\log_2 K + \frac{1}{K \ln 2} + O(1/K^2)$ and K is larger than a constant. Putting the above bounds together, we get, assuming that K is larger than $1/\eta$ by a large constant factor,

$$H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i} \wedge Z=1\}) \leq (1+\sqrt{\epsilon})\frac{1}{K}|T| \cdot H_2(1-1/K) - \Omega(\eta/K)|T|.$$

for every $\mathbf{i} \in \mathcal{J}$, which by (258) implies for $\mathbf{i} \in \mathcal{J}$

$$H(X_{\mathbf{i}}|M_{ALG},\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}, Z) \le (1+\sqrt{\epsilon})\frac{1}{K}|T| \cdot H_2(1-1/K) - \Omega\left(\frac{\eta}{K^2L^2}\right)|P| \tag{261}$$

Finally, for $\mathbf{i} \in \mathring{\mathbf{B}} \setminus \mathcal{J}$ we have the bound

$$H(X_{\mathbf{i}}|M_{ALG},\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}, Z) \le (1+\sqrt{\epsilon})\frac{1}{K}|T| \cdot H_2(1-1/K), \tag{262}$$

since the number of nonzeros in $X_{\mathbf{i}}$ is exactly $\lceil(1-1/K)|S_k\rceil$. Putting (261) and (262) together with (255) and using (257), we get

$$\begin{aligned} H(X|\Pi,\Lambda_{<(\ell,k)}) &\le \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} H(X_{\mathbf{i}}|M_{ALG},\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}) \\ &\le \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} (1+H(X_{\mathbf{i}}|M_{ALG},\Lambda_{<(\ell,k)}, \{\mathbf{j}=\mathbf{i}\}, Z)) \\ &\le \sum_{\mathbf{i}\in\mathcal{J}} \left(H(X_{\mathbf{i}}|\Lambda_{<(\ell,k)}) - \Omega\left(\frac{\eta}{K^2L^2}\right)|P|\right) + \sum_{\mathbf{i}\in\mathring{\mathbf{B}}\setminus\mathcal{J}} H(X_{\mathbf{i}}|\Lambda_{<(\ell,k)}) \\ &= \sum_{\mathbf{i}\in\mathring{\mathbf{B}}} H(X_{\mathbf{i}}|\Lambda_{<(\ell,k)}) - |\mathcal{J}|\cdot\Omega\left(\frac{\eta}{K^2L^2}\right)|P|. \end{aligned}$$

On the other hand, since $|S_k| \ge (1-\sqrt{\epsilon})\frac{1}{K}|T|$ for all choices of $\Lambda_{<(\ell,k)}$ by Lemma 85, **(2)**, we get, since the nonzeros of $X_{\mathbf{i}}$ are a uniformly random set of size $\lceil(1-1/K)|S_k|\rceil$, that

$$H(X|\Lambda_{<(\ell,k)}) \ge (1-\sqrt{\epsilon})\frac{1}{K}|T|\cdot|\mathring{\mathbf{B}}|\cdot(1-o_N(1))H_2(1-1/K).$$

Substituting this into (255), we get

$$\begin{aligned} s = |\Pi| &\ge \Omega\left(\frac{\eta}{K^2L^2}\right)|\mathcal{J}|\cdot|P| - O(\sqrt{\epsilon})\frac{1}{K}|T|\cdot|\mathring{\mathbf{B}}|\cdot H_2(1-1/K) \\ &\ge \Omega\left(\frac{\eta}{K^2L^2}\right)|\mathcal{J}|\cdot|P| \qquad \text{(since } \epsilon < K^{-100K^2} \text{ by (p6), (p5) and (p3))} \\ &\ge \Omega\left(\frac{\eta}{K^3L^3}\right)|\mathring{\mathbf{B}}|\cdot|P| \qquad \text{(since } |\mathcal{J}| \ge |\mathring{\mathbf{B}}|/(KL)\text{)} \\ &\ge \Omega_K(|\mathring{\mathbf{B}}|\cdot|P|). \end{aligned}$$

Now note that $|\mathring{\mathbf{B}}| \ge (1/2)|\mathbf{B}|$ since $|\mathrm{Ext}_k^\ell| \le K$ and n is sufficiently large as a function of K. Finally, recall that by (p0)

$$N = m^n = n^{20n},$$

and therefore

$$|\mathbf{B}| \ge |\mathcal{F}|/(KL) = 2^{\Omega(\epsilon^2 n)} = N^{\Omega_\epsilon(1/\log\log N)}.$$

To summarize, since $|P| = O(L)N$ and L is an absolute constant, we get a lower bound of

$$s = \Omega_K(|\mathbf{B}|\cdot|P|) = |P|^{1+\Omega(1/\log\log|P|)},$$

as required.

■

Acknowledgements

This project has received funding from the European Research Council (ERC) under the European Union?s Horizon 2020 research and innovation programme (grant agreement No 759471).

A Proof of Lemma 4

Proof of Lemma 4: Fix $\ell \in [L]$, and let $G^\ell = (S^\ell, T^\ell, E^\ell)$ denote the ℓ-th gadget graph. Let $(E')^\ell$ denote a subset of E^ℓ that contains every edge independently with probability $C/(\epsilon^2 n)$ for an absolute constant $C > 0$. We show that with high probability over the choice of $(E')^\ell$ the edge set $(E')^\ell$ contains a matching of at least a $1-\epsilon$ fraction of S^ℓ to $T^\ell \setminus T^\ell_*$. We drop the superscript ℓ to simplify notation.

Now note that for every subset $A \subseteq S$ and $B \subseteq T \setminus T_*$ such that $|A| \geq |B| - \epsilon n$ one has

$$|E \cap (A \times (T \setminus (T_* \cup B)))| \geq (\epsilon n/2)^2. \tag{263}$$

Indeed, sort elements of $A = \{a_1, \ldots, a_r\}, r = |A|$, so that $\pi(a_1) \leq \pi(a_2) \leq \ldots, \pi(a_r)$. We have for every $i = 1, \ldots, r$ that $\pi(a_i) \geq n/2 - r + i$. Since a_i has an edge to every $j \in T$ such that $j \geq \pi(a_i)$, we have that the degree of a_i in E is lower bounded by $n/2 + r - i$. At most $|T_* \cup B| = |T_*| + |B| \leq n/2 + (r - \epsilon n)$ of these edges go to $T_* \cup B$ (this is where we use that $|B| \leq |A| + \epsilon n$), and therefore the i-th vertex in A contributes at least $(n/2 + r - i) - (n/2 + (r - \epsilon n)) \geq \epsilon n - i$. Thus, the first $\epsilon n/2$ vertices in A have degree at least $\epsilon n/2$ outside of $T_* \cup B$, which proves (263). The probability that none of these edges are included in the sample E' is bounded by

$$\left(1 - \frac{C}{\epsilon^2 n}\right)^{(\epsilon n/2)^2} = \left(1 - \frac{C}{\epsilon^2 n}\right)^{\epsilon^2 n^2/4} \leq \exp(-Cn/4) \leq 2^{-4n}.$$

Taking a union bound over all choices of $A \subseteq S, B \subseteq T \setminus T_*$ (at most 2^{2n} choices), we get that with high probability for every $A \subseteq S$, every $B \subseteq T \setminus T_*$ such that $|A| \geq |B| + \epsilon n$ one has

$$E' \cap (A \times (T \setminus (T_* \cup B))) \neq \emptyset.$$

This precludes the existence of a vertex cover in $E' \cap (S \times (T \setminus T_*))$ of size smaller than $|S| - \epsilon n$, and thus there exists a matching of all but ϵn vertices in S to $T \setminus T_*$, as required. Combining these matchings over all gadgets gives a $1 - O(\epsilon)$-approximation to the maximum matching in $\widehat{G} = (P, Q, \widehat{E})$. ■

B Proofs omitted from Section 3

B.1 Proof of Lemma 33

Proof: We start by proving **(1)**. Due to the assumption that $y \in T_k$ we have

$$\begin{aligned}\text{line}_j(y) &= \left\{y' \in [m]^n : (y' - y)_s = 0 \text{ for all } s \neq j\right\}\\ &= \left\{y' \in [m]^n : (y' - y)_s = 0 \text{ for all } s \neq j\right\}.\end{aligned}$$

Since there are exactly m possible values for y'_j one has $|\text{line}_j(y)| = m$. Also note that $j \notin J_{<k}$, since $j \in \mathbf{B}_k$, $J_{<k} \in \mathbf{B}_{<k}$ and $\mathbf{B}_{<k} \cap \mathbf{B}_k = \emptyset$. Thus, every $y' \in \text{line}_j(y)$ coincides with y on all coordinates $s \in J_{<k}$, so $y'_{j_s}/m \in \left[0, 1 - \frac{1}{K-s}\right)$ for all $s \in \{0, 1, \ldots, k-1\}$ per (28), and hence we have $y' \in T_k$ and $\text{line}_j(y) \subseteq T_k$.

For **(2)**, we note that since $(K-s)|m$ for every $s \in [K/2]$ by (p0) and (p1), there are exactly $m/(K-k)$ values for y'_j, namely $\{m/(K-k), m/(K-k)+1, \ldots, m-1\}$, that result in $y' \notin T_k^j$, by definition of T_k^j (see (31)).

For **(3)**, we recall that by (30)

$$S_k = \left\{ x \in T_k : \text{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \right\}.$$

For every $x \in T_k$ one has

$$\text{line}_j(x) \cap S_k = \left\{ x' \in [m]^n : x'_{-j} = x_{-j} \text{ and } \text{wt}(x') \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \right\}$$

Write $x' = (x'_{-j} x'_j)$, where $x'_{-j} \in [m]^{[n]\setminus\{j\}}$. Note that by definition of wt(x') (Definition 24)

$$\text{wt}(x') = \text{wt}(x'_{-j}) + x'_j.$$

We thus get

$$\begin{aligned}
|\text{line}_j(x) \cap S_k| &= \left| \left\{ x' \in [m]^n : x'_{-j} = x_{-j} \text{ and } \text{wt}(x') \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \right\} \right| \\
&= \left| \left\{ x' \in [m]^n : x'_{-j} = x_{-j} \text{ and } \text{wt}(x'_{-j}) + x'_j \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \right\} \right| \\
&= \frac{1}{K-k} \left| \left\{ x' \in [m]^n : x'_{-j} = x_{-j} \right\} \right| \\
&= \frac{1}{K-k} \left| \text{line}_j(x) \right|,
\end{aligned}$$

where the last equality uses the fact that since $W \mid m$ and $(K-k) \mid W$ by (p0) and (p1), exactly a $\frac{1}{K-k}$ fraction of settings of $x_j \in [m]$ result in

$$\text{wt}(x') = \text{wt}(x'_{-j}) + x'_j \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W}.$$

This establishes **(3)**.

For **(4)**, we first recall that by (31)

$$S_k^j = \left\{ x \in S_k : x_j/m \in \left[0, 1 - \frac{1}{K-k}\right) \right\}.$$

Thus for every $x \in S_k^j$ one has

$$\begin{aligned}
\left|\text{line}_j(x) \cap S_k^j\right| = \Bigg| \Bigg\{ x' \in [m]^n : x'_{-j} = x_{-j} \text{ and } \text{wt}(x') \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod{W} \\
\text{and} \\
x'_j/m \in \left[0, 1 - \frac{1}{K-k}\right) \Bigg\} \Bigg| \\
= \frac{1}{K-k} \left| \left\{ x' \in [m]^n : x'_{-j} = x_{-j} \text{ and } x'_j/m \in \left[0, 1 - \frac{1}{K-k}\right) \right\} \right|
\end{aligned}$$

where the last equality uses the fact that exactly $\frac{1}{K-k}$ fraction of settings of $x'_j \in \left\{0, 1, \ldots, (1 - \frac{1}{K-k})m - 1\right\}$ lead to

$$\mathrm{wt}(x') = \mathrm{wt}(x'_{-j}) + x'_j \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W.$$

since $(K-k) \mid m$ and $W \mid m/(K-k)$ by (p0) and (p1). We now note that since $K-k \mid m$, we get

$$\left|\left\{x' \in [m]^n : x'_{-j} = x_{-j} \text{ and } x'_j/m \in \left[0, 1 - \frac{1}{K-k}\right)\right\}\right| = \left(1 - \frac{1}{K-k}\right) |\mathrm{line}_j(x)|.$$

Putting the two bounds together yields the result. ■

B.2 Proof of Lemma 32

Proof of Lemma 32: We start by proving **(1)**:

$$\begin{aligned}
|T_k| &= |T_0| \cdot \mathbf{Pr}_{y \sim UNIF([m]^n)} \left[y_{j_s/m} \in \left[0, 1 - \frac{1}{K-s}\right) \text{ for every } s = 0, \ldots, k-1 \right] \\
&= |T_0| \cdot \prod_{s=0}^{k-1} \mathbf{Pr}_{y \sim UNIF([m]^n)} \left[y_{j_s}/m \in \left[0, 1 - \frac{1}{K-s}\right) \right] \\
&= |T_0| \cdot \prod_{s=0}^{k-1} \left(1 - \frac{1}{K-s}\right) \qquad \text{(since } K-s \text{ divides } m \text{ for all } s \in [K/2] \text{ by assumption)} \\
&= |T_0| \cdot \prod_{s=0}^{k-1} \frac{K-s-1}{K-s} \\
&= |T_0| \cdot \frac{K-(k-1)-1}{K} \\
&= |T_0| \cdot (1 - k/K),
\end{aligned}$$

as required.

We now prove **(2)**. Pick any coordinate $r \in \mathbf{B}_k$, and recall that T_k does not depend on r, i.e. for every $x_{-r} \in [m]^{[n]\setminus\{r\}}$ such that $(x_r, x_{-r}) \in T_k$ for some $x_r \in [m]$ one has (x_r, x_{-r}) for every $x_r \in [m]$. This is because by (28) T_k only depends on coordinates in $\mathbf{B}_{<k}$. This means that

$$\begin{aligned}
|S_k| &= \mathbf{Pr}_{x \sim UNIF(T_k)} \left[\sum_{s \in [n]} x_s \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W \right] \\
&= \mathbf{E}_{x_{-r} \sim UNIF(T_k)} \left[\mathbf{Pr}_{x_r \sim UNIF([m])} \left[\sum_{s \in [n]} x_s \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W \right] \right],
\end{aligned} \tag{264}$$

where we used the fact that T_k is independent of r to conclude that $x_r \sim UNIF([m])$ in the inner probability regardless of the choice of x_{-r}. For the inner probability we get

$$\begin{aligned}
&\mathbf{Pr}_{x_r \sim UNIF([m])} \left[\sum_{s \in [n]} x_s \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W \right] \\
&= \mathbf{Pr}_{x_r \sim UNIF([m])} \left[x_r \in \left(\left[0, \frac{1}{K-k}\right) \cdot W - \sum_{s \in [n]\setminus\{r\}} x_s \right) \pmod W \right] \\
&= \frac{1}{K-k},
\end{aligned}$$

where the last line uses the assumption that $K-k \mid W$ and $W \mid m$. Substituting this into (264), we get $|S_k| = \frac{1}{K-k}|T_k|$. Since by **(1)** one has $|T_k| = |T_0| \cdot (1-k/K)$, this implies that

$$|S_k| = \frac{1}{K-k}|T_k| = \frac{1}{K-k} \cdot (1-k/K)|T_0| = \frac{1}{K}|T_0|,$$

as required.

■

C Proofs omitted from Section 5

C.1 Construction of the set $\mathcal{F}$

Lemma 157 *For any $\epsilon \in (0,1)$, any integers $m \geq 1$ and $w = (\epsilon/2)m$, there exists a collection $\mathcal{F}_{m,w,\epsilon} \subset \{0,1\}^m$ of vectors of Hamming weight w with $\log|\mathcal{F}_{m,w,\epsilon}| = \Omega(\epsilon^2 m)$ such that for all $\mathbf{u} \neq \mathbf{u}' \in \mathcal{F}_{w,\epsilon}$, $(\mathbf{u}, \mathbf{u}') < \epsilon w$.*

Proof: The proof is via the probabilistic method. Partition $[m]$ into w subsets $I_1, \ldots, I_w$, with $|I_s| = m/w$ for $s = 1, \ldots, w$. We pick $\mathbf{u}_1, \ldots, \mathbf{u}_N$ independently as follows. For every $j = 1, \ldots, N$, the vector $\mathbf{u}_j$ includes exactly one random element of I_s for each $s = 1, \ldots, w$. This ensures that the Hamming weight of each $\mathbf{u}_j$ is exactly w.

We now show that the vectors have small intersection size with high probability. Fix $i \neq j \in [N]$. Imagine $\mathbf{u}_i$ being fixed and picking the w elements of $\mathbf{u}_j$ one by one. Let X_s denote the indicator random variable for the event that the sth element of $\mathbf{u}_j$ (picked from I_s) is also in S_i. Then $(\mathbf{u}_i, \mathbf{u}_j) = \sum_{s=1}^{w} X_k$, and we set $\mu := \mathbf{E}[(\mathbf{u}_i, \mathbf{u}_j)]$. Note that $\mu = (w/m) \cdot w$, since for every $s = 1, \ldots, w$ the vector $\mathbf{u}_i$ has exactly one nonzero coordinate in I_s, and the probability that $\mathbf{u}_j$ chooses the same coordinate is $1/|I_s| = w/m$. We have $\mathbf{Pr}[(\mathbf{u}_i, \mathbf{u}_j) \geq \epsilon w] = \mathbf{Pr}[\sum_{s=1}^{w} X_s \geq 2\mu]$ The random variables X_s are independent and thus the Chernoff bound yields

$$\mathbf{Pr}[(\mathbf{u}_i, \mathbf{u}_j) \geq 2\mu) \leq \left(\frac{e}{4}\right)^{\mu} \leq e^{-\Omega((w/m)w)} \leq e^{-c\epsilon^2 m}$$

for a constant $c > 0$. Setting $N = 2^{(\ln_2 e)c\epsilon^2 m/2}$ so that $\binom{N}{2} < N^2 = 2^{(\ln_2 e)c\epsilon^2 m} = e^{c\epsilon^2 m}$, by a union bound with positive probability $|\mathbf{u}_i \cap \mathbf{u}_j| < \epsilon w$ for all $i \neq j$, simultaneously, as desired. Note for this choice of N, we have $\log|\mathcal{F}_{m,w,\epsilon}| = \log N = \Theta(\epsilon^2 m)$. ■

C.2 Proofs of Lemma 102 and Lemma 113

Claim 158 *For every $x \in [m]^n$, every $\mathbf{j} \in \mathcal{F}$, every pair of integers c, d, $c \leq d$ such that $(W/w) \mid (d-c)$, if λ divides W/w,*

$$|\{c \leq t < d : \mathit{wt}(x + t \cdot \mathbf{j}) \pmod{W} \in [0, 1/\lambda) \cdot W\}| = \frac{1}{\lambda} \cdot (d-c).$$

Proof: First, we write

$$t = u \cdot (W/w) + v,$$

where $u = \lfloor t/(W/w) \rfloor$ and $v = t \pmod{W/w}$, so that

$$\begin{aligned}
\mathrm{wt}(x + t \cdot \mathbf{j}) \pmod{W} &= (\mathrm{wt}(x) + t \cdot w) \pmod{W} \\
&= (\mathrm{wt}(x) + (u \cdot (W/w) + v) \cdot w) \pmod{W} \qquad (265) \\
&= (\mathrm{wt}(x) \pmod{W} + v \cdot w) \pmod{W}.
\end{aligned}$$

Similarly, write

$$c = f \cdot (W/w) + e$$
$$d = g \cdot (W/w) + e,$$

where $f = \lfloor c/(W/w) \rfloor$, $g = \lfloor c/(W/w) \rfloor$ and $e = c \pmod{W/w} = d \pmod{W/w}$ (the last equality is justified by the assumption that $(W/w) \mid (d-c)$). With this notation in place, using (265), we can express the set in question conveniently as

$$\begin{aligned}
&\{c \le t < d : \mathrm{wt}(x + t \cdot \mathbf{j}) \pmod W \in [0, 1/\lambda) \cdot W\} \\
&= \{f \cdot (W/w) + e \le t < g \cdot (W/w) + e : \\
&\qquad (\mathrm{wt}(x) \pmod W + v \cdot w) \pmod W \in [0, 1/\lambda) \cdot W\} \qquad (266) \\
&= \{f \cdot (W/w) \le u \cdot (W/w) + v - e < g \cdot (W/w) : \\
&\qquad (\mathrm{wt}(x) \pmod W + v \cdot w) \pmod W \in [0, 1/\lambda) \cdot W\}
\end{aligned}$$

Note that for every u such that

$$f + 1 \le u < g \qquad (267)$$

one has

$$f \cdot (W/w) \le u \cdot (W/w) + v - e < g \cdot (W/w) \qquad (268)$$

for all $v \in [W/w] = \{0, 1, \ldots, W/w - 1\}$, since $e \in [W/w] = \{0, 1, \ldots, W/w - 1\}$ by definition of e. Now since $\lambda \mid W/w$ by assumption, using (265) we get that for every u that satisfies (267) exactly $\frac{1}{\lambda} \cdot (W/w)$ choices for $v \in [W/w]$ lead to

$$(\mathrm{wt}(x) \pmod W + v \cdot w) \pmod W \in [0, 1/\lambda) \cdot W. \qquad (269)$$

It remains to note that for $u = f$ the condition in (268) is satisfied if and only if $e \le v < W/w$, and for $u = g$ the condition in (268) is satisfied if and only if $0 \le v < e$. Since $\{e, e+1, \ldots, W/w - 1\} \cup \{0, 1, \ldots, e-1\} = [W/w]$, we again get that overall exactly $\frac{1}{\lambda} \cdot (W/w)$ choices of v satisfy (269). This establishes the claim. ■

Lemma 159 (Intersection of a cube with a subspace) *For every* $\mathbf{I}, \mathbf{J} \subset \mathcal{F}$, $|\mathbf{I}|, |\mathbf{J}| \le K^2$, *every* $\mathbf{a} \in \Delta \cdot \mathbb{Z} \cap [0,1)^{\mathbf{J}}$, *if* $R = \textsc{Rect}(\mathbf{J}, \mathbf{a})$, *the following conditions hold.*

(1) *For every* $x \in [m]^n \setminus B$ *one has*

$$(1 - \epsilon^{2/3}) \cdot \Delta^{|\mathbf{I} \cap \mathbf{J}|} \cdot G \le |\mathit{subspace}_{\mathbf{I}}(x) \cap R| \le (1 + \epsilon^{2/3}) \cdot \Delta^{|\mathbf{I} \cap \mathbf{J}|} \cdot G,$$

where $G = (M/w)^{|\mathbf{I}|}$.

(2) *For every positive integer* $\lambda \le K$, *if*

$$R' = \{x \in R : \mathit{wt}(x) \pmod W \in [0, 1/\lambda) \cdot W\},$$

one has for every $x \in [m]^n \setminus B$

$$(1 - \epsilon^{2/3}) \cdot \frac{1}{\lambda} \cdot \Delta^{|\mathbf{I} \cap \mathbf{J}|} \cdot G \le \left|\mathit{subspace}_{\mathbf{I}}(x) \cap R'\right| \le (1 + \epsilon^{2/3}) \cdot \frac{1}{\lambda} \cdot \Delta^{|\mathbf{I} \cap \mathbf{J}|} \cdot G,$$

where $G = (M/w)^{|\mathbf{I}|}$.

Proof: For $t \in \mathbb{Z}^{\mathbf{I}}$ with $||t||_\infty \leq 2M/w$ consider

$$x' = x + \sum_{\mathbf{i} \in \mathbf{I}} t_{\mathbf{i}} \cdot \mathbf{i}, \tag{270}$$

and note that every vertex in $\text{subspace}_{\mathbf{I}}(x)$ can be written in this form by Definition 108. Since x is not a boundary point, i.e. $x \in [m]^n \setminus B$ (see Definition 78), one has $x' \in [m]^n$ for every such t. Thus, it suffices to bound the number of choices of such coefficients t that result in both $\text{block}_{\mathbf{I}}(x') = \text{block}_{\mathbf{I}}(x)$ and $x' \in R$ to prove **(1)** and similarly bound the number of choices of t that result in both $\text{block}_{\mathbf{I}}(x') = \text{block}_{\mathbf{I}}(x)$ and $x' \in R'$ to prove **(2)**. We do this in what follows.

Notation and basic properties of x'. We start by noting some basic properties of x'. First note that for every $\mathbf{k} \in \mathbf{I} \cap \mathbf{J}$

$$\begin{aligned}
\left|\langle x', \mathbf{k}\rangle - (\langle x, \mathbf{k}\rangle + t_{\mathbf{k}} \cdot w)\right| &= \left|\langle x + \sum_{\mathbf{i} \in \mathbf{I}} t_{\mathbf{i}} \cdot \mathbf{i}, \mathbf{k}\rangle - (\langle x, \mathbf{k}\rangle + t_{\mathbf{k}} \cdot w)\right| \\
&= \left|\sum_{\mathbf{i} \in \mathbf{I} \setminus \{\mathbf{k}\}} t_{\mathbf{i}} \cdot \langle \mathbf{i}, \mathbf{k}\rangle\right| \\
&\leq \sum_{\mathbf{i} \in \mathbf{I} \setminus \{\mathbf{k}\}} t_{\mathbf{i}} \cdot |\langle \mathbf{i}, \mathbf{k}\rangle| \\
&\leq \epsilon|\mathbf{I}| \cdot ||t||_\infty \cdot w \\
&\leq (2\epsilon|\mathbf{I}|) \cdot M.
\end{aligned} \tag{271}$$

and for every $\mathbf{k} \in \mathbf{J} \setminus \mathbf{I}$

$$\begin{aligned}
\left|\langle x', \mathbf{k}\rangle - \langle x, \mathbf{k}\rangle\right| &= \left|\langle x + \sum_{\mathbf{i} \in \mathbf{I}} t_{\mathbf{i}} \cdot \mathbf{i}, \mathbf{k}\rangle - \langle x, \mathbf{k}\rangle\right| \\
&= \left|\sum_{\mathbf{i} \in \mathbf{I}} t_{\mathbf{i}} \cdot \langle \mathbf{i}, \mathbf{k}\rangle\right| \\
&\leq \sum_{\mathbf{i} \in \mathbf{I}} t_{\mathbf{i}} \cdot |\langle \mathbf{i}, \mathbf{k}\rangle| \\
&\leq \epsilon|\mathbf{I}| \cdot ||t||_\infty \cdot w \\
&\leq (2\epsilon|\mathbf{I}|)M.
\end{aligned} \tag{272}$$

For every $\mathbf{k} \in \mathbf{I}$ define

$$q_{\mathbf{k}} = \left\lfloor \frac{1}{w} \left(\langle x, \mathbf{k}\rangle \pmod{M}\right)\right\rfloor \tag{273}$$

for convenience, and note that

$$0 \leq \langle x, \mathbf{k}\rangle \pmod{M} - w\left\lfloor \frac{1}{w}\left(\langle x, \mathbf{k}\rangle \pmod{M}\right)\right\rfloor < w. \tag{274}$$

Fix $\eta \in (0, 1/10)$, and assume that η satisfies

$$\eta > 2w/M \ \text{ and } \ \eta \geq 5\epsilon|\mathbf{I}|. \tag{275}$$

Lower bound. We now prove that any t such that

$$-q_{\mathbf{k}}+\frac{M}{w}\cdot(\mathbf{a}_{\mathbf{k}}+\eta)\leq t_{\mathbf{k}}<-q_{\mathbf{k}}+\frac{M}{w}\cdot(\mathbf{a}_{\mathbf{k}}+\Delta-\eta) \tag{276}$$

for all $\mathbf{k}\in\mathbf{I}\cap\mathbf{J}$ and

$$-q_{\mathbf{k}}+\frac{M}{w}\cdot\eta\leq t_{\mathbf{k}}<-q_{\mathbf{k}}+\frac{M}{w}\cdot(1-\eta) \tag{277}$$

for $\mathbf{k}\in\mathbf{I}\setminus\mathbf{J}$ satisfies

(a) $x'=x+\sum_{\mathbf{i}\in\mathbf{I}}t_{\mathbf{i}}\cdot\mathbf{i}\in\text{subspace}_{\mathbf{I}}(x)\cap R$ as long as η is not too small (recall that $q_{\mathbf{k}}$ is defined in (273));

(b) $\text{block}_{\mathbf{I}}(x')=\text{block}_{\mathbf{I}}(x)$.

The two bounds above show that any t that satisfies both (276) and (277) leads to $x'\in\text{subspace}_{\mathbf{I}}(x)\cap R$. Counting the number of settings of t that satisfy these constraints, we get

$$\begin{aligned}|\text{subspace}_{\mathbf{I}}(x)\cap R|&\geq(M/w)^{|\mathbf{I}|}(1-4\eta)^{|\mathbf{I}\setminus\mathbf{J}|}(\Delta-4\eta)^{|\mathbf{I}\cap\mathbf{J}|}\\&\geq(M/w)^{|\mathbf{I}|}\Delta^{|\mathbf{I}\cap\mathbf{J}|}(1-4\eta/\Delta)^{|\mathbf{I}|},\end{aligned} \tag{278}$$

where we used the fact that since $\eta>2w/M$ by assumption, we have $\lceil\eta M/w\rceil\leq 2\eta M/w$.

We start with **(a)**. We verify that the dot product of every x' as above with $\mathbf{k}\in\mathbf{I}\cap\mathbf{J}$ satisfies

$$\langle x',\mathbf{k}\rangle\pmod M\in[\mathbf{a}_k,\mathbf{a}_k+\Delta)\cdot M. \tag{279}$$

First, for $k\in\mathbf{I}\cap\mathbf{J}$, using (271), it suffices to show that

$$\langle x,\mathbf{k}\rangle\pmod M+t_{\mathbf{k}}\cdot w\in[\mathbf{a}_k,\mathbf{a}_k+\Delta)\cdot M,$$

as well as show that the quantity on the lhs above does not fall too close to the boundary of the interval on the rhs (to ensure that the error terms in (271) can be absorbed).

We have using the upper bound on $t_{\mathbf{k}}$ from (276) as well as (274)

$$\begin{aligned}\langle x,\mathbf{k}\rangle\pmod M+t_{\mathbf{k}}\cdot w&\leq\langle x,\mathbf{k}\rangle\pmod M-w\cdot\mathbf{q}_{\mathbf{k}}+(\mathbf{a}_{\mathbf{k}}+\Delta-\eta)\cdot M&&\text{(by (276))}\\&=(\langle x,\mathbf{k}\rangle\pmod M-w\cdot\mathbf{q}_{\mathbf{k}})+(\mathbf{a}_{\mathbf{k}}+\Delta-\eta)\cdot M\\&\leq w+(\mathbf{a}_{\mathbf{k}}+\Delta-\eta)\cdot M&&\text{(by (274))}\\&=(\mathbf{a}_{\mathbf{k}}+\Delta+\frac{w}{M}-\eta)\cdot M.\end{aligned}$$

We also have using the lower bound on $t_{\mathbf{k}}$ from (276)as well as (274)

$$\begin{aligned}\langle x,\mathbf{k}\rangle\pmod M+t_{\mathbf{k}}\cdot w&\geq\langle x,\mathbf{k}\rangle\pmod M-w\cdot\mathbf{q}_{\mathbf{k}}+(\mathbf{a}_{\mathbf{k}}+\eta)\cdot M&&\text{(by (276))}\\&=(\langle x,\mathbf{k}\rangle\pmod M-w\cdot\mathbf{q}_{\mathbf{k}})+(\mathbf{a}_{\mathbf{k}}+\eta)\cdot M\\&\geq(\mathbf{a}_{\mathbf{k}}+\eta)\cdot M.&&\text{(by (274))}\end{aligned}$$

The two bounds together imply that for all t satisfying (276) one has

$$(\mathbf{a}_{\mathbf{k}}+\eta)\cdot M\leq(\langle x,\mathbf{k}\rangle+t_{\mathbf{k}}\cdot w)\pmod M\leq(\mathbf{a}_{\mathbf{k}}+\Delta+\frac{w}{M}-\eta)\cdot M.$$

We also note that $\mathbf{q}_{\mathbf{k}}\in[0,M/w)$, implying that one has $|t_{\mathbf{k}}|\leq 2M/w$ for all $\mathbf{k}\in\mathbf{I}$ for every t satisfying (276) and (277) as long as $\eta<1$. Combining this with (271), we get that for every t satisfying (276) the point

$x' = x + \sum_{\mathbf{i}\in\mathbf{I}} t_{\mathbf{i}} \cdot \mathbf{i}$ satisfies (279) for $t \in \mathbf{I} \cap \mathbf{J}$ by (275). Similarly, we get using (272) that for every t satisfying (276) and (277) the point $x' = x + \sum_{\mathbf{i}\in\mathbf{I}} t_{\mathbf{i}} \cdot \mathbf{i}$ satisfies (279) for $t \in \mathbf{J} \setminus \mathbf{I}$ as long as (275) holds.

We now establish **(b)**. Note that for every t satisfying (276) and (277) and every $\mathbf{k} \in \mathbf{I}$ one has, using (271) and (272) that

$$-q_{\mathbf{k}} \cdot w + \eta M - (2\epsilon|\mathbf{I}|)M \leq \langle x', \mathbf{k}\rangle - \langle x, k\rangle \leq -q_{\mathbf{k}} \cdot w + (1-\eta)M + (2\epsilon\mathbf{I})M.$$

Indeed, this follows directly from (277) for $\mathbf{k} \in \mathbf{I} \setminus \mathbf{J}$, and follows from (276) for $\mathbf{k} \in \mathbf{I} \cap \mathbf{J}$ by recalling that $\mathbf{a_k} \in \Delta \cdot \mathbb{Z} \cap [0, 1) \subseteq [0, 1 - \Delta]$. Rearranging the terms and using (275) , we get

$$\langle x, \mathbf{k}\rangle - q_{\mathbf{k}} \cdot w < \langle x', \mathbf{k}\rangle < \langle x, \mathbf{k}\rangle - q_{\mathbf{k}} \cdot w + M.$$

By definition of $q_{\mathbf{k}}$ (see (273)) we have $0 \leq q_{\mathbf{k}} \cdot w < (\langle x, \mathbf{k}\rangle \pmod M)$. Thus, the above implies

$$\left\lfloor \frac{1}{M}\langle x', \mathbf{k}\rangle \right\rfloor = \left\lfloor \frac{1}{M}\langle x, \mathbf{k}\rangle \right\rfloor$$

for all $\mathbf{k} \in \mathbf{I}$, and therefore $\text{block}_{\mathbf{I}}(x') = \text{block}_{\mathbf{I}}(x)$. Since $||t||_\infty \leq 2M/w$, we get that $x' \in \text{subspace}_{\mathbf{I}}(x)$.

Upper bound. We now upper bound the number of choices for t such that x' as in (270) belongs to $\text{subspace}_{\mathbf{I}}(x) \cap R$. We first note that every such t that leads to $x' \in \text{subspace}_{\mathbf{I}}(x) \cap R$ must satisfy

(a) for all $\mathbf{k} \in \mathbf{I}$

$$-\mathbf{q_k} - \eta\frac{M}{w} \leq t_{\mathbf{k}} \leq -q_{\mathbf{k}} + (1+\eta)\frac{M}{w} \tag{280}$$

(b) for all $k \in \mathbf{I} \cap \mathbf{J}$

$$t_{\mathbf{k}} \notin \left[-q_{\mathbf{k}} + \eta\frac{M}{w}, -q_{\mathbf{k}} + \frac{M}{w} \cdot (\mathbf{a_k} - \eta)\right) \cup \left(-q_{\mathbf{k}} + \frac{M}{w} \cdot (\mathbf{a_k} + \Delta + \eta), -q_{\mathbf{k}} + (1-\eta)\frac{M}{w}\right] \tag{281}$$

We start by proving **(a)**. Suppose that (280) is not true for some $\mathbf{k} \in \mathbf{I}$. We assume that $t_{\mathbf{k}} \leq -\mathbf{q_k} - \eta\frac{M}{w}$ (the other case is analogous). Then one has

$$\begin{aligned}\langle x', \mathbf{k}\rangle &\leq \langle x, \mathbf{k}\rangle - \mathbf{q_k} - \eta M + \sum_{\mathbf{i}\in\mathbf{I}\setminus\{\mathbf{k}\}} |t_{\mathbf{i}}| \cdot \langle \mathbf{i}, \mathbf{k}\rangle \\ &\leq (w/M - \eta + (2\epsilon|\mathbf{I}|))M,\end{aligned}$$

where we upper bounded the difference of the first two terms on the rhs by w as per (274), and used the fact that $||t||_\infty \leq 2M/w$ to upper bound the last term. Since $\eta > 2w/M$ and $\eta \geq 5\epsilon|\mathbf{I}|$, we get $\lfloor\langle x', \mathbf{k}\rangle/M\rfloor < \lfloor\langle x, \mathbf{k}\rangle/M\rfloor$, and hence $\text{block}_{\mathbf{I}}(x') \neq \text{block}_{\mathbf{I}}(x)$.

We now prove **(b)**. We consider two cases.

Case 1: Suppose that $-\mathbf{q_k} + \eta\frac{M}{w} \leq t_{\mathbf{k}} < -\mathbf{q_k} + \frac{M}{w} \cdot (\mathbf{a_k} - \eta)$. Since

$$\langle x, \mathbf{k}\rangle \pmod M - w \cdot \mathbf{q_k} + (\mathbf{a_k} - \eta) \cdot M \leq (\mathbf{a_k} + \frac{w}{M} - \eta) \cdot M \qquad \text{(by (274))}$$

and

$$\langle x, \mathbf{k}\rangle \pmod M - w \cdot \mathbf{q_k} + \eta \cdot M \geq \eta \cdot M,$$

we get, using (271) and (275) together with the assumption that $\eta < 1/10$ and the fact that $\Delta \leq 1/2$ by (p3), that $\langle x', \mathbf{k}\rangle \pmod M \notin [\mathbf{a_k}, \mathbf{a_k} + \Delta) \cdot M$.

Case 2: Suppose that $-q_{\mathbf{k}}+\frac{M}{w}\cdot(\mathbf{a_k}+\Delta+\eta)<t_{\mathbf{k}}\leq -q_{\mathbf{k}}+(1-\eta)\frac{M}{w}$. Then we have

$$\langle x,\mathbf{k}\rangle \pmod M - w\cdot \mathbf{q_k}+(\mathbf{a_k}+\Delta+\eta)\cdot M\geq (\mathbf{a_k}+\Delta+\eta)M \qquad \text{(by (274))}$$

and

$$\langle x,\mathbf{k}\rangle \pmod M - w\cdot \mathbf{q_k}+(1+\eta)\cdot M\leq (1+w/M-\eta)\cdot M,$$

and hence using (271) and (275) together with the assumption that $\eta<1/10$ we get $\langle x',\mathbf{k}\rangle\notin[\mathbf{a_k},\mathbf{a_k}+\Delta)\cdot M$.

Counting the number of settings for t that satisfy both **(a)** and **(b)**, we get

$$|\text{subspace}_{\mathbf{I}}(x)\cap R|\leq (M/w)^{|\mathbf{I}|}(1+4\eta)^{|\mathbf{I}\setminus\mathbf{J}|}(\Delta+4\eta)^{|\mathbf{I}\cap\mathbf{J}|}\leq (M/w)^{|\mathbf{I}|}\Delta^{|\mathbf{I}\cap\mathbf{J}|}(1+4\eta/\Delta)^{|\mathbf{I}|}. \tag{282}$$

Gathering bounds and setting the parameter η. We now let

$$\eta=\epsilon\cdot K^3, \tag{283}$$

so that

$$\begin{aligned}(1+4\eta/\Delta)^{|\mathbf{I}|}&\leq (1+4\eta/\Delta)^{K^2} && \text{(since } |\mathbf{I}|\leq K^2\text{)}\\ &\leq (1+4\epsilon K^3/\Delta)^{K^2} && \text{(by setting of } \eta\text{)}\\ &\leq (1+4\epsilon K^3\cdot K^K)^{K^2} && \text{(since } \Delta\geq K^{-K} \text{ by (p3))}\\ &\leq 1+8\epsilon K^{K+5} && \text{(since } 4\epsilon K^5\cdot K^K<1 \text{ by (p6), (p5) and (p3))}\\ &\leq 1+\epsilon^{2/3}(8\epsilon^{1/3}K^{K+5})\\ &\leq 1+\epsilon^{2/3}/3 && \text{(by (p6)).}\end{aligned} \tag{284}$$

The last transition uses the fact that

$$\begin{aligned}8\epsilon^{1/3}K^{K+5}&\leq 8\delta^{2/3}K^{K+5} && \text{(by (p5))}\\ &\leq 8K^{-50K^2}K^{K+5} && \text{(by (p3) and (p5))}\\ &\leq 1/3,\end{aligned}$$

since K is larger than an absolute constant. Similarly we have $(1-4\eta/\Delta)^{|\mathbf{I}|}\geq 1-\epsilon^{2/3}/3$. We also verify that our setting of η in (283) satisfies conditions in (275). First, we have $\eta=\epsilon K^3\geq 5\epsilon|\mathbf{I}|$ since $|\mathbf{I}|\leq K^2$ by assumption and K is larger than an absolute constant. We also have $\eta>2w/M$ by (p7). This completes the proof of **(1)**.

We now prove **(2)**, the second bound of the lemma. We consider two cases, depending on whether $\mathbf{I}\cap\mathbf{J}\neq\emptyset$.

Case 1: $\mathbf{I}\cap\mathbf{J}\neq\emptyset$. Consider any choice of t that satisfies (276) and (277), which by our analysis above leads to $x'\in\text{subspace}_{\mathbf{I}}(x)$. Now select $\mathbf{k}_*\in\mathbf{I}\cap\mathbf{J}$ arbitrarily, and let $t_{\mathbf{k}_*}$ vary in the range

$$-q_{\mathbf{k}}+\frac{M}{w}\cdot\mathbf{a_k}\leq t_{\mathbf{k}_*}<-q_{\mathbf{k}}+\frac{M}{w}\cdot(\mathbf{a_k}+\Delta). \tag{285}$$

We have per (270) together with the fact that $|\mathbf{u}|=w$ for all $\mathbf{u}\in\mathcal{F}$ that

$$\text{wt}(x')=\text{wt}(x)+\sum_{\mathbf{k}\in\mathbf{I}}w\cdot t_{\mathbf{k}}.$$

Letting $z = x' + \sum_{\mathbf{k} \in \mathbf{I} \setminus \{\mathbf{k}_*\}} \mathbf{k} \cdot t_{\mathbf{k}}$, we get by Claim 158

$$\begin{aligned}|\{-q_{\mathbf{k}_*} + \mathbf{a}_{\mathbf{k}_*} \cdot \frac{M}{w} \leq t_{\mathbf{k}_*} < -q_{\mathbf{k}_*} + (\mathbf{a}_{\mathbf{k}_*} + \Delta) \cdot \frac{M}{w} :& \\ \text{wt}(z + t \cdot \mathbf{k}_*) \pmod{W} \in [0, 1/\lambda) \cdot W\}| &= \frac{1}{\lambda} \cdot \Delta \cdot \frac{M}{W}.\end{aligned}$$

Note that the preconditions of Claim 158 are satisfied since $\frac{W}{w} \mid \Delta \cdot \frac{M}{w}$ by (p2) and $\lambda \mid \frac{W}{w}$ since $\lambda \leq K$ is a positive integer by assumption of the lemma as well as (p1).

Since our analysis above shows that every t that satisfies (276) and 277 leads to $x' \in R$, we get

$$\left|\text{subspace}_{\mathbf{I}}(x) \cap R'\right| \geq \left(\frac{1}{\lambda}\Delta - 4\eta\right) \cdot (M/w)^{|\mathbf{I}|}(1 - 4\eta)^{|\mathbf{I} \setminus \mathbf{J}|}(\Delta + 4\eta)^{|\mathbf{I} \cap \mathbf{J}|-1}, \tag{286}$$

where the $\frac{1}{\lambda} \cdot \Delta - 4\eta$ term above is due to the fact that by (286) one has

$$\begin{aligned}&|\{-q_{\mathbf{k}_*} + (\mathbf{a}_{\mathbf{k}_*} + \eta) \cdot \frac{M}{w} \leq t_{\mathbf{k}_*} < -q_{\mathbf{k}_*} + (\mathbf{a}_{\mathbf{k}_*} + \Delta - \eta) \cdot \frac{M}{w} : \\ &\qquad \text{wt}(z + t \cdot \mathbf{k}_*) \pmod{W} \in [0, 1/\lambda) \cdot W\}| \\ \geq &|\{-q_{\mathbf{k}_*} + \mathbf{a}_{\mathbf{k}_*} \cdot \frac{M}{w} \leq t_{\mathbf{k}_*} < -q_{\mathbf{k}_*} + (\mathbf{a}_{\mathbf{k}_*} + \Delta) \cdot \frac{M}{w} : \\ &\qquad \text{wt}(z + t \cdot \mathbf{k}_*) \pmod{W} \in [0, 1/\lambda) \cdot W\}| - 4\eta M/w \\ \geq &\left(\frac{1}{\lambda} \cdot \Delta - 4\eta\right) \cdot \frac{M}{w},\end{aligned}$$

as the assumption $\eta > 2w/M$ implies that $\lceil \eta M/w \rceil \leq 2\eta M/w$. Similarly, we get

$$\left|\text{subspace}_{\mathbf{I}}(x) \cap R'\right| \leq \left(\frac{1}{\lambda} \cdot \Delta + 4\eta\right) \cdot (M/w)^{|\mathbf{I}|}(1 + 4\eta)^{|\mathbf{I} \setminus \mathbf{J}|}(\Delta + 4\eta)^{|\mathbf{I} \cap \mathbf{J}|-1}.$$

Similarly to (284) we get

$$\frac{1}{\lambda} \cdot \Delta + 4\eta \leq (1 + \epsilon^{2/3}/4)\frac{1}{\lambda} \quad \text{and} \quad \frac{1}{\lambda} \cdot \Delta - 4\eta \geq (1 - \epsilon^{2/3}/4)\frac{1}{\lambda}$$

since λ is a positive integer bounded by K by assumption. Thus,

$$(1 - \epsilon^{2/3})\frac{1}{\lambda} \cdot (M/w)^{|\mathbf{I}|}\Delta^{|\mathbf{I} \cap \mathbf{J}|} \leq \left|\text{subspace}_{\mathbf{I}}(x) \cap R'\right| \leq (1 + \epsilon^{2/3})\frac{1}{\lambda} \cdot (M/w)^{|\mathbf{I}|}\Delta^{|\mathbf{I} \cap \mathbf{J}|}$$

as required.

Case 2: $\mathbf{I} \cap \mathbf{J} = \emptyset$. The proof is similar to **Case 1** above. Consider any choice of t that satisfies (276) and (277), which by our analysis above leads to $x' \in \text{subspace}_{\mathbf{I}}(x)$. Now select $\mathbf{k}_* \in \mathbf{I}$ arbitrarily, and let $t_{\mathbf{k}_*}$ vary in the range

$$-q_{\mathbf{k}} \leq t_{\mathbf{k}_*} < -q_{\mathbf{k}} + \frac{M}{w}. \tag{287}$$

We have per (270) that $\text{wt}(x') = \text{wt}(x) + \sum_{\mathbf{k} \in \mathbf{I}} w \cdot t_{\mathbf{k}}$. Letting $z = x' + \sum_{\mathbf{k} \in \mathbf{I} \setminus \{\mathbf{k}_*\}} \mathbf{k} \cdot t_{\mathbf{k}}$, we get by Claim 158

$$\begin{aligned}|\{-q_{\mathbf{k}_*} \leq t_{\mathbf{k}_*} < -q_{\mathbf{k}_*} + \frac{M}{w} :& \\ \text{wt}(z + t \cdot \mathbf{k}_*) \pmod{W} \in [0, 1/\lambda) \cdot W\}| &= \frac{1}{\lambda} \cdot \frac{M}{W}.\end{aligned}$$

Note that the preconditions of Claim 158 are satisfied since $\frac{W}{w} \mid \frac{M}{w}$ by (p2) and $\lambda \mid \frac{W}{w}$ since $\lambda \leq K$ is a positive integer by assumption of the lemma as well as (p1).

Similarly to **Case 1**, we now get

$$\left|\text{subspace}_{\mathbf{I}}(x) \cap R'\right| \leq \left(\frac{1}{\lambda} + 4\eta\right) \cdot (M/w)^{|\mathbf{I}|}(1 + 4\eta/\Delta)^{|\mathbf{I}|}$$
$$\left|\text{subspace}_{\mathbf{I}}(x) \cap R'\right| \geq \left(\frac{1}{\lambda} - 4\eta\right) \cdot (M/w)^{|\mathbf{I}|}(1 - 4\eta/\Delta)^{|\mathbf{I}|},$$

and

$$(1 - \epsilon^{2/3})\frac{1}{\lambda} \cdot (M/w)^{|\mathbf{I}|} \leq \left|\text{subspace}_{\mathbf{I}}(x) \cap R'\right| \leq (1 + \epsilon^{2/3})\frac{1}{\lambda} \cdot (M/w)^{|\mathbf{I}|}$$

as required. ■

We now give a proof of Lemma 113, restated here for convenience of the reader:

Lemma 113 *(Restated)*

For every $\mathbf{I}, \mathbf{J} \subset \mathcal{F}, |\mathbf{I}|, |\mathbf{J}| \leq K^2$, every $\mathbf{a}, \mathbf{b} \in \Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{J}}, \mathbf{a} < \mathbf{b}$, if $R = \textsc{Rect}(\mathbf{J}, \mathbf{a}, \mathbf{b})$ is a rectangle such that $\gamma := \prod_{\mathbf{i} \in \mathbf{I} \cap \mathbf{J}}(\mathbf{b_i} - \mathbf{a_i})$, the following conditions hold.

(1) *For every $x \in [m]^n \setminus B$ one has*

$$(1 - \epsilon^{2/3}) \cdot \gamma \cdot G \leq |\mathit{subspace}_{\mathbf{I}}(x) \cap R| \leq (1 + \epsilon^{2/3}) \cdot \gamma \cdot G,$$

where $G = (M/w)^{|\mathbf{I}|}$.

(2) *For every positive integer $\lambda \leq K$ such that $\lambda \mid W/w$, if*

$$R' = \{x \in R : \mathit{wt}(x) \pmod W \in [0, 1/\lambda) \cdot W\},$$

one has for every $x \in [m]^n \setminus B$

$$(1 - \epsilon^{2/3}) \cdot \frac{1}{\lambda} \cdot \gamma \cdot G \leq \left|\mathit{subspace}_{\mathbf{I}}(x) \cap R'\right| \leq (1 + \epsilon^{2/3}) \cdot \frac{1}{\lambda} \cdot \gamma \cdot G,$$

where $G = (M/w)^{|\mathbf{I}|}$.

Proof: We have $R = \textsc{Rect}(\mathbf{I}, \mathbf{a}, \mathbf{b}) = \bigcup_{\mathbf{q} \in Q} \textsc{Rect}(\mathbf{I}, \mathbf{q})$ for a subset Q of $\Delta \cdot \mathbb{Z} \cap [0,1]^{\mathbf{I}}$ by Claim 101, and hence by Lemma 159 one has

$$\begin{aligned}|\textsc{Rect}(\mathbf{I}, \mathbf{a}, \mathbf{b}) \cap \text{subspace}_{\mathbf{I}}(x)| &= \left|\bigcup_{\mathbf{q} \in Q} \textsc{Rect}(\mathbf{I}, \mathbf{q}) \cap \text{subspace}_{\mathbf{I}}(x)\right| \\ &= \sum_{\mathbf{q} \in Q} |\textsc{Rect}(\mathbf{I}, \mathbf{q}) \cap \text{subspace}_{\mathbf{I}}(x)|.\end{aligned}$$

The result now follows by Lemma 159. ■

We now give a proof of Lemma 102, restated here for convenience of the reader:

Lemma 102 *(Bounds on sizes of rectangles) For every $\mathbf{I} \subseteq \mathcal{F}$ such that $|\mathbf{I}| \leq K^2$, for every $\mathbf{c}, \mathbf{d} \in (\Delta \cdot \mathbb{Z} \cap [0,1])^{\mathbf{I}}, \mathbf{c} < \mathbf{d}$, $\gamma := \prod_{\mathbf{i} \in \mathbf{I}}(\mathbf{d_i} - \mathbf{c_i})$, $R = \textsc{Rect}(\mathbf{I}, \mathbf{c}, \mathbf{d})$, for every positive integer $\lambda \leq K$ such that $\lambda \mid W/w$, if*

$$R' = \{x \in R : \mathit{wt}(x) \pmod W \in [0, 1/\lambda) \cdot W\},$$

the following conditions hold:

(1) *the cardinality of R is bounded as*

$$(1-\sqrt{\epsilon})\gamma \leq |R|/m^n \leq (1+\sqrt{\epsilon})\cdot\gamma$$

(2) *the cardinality of R' is bounded as*

$$\frac{1}{\lambda}\cdot(1-\sqrt{\epsilon})\gamma \leq \left|R'\right|/m^n \leq \frac{1}{\lambda}\cdot(1+\sqrt{\epsilon})\gamma.$$

Proof: Let $C \subset [m]^n$ denote a minimal $\mathbf{I}$-subspace cover as per Definition 112, i.e. a collection of x such that $\bigcup_{x\in C}\text{subspace}_{\mathbf{I}}(x) = [m]^n$ and $\text{subspace}_{\mathbf{I}}(x)\cap\text{subspace}_{\mathbf{I}}(x') = \emptyset$ for $x, x' \in C$, $x \neq x'$. We have

$$\begin{aligned}|\textsc{Rect}(\mathbf{I},\mathbf{c},\mathbf{d})| &= \sum_{x\in C}|\textsc{Rect}(\mathbf{I},\mathbf{c},\mathbf{d})\cap\text{subspace}_{\mathbf{I}}(x)|\\ &= \sum_{x\in C\setminus B}|\textsc{Rect}(\mathbf{I},\mathbf{c},\mathbf{d})\cap\text{subspace}_{\mathbf{I}}(x)| + \sum_{x\in B}|\textsc{Rect}(\mathbf{I},\mathbf{c},\mathbf{d})\cap\text{subspace}_{\mathbf{I}}(x)|\end{aligned} \tag{288}$$

First note that the second term above is upper bounded by

$$|B|\cdot(5M/w)^{|\mathbf{I}|} \leq \frac{1}{n^{10}}\cdot m^n\cdot(5M/w)^{|\mathbf{I}|} \leq \epsilon^{2/3}\cdot\gamma\cdot m^n, \tag{289}$$

where we used that fact that for every $x\in[m]^n$ and every $\mathbf{I}\subseteq\mathcal{F}$ one has $|\text{subspace}_{\mathbf{I}}(x)| \leq (5M/w)^{|\mathbf{I}|}$ due to the fact that the integer vector t of coefficients in the definition of $\text{subspace}_{\mathbf{I}}(x)$ is constrained to be bounded by $2M/w$ coordinatewise, as well as the fact that n is sufficiently large as a function of $M, W, K, L, \Delta, \delta$ and ϵ.

For $x \in C\setminus B$ we have by Lemma 113

$$G\cdot(1-\epsilon^{2/3}) \leq |\text{subspace}_{\mathbf{I}}(x)\cap\textsc{Rect}(\mathbf{I},\mathbf{c},\mathbf{d})| \leq G\cdot(1+\epsilon^{2/3}),$$

where $G = (M/w)^{|\mathbf{I}|}\prod_{\mathbf{i}\in\mathbf{I}}(\mathbf{d}_\mathbf{i}-\mathbf{c}_\mathbf{i})$. Summing over all $x\in C$ as per (288) and using the upper bound on the second term of (288) provided by (289) gives the result. ■

C.3 Proof of Lemma 152

Proof of Lemma 152: We start by noting that by (239) and (240)

$$P\cup Q = S^0 \cup \left(\bigcup_{\ell\geq 0} T^\ell\right)\cup\Upsilon_{even}\cup\Upsilon_{odd}. \tag{290}$$

For every $\ell\in[L]$ let Z^ℓ be as in Lemma 136, so that

$$T_*^\ell = Z^\ell \cup \left(\nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j=1}^{L-1-\ell}\nu_{\ell+j,j}(T^{\ell+j}\setminus T_*^{\ell+j})\right), \tag{291}$$

where

$$Z^\ell = T_*^\ell \setminus \left(\nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j=1}^{L-1-\ell}\nu_{\ell+j,j}(T^{\ell+j}\setminus T_*^{\ell+j})\right).$$

and

$$|Z^\ell| \le K^L \delta^{1/4} \cdot |P| \tag{292}$$

by Lemma 136. Adding the $j = 0$ term to the rhs of (291) and $T^\ell \setminus T_*^\ell$ to the lhs, we get, recalling that $\nu_{\ell,0}$ is the identity map,

$$T^\ell = Z^\ell \cup \left(\nu_{L-1,L-1-\ell}(T_*^{L-1}) \cup \bigcup_{j=0}^{L-1-\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}) \right). \tag{293}$$

Putting (290) and (293) together and letting $D = \bigcup_{\ell=0}^{L-1} \nu_{L-1,L-1-\ell}(T_*^{L-1})$ to simplify notation, we get

$$\begin{aligned} P \cup Q &= S^0 \cup \left(\bigcup_{\ell \in [L]} T^\ell \right) \cup \Upsilon_{even} \cup \Upsilon_{odd} \\ &= S^0 \cup D \cup \left(\bigcup_{\ell \in [L]} \bigcup_{j=0}^{\ell} \nu_{\ell+j,j}(T^{\ell+j} \setminus T_*^{\ell+j}) \right) \cup \left(\bigcup_{\ell \in [L]} Z^\ell \right) \cup \Upsilon_{even} \cup \Upsilon_{odd} \\ &= S^0 \cup D \cup \left(\bigcup_{\ell \in [L]} \bigcup_{j=0}^{\ell} \nu_{\ell,j}(T^{\ell} \setminus T_*^{\ell}) \right) \cup \left(\bigcup_{\ell \in [L]} Z^\ell \right) \cup \Upsilon_{even} \cup \Upsilon_{odd} \\ &= S^0 \cup D \cup \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ even}}} \bigcup_{j=0}^{\ell} \nu_{\ell,j}(T^{\ell} \setminus T_*^{\ell}) \right) \cup \left(\bigcup_{\substack{\ell \in [L] \\ \ell \text{ odd}}} \bigcup_{j=0}^{\ell} \nu_{\ell,j}(T^{\ell} \setminus T_*^{\ell}) \right) \cup \left(\bigcup_{\ell \in [L]} Z^\ell \right) \cup \Upsilon_{even} \\ &\quad \cup \Upsilon_{odd}. \end{aligned} \tag{294}$$

We first upper bound $|\Upsilon_{even}|$ and $|\Upsilon_{odd}|$. By Lemma 128 we have that for every $\ell \in [L], \ell > 0$, $|T_*^{\ell-1} \setminus \tau^\ell(S^\ell)| \le \delta^{1/4}|T_0^\ell| = \delta^{1/4} N$. At the same time, τ^ℓ is injective by Claim 126 and

$$|S^\ell| = \sum_{k \in [K/2]} |S_k^\ell| = (1 \pm \epsilon^{1/4})N/2$$

Lemma 85, **(2)**, and $|T_*^{\ell-1}| = (1 \pm \epsilon^{1/2})N/2$ by Lemma 85, **(1)**, together with the fact that $T_*^\ell = T_{K/2}^\ell$ by Definition 83. Putting these bounds together, we get

$$\Big| \{ s \in S^\ell : \tau^\ell(s) \text{ is not defined} \} \Big| = O(\epsilon^{1/4} + \delta^{1/4})N.$$

Thus,

$$|\Upsilon_{even} \cup \Upsilon_{odd}| = O(L \cdot (\epsilon^{1/4} + \delta^{1/4}))N = O(N), \tag{295}$$

since

$$\begin{aligned} L(\epsilon^{1/4} + \delta^{1/4}) &\le L\delta^{1/4} \qquad \text{(by (p6))} \\ &\le L \cdot \Delta^{(100/4)K^2} \qquad \text{(by (p5))} \\ &\le L \cdot K^{-25K^2} \qquad \text{(since } \Delta \le 1/K \text{ by (p4))} \\ &\le K \cdot K^{-25K^2} \qquad \text{(since } L \le K \text{ by (p3))} \\ &\le 1, \end{aligned}$$

where the last transition uses the fact that K is larger than an absolute constant. Using Corollary 139 we have

$$\begin{aligned}
|D| &= \left|\bigcup_{\ell=0}^{L-1} \nu_{L-1,L-1-\ell}(T_*^{L-1})\right| \\
&\le \sum_{\ell=0}^{L-1} \left|\nu_{L-1,L-1-\ell}(T_*^{L-1})\right| \\
&\le \sum_{\ell=0}^{L-1} (\ln 2 + C/K)^{\ell} \cdot |T_*^{L-1}| \quad \text{(by Corollary 139)} \\
&\le |T_*^{L-1}| \cdot \sum_{\ell=0}^{\infty} (\ln 2 + 0.0001)^{\ell} \\
&= O(N)
\end{aligned} \tag{296}$$

so since $|S^0| = N/2$ by definition, it suffices to show that the union of the third and the forth terms on the last line of (294) above equals $A_P \cup A_Q \cup B_P \cup B_Q$.

To that effect we recall that by Definition 130 for every $\ell = 0, \dots, L-1$ and $j = 0, \dots, \ell$ $\nu_{\ell,j+1}(T^\ell \setminus T_*^\ell) = \tau^{\ell-j}(\textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T_*^\ell)))$. Thus the union of the first and the second terms on the last line of (294) can be rewritten as

$$\begin{aligned}
&\bigcup_{\substack{\ell\in[L] \\ \ell \text{ even}}} \bigcup_{j=0}^{\ell} \nu_{\ell,j}(T^\ell \setminus T_*^\ell) \\
&= \bigcup_{\substack{\ell\in[L] \\ \ell \text{ even}}} \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \Big(\nu_{\ell,j}(T^\ell \setminus T_*^\ell) \cup \tau^{\ell-j}(\textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T_*^\ell)))\Big) \\
&= \left(\bigcup_{\substack{\ell\in[L] \\ \ell \text{ even}}} \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \nu_{\ell,j}(T^\ell \setminus T_*^\ell)\right) \cup \left(\bigcup_{\substack{\ell\in[L] \\ \ell \text{ even}}} \bigcup_{\substack{j=0 \\ j \text{ even}}}^{\ell} \tau^{\ell-j}(\textsc{DownSet}^{\ell-j}(\nu_{\ell,j}(T^\ell \setminus T_*^\ell)))\right) \\
&= A_P \cup B_Q \cup \Delta_0,
\end{aligned} \tag{297}$$

where the last transition is by (245) and (247) and we let

$$\Delta_0 = \bigcup_{\substack{\ell\in[L] \\ \ell \text{ even}}} \nu_{\ell,*}(\text{Ext}_\delta(T_*^\ell) \setminus T_*^\ell).$$

By Lemma 106 one has

$$|\text{Ext}_\delta(T_*^\ell) \setminus T_*^\ell| \le \sqrt{\delta}|T_*^\ell|,$$

which implies, since $\nu_{\ell,*}$ maps every vertex to at most $K^{L+1} \le K^K$ vertices, that

$$|\Delta_0| \le 2L \cdot K^K \cdot \sqrt{\delta}|T_*^\ell| \le \delta^{1/4} N, \tag{298}$$

where we used (p5) to conclude that $2L \cdot K^K \cdot \sqrt{\delta} \le \delta^{1/4}$.

Similarly, we get

$$\begin{aligned}
&\bigcup_{\substack{\ell\in[L]\\ \ell \text{ odd}}} \bigcup_{j=0}^{\ell} \nu_{\ell,j}(T^\ell \setminus T^\ell_*) \\
&= \left(\bigcup_{\substack{\ell\in[L]\\ \ell \text{ odd}}} \bigcup_{\substack{j=0\\ j \text{ even}}}^{\ell} \nu_{\ell,j}(T^\ell \setminus T^\ell_*) \right) \cup \left(\bigcup_{\substack{j=0\\ j \text{ odd}}}^{\ell} \nu_{\ell,j}(T^\ell \setminus T^\ell_*) \right) \qquad (299)\\
&= A_Q \cup B_P \cup \Delta_1,
\end{aligned}$$

where we used (245) and (247), and let

$$\Delta_1 = \bigcup_{\substack{\ell\in[L]\\ \ell \text{ odd}}} \nu_{\ell,*}(\mathrm{Ext}_\delta(T^\ell_*) \setminus T^\ell_*).$$

As before, by Lemma 106 one has

$$|\mathrm{Ext}_\delta(T^\ell_*) \setminus T^\ell_*| \le \sqrt{\delta}|T^\ell_*|,$$

which implies, since $\nu_{\ell,*}$ maps every vertex to at most $K^{L+1} \le K^K$ vertices, that

$$|\Delta_1| \le 2L \cdot K^K \cdot \sqrt{\delta}|T^\ell_*| \le \delta^{1/4} N, \qquad (300)$$

where we used (p5) to conclude that $2L \cdot K^K \cdot \sqrt{\delta} \le \delta^{1/4}$. Putting (292), (298) and (300) together with (296) gives the result. ■

D Lower bound of $1 - e^{-1}$ using basic gadgets

We now outline how the $1 - e^{-1} + \Omega(1)$ hardness result of [Kap13] can be obtained using our basic gadgets above. The bound is somewhat weaker in that it does not prove, for every $K \ge 2$, hardness of $(1 - (1 - 1/K)^K + \Omega(1))$-approximation when the input graph is shared by K parties, as the bound of [Kap13] does. Our construction is a slight simplification, and gets $(1-e^{-1}+O(1/K))$-hardness when the number of parties is K, which still converges to $1-e^{-1}$ with K getting large. One also notes that the sets $S_0, S_1, \ldots$ in [Kap13] have geometrically decreasing size, whereas in our case they are all of size about $|T|/K$ – this is due to a reparameterization, which is more convenient for our main result, i.e. the $\frac{1}{1+\ln 2}$ lower bound.

First, we partition $\mathcal{F}$ into disjoint subsets of equal size, letting

$$\mathcal{F} = \mathbf{B}_0 \cup \mathbf{B}_1 \cup \ldots \cup \mathbf{B}_{\widetilde{K}},$$

where $\mathbf{B}_i \cap \mathbf{B}_j = \emptyset$ if $i \neq j$, and $\widetilde{K} := \lfloor (1-e^{-1})K \rfloor$. We let

$$\mathbf{J} \in \mathbf{B}_0 \times \ldots \times \mathbf{B}_{\widetilde{K}-1}, \qquad (301)$$

i.e., $\mathbf{j}_k \in \mathbf{B}_k$ for $k \in [\widetilde{K}]$. We extend the definition of T_k and S_k for $k \in [\widetilde{K}]$ (as opposed to just $k \in [K/2+1]$). Let $T_0 = T$, and for every $k \in [\widetilde{K}]$ let

$$T_{k+1} := \left\{ y \in T_k : \langle y, \mathbf{j}_k \rangle \pmod M \in \left[0, 1 - \frac{1}{K-k}\right) \cdot M \right\}. \qquad (302)$$

Note that, as above, $T_0 \supset T_1 \supset \ldots \supset T_{\widetilde{K}}$ form a nested sequence, and for every $k \in [\widetilde{K}+1]$ one has

$$T_k := \left\{ y \in T_0 : \langle y, \mathbf{j}_s \rangle \pmod M \in \left[0, 1 - \frac{1}{K-s}\right) \cdot M \text{ for all } s \in \{0, 1, \ldots, k-1\} \right\}. \tag{303}$$

The innermost set in this sequence is again a central object of our construction:

Definition 160 (Terminal subcube) *We refer to $T_* := T_{\widetilde{K}}$ as the* terminal subcube.

Define

$$S_k :\asymp \left\{ x \in T_k : \mathrm{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W \right\}, \tag{304}$$

The above stands for S_k being a set of vertices such that $S_k \asymp \widetilde{T}_k$, where

$$\widetilde{T}_k := \left\{ x \in T_k : \mathrm{wt}(x) \in \left[0, \frac{1}{K-k}\right) \cdot W \pmod W \right\}$$

is the set of vertices in T_k whose weight modulo W belongs to a certain range. We stress here that unlike the collection of sets T_k, the sets S_k are disjoint. We also let, for every $k \in [\widetilde{K}]$ and $\mathbf{i} \in \mathbf{B}_k$

$$\begin{aligned} T_k^{\mathbf{j}} &= \left\{ y \in T_k : \langle y, \mathbf{j} \rangle \pmod M \in \left[0, 1 - \frac{1}{K-k}\right) \cdot M \right\} \\ S_k^{\mathbf{j}} &= \left\{ x \in S_k : \langle x, \mathbf{j} \rangle \pmod M \in \left[0, 1 - \frac{1}{K-k}\right) \cdot M \right\}. \end{aligned} \tag{305}$$

First, we note that size bounds in Lemma 85 and Lemma 114 extend for all $k = 0, 1, \ldots, \widetilde{K}$, i.e. apply to the sets defined above (the changes to the proof amount to extending the range of k appropriately). We state them here for convenience of the reader.

Lemma 161 *One has*

(1) *For every $k \in [\widetilde{K}+1]$ one has $|T_k| = (1 \pm \sqrt{\epsilon}) \cdot |T_0|(1 - k/K)$;*

(2) *For every $k \in [\widetilde{K}]$ one has $|S_k| = (1 \pm \sqrt{\epsilon}) \cdot |T_0|/K$;*

(3) *For every $k \in [\widetilde{K}]$, every $\mathbf{i} \in \mathbf{B}_k$ one has $|S_k^{\mathbf{j}}| = (1 \pm \sqrt{\epsilon})(1 - \frac{1}{K-k})|T_0|/K$.*

(4) *For every $k \in [\widetilde{K}]$, every $\mathbf{i} \in \mathbf{B}_k$ one has $|T_k^{\mathbf{j}}| = (1 \pm \sqrt{\epsilon})(1 - \frac{k+1}{K})|T_0|$.*

Lemma 162 *There exists a matching of a $(1 - O(1/K))$ fraction of vertices in S to $T \setminus T_*$.*

We now define the edges of $G = (S, T, E)$ incident on S_k for every $k \in [\widetilde{K}]$. For every $\mathbf{i} \in \mathbf{B}_k$ let

$$C_{\mathbf{j}} \subset [m]^n \tag{306}$$

be a minimal $\mathbf{j}$-line cover as per Definition 94. For every $y \in C$, we include a complete bipartite graph between $\mathrm{line}_{\mathbf{j}}(y) \cap \mathrm{Int}_\delta(S_k^{\mathbf{j}})$ and $\mathrm{line}_{\mathbf{j}}(y) \cap (T_k \setminus T_k^{\mathbf{j}})$: let

$$E_k = \bigcup_{\mathbf{i} \in \mathbf{B}_k} E_{k,\mathbf{j}}, \tag{307}$$

where

$$E_{k,\mathbf{j}} = \bigcup_{y \in C_{\mathbf{j}}} (\mathrm{line}_{\mathbf{j}}(y) \cap \mathrm{Int}_\delta(S_k^{\mathbf{j}})) \times (\mathrm{line}_{\mathbf{j}}(y) \cap (T_k \setminus T_k^{\mathbf{j}})). \tag{308}$$

We let $E = \bigcup_{k \in [\widetilde{K}]} E_k$.

Remark 163 *Note that the edge set E_k is fully defined by the prefix $\mathbf{J}_{<k}$.*

Remark 164 *We note that the edge set defined in* (308) *does not depend on the specific choice of a cover $C_{\mathbf{j}}$ used, i.e. any minimal $\mathbf{j}$-line cover produces the same edge set as per* (308).

Input distribution $\mathcal{D}$. For every $k \in [\widetilde{K}]$ sample $\mathbf{j}_k$, the k-th element of $\mathbf{J}$, independently and uniformly from $\mathbf{B}_k$, so that

$$\mathbf{J} \sim \text{UNIF}\left(\mathbf{B}_0 \times \ldots \times \mathbf{B}_{\widetilde{K}-1}\right).$$

For every $k \in [\widetilde{K}]$, $\mathbf{i} \in \mathbf{B}_k$ and $y \in S_k$ let

$$X_{k,\mathbf{j}}(y) = \text{Bernoulli}(1 - 1/K) \tag{309}$$

denote independent Bernoulli random variables conditioned on $\sum_{y \in S_k} X_{k,\mathbf{j}}(y) = \lceil (1 - \frac{1}{K})|S_k| \rceil$ for all k and $\mathbf{j}$. We use these variables to sample edges of the graph G as follows. Define

$$\widetilde{E}_{k,\mathbf{j}} = \bigcup_{y \in C_{\mathbf{j}}} \left\{ u \in \text{line}_{\mathbf{j}}(y) \cap \text{Int}_\delta(S_k^{\mathbf{j}}) : X_{k,\mathbf{j}}(u) = 1 \right\} \times (\text{line}_{\mathbf{j}}(y) \cap (T_k \setminus T_k^{\mathbf{j}})),$$

where $C_{\mathbf{j}}$ is a minimal $\mathbf{j}$-line cover, and let

$$\widetilde{E}_k = \bigcup_{\mathbf{i} \in \mathbf{B}_k} \widetilde{E}_{k,\mathbf{j}}.$$

Comparing this to the definition of the edge set of G in (307), one observes that we subsample edges of G in a somewhat dependent way – the set $\widetilde{E}_k$ contains, for every direction $\mathbf{i} \in \mathbf{B}_k$ and $y \in C_{\mathbf{j}}$, a complete bipartite graph between vertices u in $\text{line}_{\mathbf{j}}(y) \cap \text{Int}_\delta(S_k^{\mathbf{j}})$ that were sampled by $X_{k,\mathbf{j}}(u)$ and $\text{line}_{\mathbf{j}}(y) \cap (T_k \setminus T_k^{\mathbf{j}})$. The fact that randomness is provided by the vertices $u \in S_k$ as opposed to edges themselves will not be a problem since we are interested in concentration of matching size in G and do not need to reason about arbitrary edge sets – see proof of Lemma 165 below. Let

$$\widetilde{G} = (S \cup S_*, T, \widetilde{E} \cup M_*),$$

where S_* is a disjoint set of nodes of size equal to the size of T_*, and M_* is a perfect matching between T_* and S_*. Note that the subsampling operation used to produce $\widetilde{E}$ from E has the effect of making it hard to store edges of $\widetilde{G}$ (since the algorithm intuitively must remember which edge of G was included and which was not), but at the same time ensures that $\widetilde{G}$ contains a nearly perfect matching.

Lemma 165 (Large matching in $\widetilde{G}$) *With probability at least $1 - 1/N$ there exists a matching of $S \cup S_*$ to T of size at least $(1 - O(1/K))|T|$.*

Proof: For every edge $e \in E$ define the random variable

$$Z_e = \begin{cases} 1 & \text{if } e \in \widetilde{E} \\ 0 & \text{o.w.} \end{cases} \tag{310}$$

Note that for every matching $M \subseteq E$ random variables $\{Z_e\}_{e \in M}$ are negatively dependent, since a matching M touches every vertex at most once.

By Lemma 162 applied to $G = (S, T, E)$ there exists a matching of a $(1 - O(1/K))$ fraction of vertices in S to $T \setminus T_*$ – denote this matching by M. Let

$$\widetilde{M} := M \cap \widetilde{E} = \{e \in M : Z_e = 1\}$$

denote the subset of the edges of M that are included in $\widetilde{E}$. Note that $\widetilde{M}$ is a matching between a subset of S and a subset of $T \setminus T_*$, and we have

$$\mathbf{E}[|\widetilde{M}|] = \sum_{e \in M} \mathbf{Pr}[e \in \widetilde{E}] = \sum_{e \in M} \mathbf{E}[Z_e] = (1 - 1/K)|M|$$

by definition of Z_e in (310) and the fact that every edge in E is included in $\widetilde{E}$ with probability $1 - 1/K$ by (309). Since the random variables $\{Z_e\}_{e \in M}$ are negatively dependent, we have by an application to the Chernoff bound (for negatively dependent random variables)

$$\mathbf{Pr}[|\widetilde{M}| < (1 - 2/K)|M|] \leq \exp(-\Omega(|M|/K)).$$

Since M matches at least a constant fraction of S, we get that $|M| = \Omega(N)$, and therefore

$$\mathbf{Pr}[|\widetilde{M}| < (1 - 2/K)|M|] \leq \exp(-\Omega(N/K)) \leq N^{-2},$$

where N is the number of vertices in our graph instance. ■

Ordering of edges of $\widetilde{G}$ in the stream. The graph $\widetilde{G}$ is presented in the stream over $\widetilde{K} + 1$ *phases* as follows. For every $k \in [\widetilde{K}]$, the edges in $\widetilde{E}_k = \widetilde{E} \cap E_k$ are presented in the stream (the ordering of edges within a phase is arbitrary). Finally a perfect matching between T_* and a disjoint set of nodes S_* is presented in the stream.

Definition 166 *For $k \in [\widetilde{K}]$ we write $\widetilde{G}_{<k} = (T, S_0 \cup \ldots \cup S_{k-1}, \widetilde{E}_{<k})$, where $\widetilde{E}_{<k} = \bigcup_{s \in [k]} \widetilde{E}_s$.*

Definition 167 *For every $k \in [\widetilde{K}]$ let $\Lambda_k = (X_k, \mathbf{J}_k)$. We write $\Lambda_{<k} = (\Lambda_s)_{0 \leq s < k}$.*

Remark 168 *Note that $\widetilde{G}_{\leq k}$ is fully determined by $\Lambda_{<k}$ and X_k, and $\mathbf{j}_k$ is uniformly random in $\mathbf{B}_k$ conditioned on $\Lambda_{<k}$ and X_k.*

D.1 Upper and lower bounds on matchings in $\widetilde{G}$

We first prove

Lemma 169 (Large matching in $\widetilde{G}$) *With probability at least $1 - 1/N$ there exists a matching in $\widetilde{G}$ of size at least $(1 - O(1/K))|T|$.*

Proof: By Lemma 165 with probability at least $1 - N^{-1}$ there exists a matching of a $1 - O(1/K)$ fraction of S to $T \setminus T_*$ in $\widetilde{G}$. Since $\widetilde{G}$ also contains a perfect matching of T_* to a disjoint set of vertices S_*, this gives the result. ■

We now turn to upper bounding the performance of a small space streaming algorithm on our input distribution $\mathcal{D}$. Since the input is sampled from a distribution, we may assume by Yao's minimax principle that the streaming algorithm ALG is deterministic. Let ALG denote a deterministic streaming algorithm that uses s bits of space and at the end of the stream outputs a matching M_{ALG} in $\widetilde{G}$ such that

$$\mathbf{Pr}_{\widetilde{G} \sim \mathcal{D}}\left[|M_{ALG}| \geq \left(1 - e^{-1} + \eta\right)|M_{OPT}|\right] \geq 3/4$$

for some positive $\eta \in (0, 1)$, where M_{OPT} is a maximum matching in $\widetilde{G}$. Note that we are assuming that with probability at least $3/4$ both M_{ALG} is a matching in $\widetilde{G}$ (i.e., in particular, the algorithm does not output edges that are not in $\widetilde{G}$) and the size of M_{ALG} is large as above. At the same time by Lemma 169 one has

$$\mathbf{Pr}_{\widetilde{G} \sim \mathcal{D}}\left[|M_{OPT}| < (1 - O(1/K))|T|\right] \leq N^{-1}.$$

Putting the two bounds above together, we get

$$\mathbf{Pr}_{\widetilde{G}\sim\mathcal{D}}\left[|M_{ALG}| \geq \left(1-e^{-1}+\eta-O(1/K)\right)|T|\right] \geq 1/2. \tag{311}$$

In what follows we show that any algorithm that achieves (311) must essentially remember, for many edges of $G=(S,T,E)$ whether they were included in $\widetilde{G}$.

Upper bounding $|M_{ALG}|$.

Lemma 170 *For every matching $M \subseteq \widetilde{E}$ one has*

$$|M| \leq |M \cap ((T \setminus \mathit{Ext}_\delta(T_*)) \times \textsc{DownSet}(T_*))| + (1-e^{-1})|T| + O(|T|/K).$$

Proof: We exhibit a vertex cover of appropriate size for M. Specifically, we add to the vertex cover one endpoint of every edge in

$$M \cap ((T \setminus \mathrm{Ext}_\delta(T_*)) \times \textsc{DownSet}(T_*)),$$

as well as all vertices in $S \setminus \textsc{DownSet}(T_*)$ and $\mathrm{Ext}_\delta(T_*)$. Note that this is indeed a vertex cover for $\widetilde{G}$. The size of the vertex cover is

$$|M \cap ((T \setminus \mathrm{Ext}_\delta(T_*)) \times \textsc{DownSet}(T_*))| + |S \setminus \textsc{DownSet}(T_*)| + |\mathrm{Ext}_\delta(T_*)|. \tag{312}$$

We now bound the second and third terms above. First, by Lemma 161, **(2)**, we have

$$|S| = \sum_{k\in[\widetilde{K}]} |S_k| \leq (1+\sqrt{\epsilon}) \cdot \widetilde{K} \cdot |T|/K \leq (1+O(1/K))(1-e^{-1})|T|,$$

since $\widetilde{K} = \lfloor (1-e^{-1})K \rfloor \leq (1-e^{-1})K$ and $\sqrt{\epsilon} = O(1/K)$ by (p3), (p5) and (p6). At the same time we have

$$|\textsc{DownSet}(T_*)| = \left| \bigcup_{k\in[\widetilde{K}]} \textsc{DownSet}_k(T_*) \right| = \sum_{k\in[\widetilde{K}]} |\textsc{DownSet}_k(T_*)|.$$

For every $k \in [\widetilde{K}]$ we now apply Lemma 102, **(2)**, to lower bound $|\textsc{DownSet}_k(T_*)|$ (noting, crucially, that $T_* \subseteq T_k$ for all $k \in [\widetilde{K}]$). For that note that $T_* = \textsc{Rect}(\mathbf{I}, \mathbf{c}, \mathbf{d})$, where $\mathbf{I} = \{\mathbf{j}_k\}_{k\in[\widetilde{K}]}$, $\mathbf{c}_{\mathbf{j}_k} = 0$ and $\mathbf{d}_{\mathbf{j}_k} = 1 - \frac{1}{K-k}$ for $k \in [\widetilde{K}]$. We thus apply Lemma 102, **(2)** with $\lambda = K-k$ and

$$\gamma = \prod_{\mathbf{i}\in\mathbf{I}} (\mathbf{d}_\mathbf{i} - \mathbf{c}_\mathbf{i}) = \prod_{k=0}^{\widetilde{K}-1} \left(1 - \frac{1}{K-k}\right) = \prod_{k=0}^{\widetilde{K}-1} \frac{K-k-1}{K-k} = \frac{K-\widetilde{K}}{K} = e^{-1} + O(1/K),$$

since $\widetilde{K} = \lfloor (1-e^{-1})K \rfloor$. We thus get, since $\sqrt{\epsilon} = O(1/K)$ by (p3), (p5) and (p6), that

$$|\textsc{DownSet}_k(T_*)| \geq \frac{1}{\lambda} \cdot (1-\sqrt{\epsilon})\gamma|T| \geq e^{-1}(1-O(1/K))\frac{1}{K-k} \cdot |T|.$$

Summing over $k \in [\widetilde{K}]$, we get

$$|\textsc{DownSet}(T_*)| \geq \sum_{k\in[\widetilde{K}]} |\textsc{DownSet}_k(T_*)| \geq e^{-1}(1-O(1/K)) \left(\sum_{k\in[\widetilde{K}]} \frac{1}{K-k} \right) \cdot |T|.$$

Since

$$\sum_{k\in[\widetilde{K}]}\frac{1}{K-k}\geq\sum_{k=1}^{\lfloor(1-e^{-1})K\rfloor}\frac{1}{K-k}\geq\int_0^{1-e^{-1}-O(1/K)}\frac{1}{1-x}dx=1-O(1/K),$$

we get

$$|\textsc{DownSet}(T_*)|\geq e^{-1}(1-O(1/K))\cdot|T|.$$

Finally, we have by Lemma 106 that $|\text{Ext}_\delta(T_*)\setminus T_*|\leq\sqrt{\delta}|T_*|$, and by Lemma 102, **(1)**, using the calculation for γ above, we have $|T_*|=(1+O(1/K))e^{-1}\cdot|T|$, and therefore $|\text{Ext}_\delta(T_*)|=(1+\sqrt{\delta})(1+O(1/K))e^{-1}\cdot|T|=(1+O(1/K))e^{-1}\cdot|T|$ by (p3) and (p5). Putting these bounds together, we get

$$\begin{aligned}|S\setminus\textsc{DownSet}(T_*)|+|\text{Ext}_\delta(T_*)|&\leq(1+O(1/K))(1-e^{-1})|T|-e^{-1}(1-O(1/K))\cdot|T|\\&\quad+(1+O(1/K))e^{-1}\cdot|T|\\&\leq(1+O(1/K))(1-e^{-1})|T|,\end{aligned}$$

as required. This together with (312) gives the result of the lemma. ■

We now prove

Lemma 171 *For every matching $M\subseteq\widetilde{E}$ one has*

$$M\cap((T\setminus \mathit{Ext}_\delta(T_*))\times\textsc{DownSet}(T_*))\subseteq\bigcup_{k\in[\widetilde{K}]}E_{k,\mathbf{j}_k}.$$

Proof: Fix $k\in[\widetilde{K}]$. Consider $(x,y)\in E_k$, where $x\in T_k, y\in S_k$, such that $(x,y)\in E\cap((T\setminus\text{Ext}_\delta(T_*))\times\textsc{DownSet}(T_*))$. Since $x\in T_k\cap(T\setminus\text{Ext}_\delta(T_*))=T_k\setminus\text{Ext}_\delta(T_*)$ (see Definition 105), there exists $s\in\{k,\ldots,\widetilde{K}-1\}$ such that

$$\langle x,\mathbf{j}_s\rangle\pmod M\in\left[1-\frac{1}{K-s}+\delta,1-\delta\right)\cdot M.\tag{313}$$

Since $(x,y)\in E_k$, one has $y=x+\lambda\cdot\mathbf{u}$ for some $\mathbf{u}\in\mathbf{B}_k$ and integer λ satisfying $|\lambda|\leq 2M/w$. Suppose towards a contradiction that $\mathbf{u}\neq\mathbf{j}_k$. In that case one has

$$\begin{aligned}|\langle y,\mathbf{j}_s\rangle-\langle x,\mathbf{j}_s\rangle|&=|\langle x+\lambda\cdot\mathbf{u},\mathbf{j}_s\rangle-\langle x,\mathbf{j}_s\rangle|\\&=|\lambda|\cdot\langle\mathbf{u},\mathbf{j}_s\rangle\\&\leq|\lambda|\cdot\epsilon\cdot w\\&\leq 2\epsilon\cdot M\\&<\delta,\end{aligned}$$

where we used the fact that $\mathbf{u}\neq\mathbf{j}_s$, since $\mathbf{u}\in\mathbf{B}_k$, $\mathbf{B}_k\cap\mathbf{J}=\{\mathbf{j}_k\}$ and $\mathbf{u}\neq\mathbf{j}_k$ by assumption. The last transition is by (p6). We thus get by combining the above with (313) that

$$\langle y,\mathbf{j}_s\rangle\pmod M\notin\left[0,1-\frac{1}{K-s}\right)\cdot M,$$

and therefore $y\notin\textsc{DownSet}(T_*)$. Thus, we have $\mathbf{u}=\mathbf{j}_k$, and therefore $(x,y)\in E_{k,\mathbf{j}_k}$, as required. ■

D.2 Proof of Theorem 1

We now give
Proof of Theorem 1: Now putting (311) together with Lemma 170, we get

$$\begin{aligned}|M \cap ((T \setminus \mathrm{Ext}_\delta(T_*)) \times \textsc{DownSet}(T_*))| &\geq |M_{ALG}| - \big((1-e^{-1})|T| + O(|T|/K)\big)\\ &\geq \big(1 - e^{-1} + \eta - O(1/K)\big)\,|T| - \big((1-e^{-1})|T| + O(|T|/K)\big)\\ &\geq (\eta - O(1/K))|T|\\ &\geq (\eta/2)|T|,\end{aligned}$$

with probability at least $1/2$, where we assumed that K is larger than an absolute constant that depends on η in the last transition. Thus,

$$\mathbf{Pr}_{\widehat{G}\sim\mathcal{D}}\left[|M_{ALG} \cap ((T \setminus \mathrm{Ext}_\delta(T_*)) \times \textsc{DownSet}(T_*))| \geq (\eta/2)|T| \text{ and } M_{ALG} \subseteq \widetilde{E}\right] \geq 1/2. \tag{314}$$

Note that the second condition above, namely $M_{ALG} \subseteq \widetilde{E}$ enforces the constraint that the algorithm does not output non-edges[10]. We do not add this condition explicitly in calculations below to simplify notation (one can think of $|M_{ALG}|$ as being defined as zero when M_{ALG} contains non-edges). Now recall that by Lemma 171 we have

$$M_{ALG} \cap ((T \setminus \mathrm{Ext}_\delta(T_*)) \times \textsc{DownSet}(T_*)) \subseteq \bigcup_{k \in [\widetilde{K}]} E_{k,\mathbf{j}_k}$$

Thus, there exists $k^* \in [\widetilde{K}]$ such that

$$\mathbf{Pr}\left[|M_{ALG} \cap \widetilde{E}_{k^*,\mathbf{j}_{k^*}}| \geq \frac{\eta}{2K}|T|\right] \geq \frac{1}{2K}. \tag{315}$$

Indeed, otherwise one would have

$$\begin{aligned}&\mathbf{Pr}[|M_{ALG} \cap ((T \setminus \mathrm{Ext}_\delta(T_*)) \times \textsc{DownSet}(T_*))| \geq (\eta/2)|T|]\\ &\leq \mathbf{Pr}\left[\text{exists } k \in [\widetilde{K}] \text{ such that } |M_{ALG} \cap E_{k,\mathbf{j}_k}| \geq \frac{\eta}{2K}|T|\right]\\ &\leq \sum_{k \in [\widetilde{K}]} \mathbf{Pr}\left[|M_{ALG} \cap E_{k,\mathbf{j}_k}| \geq \frac{\eta}{2K}|P|\right]\\ &< \sum_{k \in [\widetilde{K}]} \frac{1}{2K}\\ &\leq K \cdot \frac{1}{2K}\\ &= 1/2,\end{aligned}$$

a contradiction with (314).

To simplify notation, we let $k = k^*$. Recall that **(a)** $\widetilde{G}_{\leq k}$ is fully determined by $\Lambda_{<k}$ and X_k (see Definition 167) and **(b)** conditioned on $\Lambda_{<k}$ and X_k one has $\mathbf{j}_k \sim UNIF(\mathbf{B}_k)$. For simplicity of notation we write $\mathbf{B} = \mathbf{B}_k$, $\mathbf{j} = \mathbf{j}_k$ and $X = X_k$.

[10] The analysis generalizes easily to the setting where the algorithm is allowed to output a small fraction of non-edges, but this is a rather non-standard assumption, and we prefer to operate under the more standard model where M_{ALG} must be a subset of $\widehat{E}$ with a good probability.

Lower bounding the space usage of ALG. In what follows we show that since M_{ALG} often returns many edges from $\widetilde{E}_k$ as per (315), the conditional entropy of X_k given Π and $\Lambda_{\leq k}$ is low, which gives the desired lower bound on s. Let $\Pi \in \{0,1\}^s$ denote the state of ALG after it has been presented with $\widehat{G}_{\leq k}$. Then finish running ALG on $\widehat{G}_{>k}$ starting with state Π. Let M_{ALG} denote the matching output by ALG. We have

$$\begin{aligned} s = |\Pi| &\geq H(\Pi) \\ &\geq H(\Pi|\Lambda_{<k}) \\ &\geq I(\Pi; X|\Lambda_{<k}) \\ &\geq \sum_{\mathbf{i}\in\mathbf{B}} I(\Pi; X_{\mathbf{i}}|\Lambda_{<k}) \\ &= \sum_{\mathbf{i}\in\mathbf{B}} I(\Pi; X_{\mathbf{i}}|\Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}) \\ &\geq \sum_{\mathbf{i}\in\mathbf{B}} I(M_{ALG}; X_{\mathbf{i}}|\Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}) \end{aligned} \tag{316}$$

The second transition uses the fact that conditioning does not increase entropy, the forth transition uses the fact that $X_{\mathbf{i}}$'s are independent conditioned on $\Lambda_{<k}$, the forth transition uses the fact that $\mathbf{J}$ is independent of Π and $X_{\mathbf{i}}$ conditioned on $\Lambda_{<k}$. The final transition is by the data processing inequality:

Lemma 172 (Data Processing Inequality) *For any random variables (X, Y, Z) such that $X \to Y \to Z$ forms a Markov chain, we have $I(X;Z) \leq I(X;Y)$.*

We now lower bound

$$\begin{aligned} \sum_{\mathbf{i}\in\mathbf{B}} I(M_{ALG}; X_{\mathbf{i}}|\Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}) &= \sum_{\mathbf{i}\in\mathbf{B}} H(X_{\mathbf{i}}|\Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}) - H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}) \\ &= \sum_{\mathbf{i}\in\mathbf{B}} H(X_{\mathbf{i}}) - H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}). \end{aligned} \tag{317}$$

We now upper bound $H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\})$ on the rhs of (317). Let

$$\mathcal{E} := \left\{|M_{ALG} \cap E_{k,\mathbf{j}}| \geq \frac{\eta}{2K}|P| \text{ and } M_{ALG} \subseteq \widehat{E}\right\} \tag{318}$$

and let Z denote the indicator of $\mathcal{E}$. Note that $\mathbf{E}[Z] = \mathbf{Pr}[\mathcal{E}] \geq \frac{1}{2K}$ by (315). We have

$$\begin{aligned} H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}) &\leq H(X_{\mathbf{i}}, Z|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}) \\ &\leq H(Z) + H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}, Z) \\ &\leq 1 + H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}, Z), \end{aligned} \tag{319}$$

where we used the fact that $H(Z) \leq 1$, as Z is a binary variable. At the same time, since $\mathbf{E}[Z] = \mathbf{E}_{\mathbf{i}\sim UNIF(\mathbf{B})}[Z|\{\mathbf{j}=\mathbf{i}\}] \geq \frac{1}{2K}$ by (315), and $\mathbf{J} \sim UNIF(\mathbf{B})$, there exists a subset $\mathcal{J} \subseteq \mathbf{B}$ such that $|\mathcal{J}| \geq \frac{1}{4K}|\mathbf{B}|$ and for every $\mathbf{i} \in \mathcal{J}$ one has $\mathbf{E}[Z|\{\mathbf{j}=\mathbf{i}\}] \geq \frac{1}{4K}$. For every $\mathbf{j} \in \mathcal{J}$ one has

$$\begin{aligned} H(X_{\mathbf{i}}|M_{ALG},&\Lambda_{<k}, \{\mathbf{j}=\mathbf{i}\}, Z) \\ &= H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i} \wedge Z=1\}) \cdot \mathbf{Pr}[Z=1|\{\mathbf{j}=\mathbf{i}\}] \\ &+ H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i} \wedge Z=0\}) \cdot \mathbf{Pr}[Z=0|\{\mathbf{j}=\mathbf{i}\}] \end{aligned} \tag{320}$$

We now bound both terms on the rhs in (320). For the second term we have

$$\begin{aligned} H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j}=\mathbf{i} \wedge Z=0\}) &\leq \mathbf{E}_{\Lambda_{<k}}[|S_k|] \cdot H_2(1-1/K) \\ &\leq (1+\sqrt{\epsilon})\frac{1}{K}|T| \cdot H_2(1-1/K) \end{aligned} \tag{321}$$

where the first transition is because $\sum_{y \in S_k} X_{\mathbf{i}}(y) = \lceil (1 - \frac{1}{K})|S_k| \rceil$ by definition of $X_{\mathbf{i}}$ and the second transition is by Lemma 161, **(2)**.

For the first term on the rhs in (320) we note that since $M_{ALG} \subseteq \widetilde{E}$ as we are conditioning on the event $\mathcal{E}$ (by conditioning on $\{Z = 1\}$) for every $y \in S_k$ that is matched by M_{ALG} one has $X_{\mathbf{i}}(y) = 1$. By conditioning on $\{Z = 1 \wedge \mathbf{j} = \mathbf{i}\}$, we get by (318) $|M_{ALG} \cap E_{k,\mathbf{j}}| \geq \frac{\eta |P|}{2K}$, and hence

$$\gamma := \frac{|M_{ALG} \cap E_{k,\mathbf{j}}|}{|S_k|} \geq \frac{\eta |P|}{2K|S_k|} \geq \frac{\eta |T|}{4K|S_k|} \geq \eta/8.$$

For every fixing λ of $\Lambda_{<k}$ one has,

$$H(X_{\mathbf{i}} | M_{ALG}, \{\Lambda_{<k} = \lambda \wedge \mathbf{j} = \mathbf{i} \wedge Z = 1\}) \leq (1-\gamma)|S_k| H_2 \left(1 - \frac{1}{K(1-\gamma)}\right),$$

since conditioned on M_{ALG}, $\lambda, \mathbf{j} = \mathbf{i}$ and the success event $Z = 1$ there are exactly $(1-\gamma)|S_k|$ values of $y \in S_k \setminus M_{ALG}$ such that $X_{\mathbf{i}}(y) = 1$, and hence the conditional entropy of $X_{\mathbf{i}}$ is bounded by

$$\begin{aligned} \log_2 \binom{|S_k \setminus M_{ALG}|}{(1 - \frac{1}{K} - \gamma)|S_k|} &= \log_2 \binom{(1-\gamma)|S_k|}{(1 - \frac{1}{K} - \gamma)|S_k|} \\ &= \log_2 \binom{(1-\gamma)|S_k|}{(1 - \frac{1}{K(1-\gamma)})(1-\gamma)|S_k|} \\ &\leq (1-\gamma)|S_k| H_2 \left(1 - \frac{1}{K(1-\gamma)}\right), \end{aligned}$$

where the last transition is by subadditivity of entropy. Recalling that $\gamma \geq \eta/8$ and $\eta > 0$ is a small constant we bound the rhs above by

$$\begin{aligned} (1-\gamma)|S_k| H_2 \left(1 - \frac{1}{K(1-\gamma)}\right) &\leq (1-\eta/8)|S_k| H_2 \left(1 - \frac{1}{K(1-\eta/8)}\right) \\ &\leq (1+\sqrt{\epsilon}) \frac{1}{K} |T| \cdot (1-\eta/8) H_2 \left(1 - \frac{1}{K(1-\eta/8)}\right), \end{aligned} \tag{322}$$

where in the second transition we also used the fact that by Lemma 161, **(2)**, we have $|S_k| \leq (1+\sqrt{\epsilon})\frac{1}{K}|T|$. At this point we also note that

$$\begin{aligned} (1-\eta/8) H_2 \left(1 - \frac{1}{K(1-\eta/8)}\right) &= \frac{1}{K} \log_2 K + \frac{1}{K \ln 2} - \frac{1}{K} \log \frac{1}{1 - 8/\eta} + O(1/K^2) \\ &\leq H_2(1 - 1/K) - \frac{1}{K} \log \frac{1}{1 - \eta/8} + O(1/K^2). \end{aligned}$$

since $H_2(1 - 1/K) = \frac{1}{K} \log_2 K + \frac{1}{K \ln 2} + O(1/K^2)$ and K is larger than a constant. Putting the above bounds together, we get, assuming that K is larger than $1/\eta$ by a large constant factor,

$$H(X_{\mathbf{i}} | M_{ALG}, \Lambda_{<k}, \{\mathbf{j} = \mathbf{i} \wedge Z = 1\}) \leq (1+\sqrt{\epsilon}) \frac{1}{K} |T| \cdot H_2(1 - 1/K) - \Omega(\eta/K)|T|.$$

for every $\mathbf{i} \in \mathcal{J}$, which by (320) implies for $\mathbf{i} \in \mathcal{J}$

$$H(X_{\mathbf{i}} | M_{ALG}, \Lambda_{<k}, \{\mathbf{j} = \mathbf{i}\}, Z) \leq (1+\sqrt{\epsilon}) \frac{1}{K} |T| \cdot H_2(1 - 1/K) - \Omega\left(\frac{\eta}{K^2}\right) |T| \tag{323}$$

Finally, for $\mathbf{i} \in \mathbf{B} \setminus \mathcal{J}$ we have the bound

$$H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j} = \mathbf{i}\}, Z) \leq (1 + \sqrt{\epsilon})\frac{1}{K}|T| \cdot H_2(1 - 1/K), \tag{324}$$

since the number of nonzeros in $X_{\mathbf{i}}$ is exactly $\lceil(1 - 1/K)|S_k\rceil$. Putting (323) and (324) together with (317) and using (319), we get

$$\begin{aligned} H(X|\Pi, \Lambda_{<k}) &\leq \sum_{\mathbf{i}\in\mathbf{B}} H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j} = \mathbf{i}\}) \\ &\leq \sum_{\mathbf{i}\in\mathbf{B}} (1 + H(X_{\mathbf{i}}|M_{ALG}, \Lambda_{<k}, \{\mathbf{j} = \mathbf{i}\}, Z)) \\ &\leq \sum_{\mathbf{i}\in\mathcal{J}} \left(H(X_{\mathbf{i}}|\Lambda_{<k}) - \Omega\left(\frac{\eta}{K^2}\right)|T|\right) + \sum_{\mathbf{i}\in\mathbf{B}\setminus\mathcal{J}} H(X_{\mathbf{i}}|\Lambda_{<k}) \\ &= \sum_{\mathbf{i}\in\mathbf{B}} H(X_{\mathbf{i}}|\Lambda_{<k}) - |\mathcal{J}| \cdot \Omega\left(\frac{\eta}{K^2}\right)|T|. \end{aligned}$$

On the other hand, since $|S_k| \geq (1 - \sqrt{\epsilon})\frac{1}{K}|T|$ for all choices of $\Lambda_{<k}$ by Lemma 161, **(2)**, we get, since the nonzeros of $X_{\mathbf{i}}$ are a uniformly random set of size $\lceil(1 - 1/K)|S_k|\rceil$, that

$$H(X|\Lambda_{<k}) \geq (1 - \sqrt{\epsilon})\frac{1}{K}|T| \cdot |\mathbf{B}| \cdot (1 - o_N(1))H_2(1 - 1/K).$$

Substituting this into (317), we get

$$\begin{aligned} s = |\Pi| &\geq \Omega\left(\frac{\eta}{K^2}\right)|\mathcal{J}| \cdot |T| - O(\sqrt{\epsilon})\frac{1}{K}|T| \cdot |\mathbf{B}| \cdot H_2(1 - 1/K) \\ &\geq \Omega\left(\frac{\eta}{K^2}\right)|\mathcal{J}| \cdot |T| \qquad (\text{since } \epsilon < K^{-100K^2} \text{ by (p6), (p5) and (p3)}) \\ &\geq \Omega\left(\frac{\eta}{K^3}\right)|\mathbf{B}| \cdot |T| \qquad (\text{since } |\mathcal{J}| \geq |\mathbf{B}|/(4K)) \\ &\geq \Omega_K(|\mathbf{B}| \cdot |T|). \end{aligned}$$

Finally, recall that by (p0)

$$N = m^n = n^{20n},$$

and therefore

$$|\mathbf{B}| \geq |\mathcal{F}|/K = 2^{\Omega(\epsilon^2 n)} = N^{\Omega_\epsilon(1/\log\log N)}.$$

To summarize, we get a lower bound of

$$s = \Omega_K(|\mathbf{B}| \cdot |T|) = |T|^{1+\Omega(1/\log\log|T|)},$$

as required.

■

References

[AK17] Sepehr Assadi and Sanjeev Khanna. Randomized composable coresets for matching and vertex cover. In Christian Scheideler and Mohammad Taghi Hajiaghayi, editors, *Proceedings of the 29th ACM Symposium on Parallelism in Algorithms and Architectures, SPAA 2017, Washington DC, USA, July 24-26, 2017*, pages 3–12. ACM, 2017.

[AKL17] Sepehr Assadi, Sanjeev Khanna, and Yang Li. On estimating maximum matching size in graph streams. In Klein [Kle17], pages 1723–1742.

[AKLY16] Sepehr Assadi, Sanjeev Khanna, Yang Li, and Grigory Yaroslavtsev. Maximum matchings in dynamic graph streams and the simultaneous communication model. In Krauthgamer [Kra16], pages 1345–1364.

[AMS96] Noga Alon, Yossi Matias, and Mario Szegedy. The space complexity of approximating the frequency moments. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 20–29. ACM, 1996.

[BGM$^+$19] Marc Bury, Elena Grigorescu, Andrew McGregor, Morteza Monemizadeh, Chris Schwiegelshohn, Sofya Vorotnikova, and Samson Zhou. Structural results on matching estimation with applications to streaming. *Algorithmica*, 81(1):367–392, 2019.

[BS15] Marc Bury and Chris Schwiegelshohn. Sublinear estimation of weighted matchings in dynamic data streams. In Nikhil Bansal and Irene Finocchi, editors, *Algorithms - ESA 2015 - 23rd Annual European Symposium, Patras, Greece, September 14-16, 2015, Proceedings*, volume 9294 of *Lecture Notes in Computer Science*, pages 263–274. Springer, 2015.

[CCE$^+$16] Rajesh Chitnis, Graham Cormode, Hossein Esfandiari, MohammadTaghi Hajiaghayi, Andrew McGregor, Morteza Monemizadeh, and Sofya Vorotnikova. Kernelization via sampling with applications to finding matchings and related problems in dynamic graph streams. In Krauthgamer [Kra16], pages 1326–1344.

[CJMM17] Graham Cormode, Hossein Jowhari, Morteza Monemizadeh, and S. Muthukrishnan. The sparse awakens: Streaming algorithms for matching size estimation in sparse graphs. In Kirk Pruhs and Christian Sohler, editors, *25th Annual European Symposium on Algorithms, ESA 2017, September 4-6, 2017, Vienna, Austria*, volume 87 of *LIPIcs*, pages 29:1–29:15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[CS14] Michael Crouch and Daniel S. Stubbs. Improved streaming algorithms for weighted matching, via unweighted matching. In Klaus Jansen, José D. P. Rolim, Nikhil R. Devanur, and Cristopher Moore, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2014, September 4-6, 2014, Barcelona, Spain*, volume 28 of *LIPIcs*, pages 96–104. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2014.

[EHL$^+$15] Hossein Esfandiari, Mohammad Taghi Hajiaghayi, Vahid Liaghat, Morteza Monemizadeh, and Krzysztof Onak. Streaming algorithms for estimating the matching size in planar graphs and beyond. In Piotr Indyk, editor, *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 1217–1233. SIAM, 2015.

[EHM16] Hossein Esfandiari, MohammadTaghi Hajiaghayi, and Morteza Monemizadeh. Finding large matchings in semi-streaming. In Carlotta Domeniconi, Francesco Gullo, Francesco Bonchi, Josep Domingo-Ferrer, Ricardo A. Baeza-Yates, Zhi-Hua Zhou, and Xindong Wu, editors, *IEEE International Conference on Data Mining Workshops, ICDM Workshops 2016, December 12-15, 2016, Barcelona, Spain.*, pages 608–614. IEEE Computer Society, 2016.

[ELSW13] Leah Epstein, Asaf Levin, Danny Segev, and Oren Weimann. Improved bounds for online preemptive matching. In Natacha Portier and Thomas Wilke, editors, *30th International Symposium on Theoretical Aspects of Computer Science, STACS 2013, February 27 - March 2, 2013, Kiel, Germany*, volume 20 of *LIPIcs*, pages 389–399. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2013.

[FKM$^+$05] Joan Feigenbaum, Sampath Kannan, Andrew McGregor, Siddharth Suri, and Jian Zhang. On graph problems in a semi-streaming model. *Theoretical Computer Science*, 348(2-3):207–216, 2005.

[FLN$^+$02] Eldar Fischer, Eric Lehman, Ilan Newman, Sofya Raskhodnikova, Ronitt Rubinfeld, and Alex Samorodnitsky. Monotonicity testing over general poset domains. In John H. Reif, editor, *Proceedings on 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada*, pages 474–483. ACM, 2002.

[GKK12] Ashish Goel, Michael Kapralov, and Sanjeev Khanna. On the communication and streaming complexity of maximum bipartite matching. In Yuval Rabani, editor, *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2012, Kyoto, Japan, January 17-19, 2012*, pages 468–485. SIAM, 2012.

[GKM$^+$19] Buddhima Gamlath, Michael Kapralov, Andreas Maggiori, Ola Svensson, and David Wajc. Online matching with general arrivals. In David Zuckerman, editor, *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019, Baltimore, Maryland, USA, November 9-12, 2019*, pages 26–37. IEEE Computer Society, 2019.

[GO16] Venkatesan Guruswami and Krzysztof Onak. Superlinear lower bounds for multipass graph processing. *Algorithmica*, 76(3):654–683, 2016.

[HPT$^+$19] Zhiyi Huang, Binghui Peng, Zhihao Gavin Tang, Runzhou Tao, Xiaowei Wu, and Yuhao Zhang. Tight competitive ratios of classic matching algorithms in the fully online model. In Timothy M. Chan, editor, *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2019, San Diego, California, USA, January 6-9, 2019*, pages 2875–2886. SIAM, 2019.

[Kap13] Michael Kapralov. Better bounds for matchings in the streaming model. In Sanjeev Khanna, editor, *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2013, New Orleans, Louisiana, USA, January 6-8, 2013*, pages 1679–1697. SIAM, 2013.

[KKS14] Michael Kapralov, Sanjeev Khanna, and Madhu Sudan. Approximating matching size from random streams. In Chandra Chekuri, editor, *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 734–751. SIAM, 2014.

[Kle17] Philip N. Klein, editor. *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*. SIAM, 2017.

[KMNT20] Michael Kapralov, Slobodan Mitrovic, Ashkan Norouzi-Fard, and Jakab Tardos. Space efficient approximation to maximum matching size from uniform edge samples. In Shuchi Chawla, editor, *Proceedings of the 2020 ACM-SIAM Symposium on Discrete Algorithms, SODA 2020, Salt Lake City, UT, USA, January 5-8, 2020*, pages 1753–1772. SIAM, 2020.

[Kra16] Robert Krauthgamer, editor. *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*. SIAM, 2016.

[KT17] Sagar Kale and Sumedh Tirodkar. Maximum matching in two, three, and a few more passes over graph streams. In Klaus Jansen, José D. P. Rolim, David Williamson, and Santosh S. Vempala, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2017, August 16-18, 2017, Berkeley, CA, USA*, volume 81 of *LIPIcs*, pages 15:1–15:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

[KVV90] Richard M. Karp, Umesh V. Vazirani, and Vijay V. Vazirani. An optimal algorithm for on-line bipartite matching. In Harriet Ortiz, editor, *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pages 352–358. ACM, 1990.

[MMPS17] Morteza Monemizadeh, S. Muthukrishnan, Pan Peng, and Christian Sohler. Testable bounded degree graph properties are random order streamable. In Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland*, volume 80 of *LIPIcs*, pages 131:1–131:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[MV16] Andrew McGregor and Sofya Vorotnikova. Planar matching in streams revisited. In Klaus Jansen, Claire Mathieu, José D. P. Rolim, and Chris Umans, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2016, September 7-9, 2016, Paris, France*, volume 60 of *LIPIcs*, pages 17:1–17:12. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

[MV18] Andrew McGregor and Sofya Vorotnikova. A simple, space-efficient, streaming algorithm for matchings in low arboricity graphs. In Raimund Seidel, editor, *1st Symposium on Simplicity in Algorithms, SOSA 2018, January 7-10, 2018, New Orleans, LA, USA*, volume 61 of *OASICS*, pages 14:1–14:4. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

[PS17] Ami Paz and Gregory Schwartzman. A $(2+\epsilon)$-approximation for maximum weight matching in the semi-streaming model. In Klein [Kle17], pages 2153–2161.

[WW15] Yajun Wang and Sam Chiu-wai Wong. Two-sided online bipartite matching and vertex cover: Beating the greedy algorithm. In Magnús M. Halldórsson, Kazuo Iwama, Naoki Kobayashi, and Bettina Speckmann, editors, *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part I*, volume 9134 of *Lecture Notes in Computer Science*, pages 1070–1081. Springer, 2015.