Topics in Theoretical Computer Science	March 30, 2013
Lecture 7	
Lecturer: Ola Svensson	*Scribes: Cedric Bastin*

The lecture and notes were inspired by

- *http://www-math.mit.edu/ goemans/18433S09/matroid-intersect-notes.pdf*
- *http://math.mit.edu/ goemans/18438F09/lec11.pdf*
- *https://courses.engr.illinois.edu/cs598csc/sp2010/Lectures/Lecture17.pdf*

1 Last lecture

Matroid A matroid is defined as $M = (E, \mathcal{I})$ where E is the ground set and $\mathcal{I} \subseteq 2^E$ is a set containing subsets of E which we call independent sets, such that:

(i) if $A \subseteq B \subseteq E$ and $B \in \mathcal{I}$ then $A \in \mathcal{I}$ (downward monotonicity).

(ii) if $A \in \mathcal{I}$ and $B \in \mathcal{I}$ and $|A| > |B|$ the $\exists a \in A \backslash B$ s.t. $B + a \in \mathcal{I}$ (here, the $+$ operator is defined as follows: given $A \subseteq E$ and $a \in E$, $A + a = A \cup \{a\}$).

A matroid typically represents a problem that can be solved optimally using a greedy algorithm, and thus has a limited expressiveness. This follows from the fact that there is a greedy algorithm that, given any matroid, returns a maximum weight independent set.

Circuit A circuit of a matroid is a *minimal dependent* set (inclusion wise), i.e., for matroid $M = (E, \mathcal{I})$ $C \subseteq E$ is a circuit iff $C \notin \mathcal{I}$ and $\{C - x : \forall x \in C\}$ are independent sets. It follows that if $S \in \mathcal{I}$ and $C = S + e$ is a circuit, C is the only subset of $S + e$ that is a circuit.

Rank Given a matroid $M = (E, \mathcal{I})$, the rank function $r_M : 2^E \to \mathbb{N}$ of M is defined as:

$$r_M(S) = \max\{|I| : I \subseteq S, I \in \mathcal{I}\}$$

Frequently, we drop the subscript and write r instead of r_M. The rank function has the following properties: $0 \leq r(S) \leq |S|$ and $r(S) \leq r(T)$ for $S \subseteq T$.

Span Given a matroid $M = (E, \mathcal{I})$, the span of $S \subseteq E$ is the set defined as:

$$\text{span}(S) = \{e \in E : r(S + e) = r(S)\}$$

Clearly, for any $S \subseteq E$, $S \subseteq \text{span}(S)$.

Matroid Polytope Given a matroid $M = (E, \mathcal{I})$, its matroid polytope $P_M = \text{conv}(\{x_s \in \{0,1\}^{|E|} : S \in \mathcal{I}\})$ is the convex hull of the incidence vectors of the independent sets of M. It can be proved that the matroid polytope can be described exactly by the following set of linear inequalities:

$$P_M = \{x \in \mathbb{R}_+^{|E|} : \sum_{e \in S} x_e \leq r(S), \forall S \subseteq E\}$$

Matroid Base Polytope Similarly, given a matroid $M = (E, \mathcal{I})$, its matroid base polytope is defined as is the convex hull of the incidence vectors of the bases of M: $P_M^B = \text{conv}(\{x_s \in \{0,1\}^{|E|} : S \text{ is a base of } M\})$. Similarly to the case of the matroid polytope, the matroid base polytope can be described by the following set of linear inequalities:

$$P_M^B = \{x \in \mathbb{R}_+^{|E|} : \sum_{e \in S} x_e \leq r(S), \forall S \subseteq E \text{ and } \sum_{e \in E} x_e = r(E)\}$$

2 Matroid Intersection

To overcome the limited expressiveness of matroids we introduce matroid intersection, which allows us to express additional combinatorial optimization problems such as bipartite matching. The algorithm for optimizing over the intersection of 2 matroids runs in polynomial time, whereas optimizing over the intersection of 3 or more matroids is NP-hard. We will introduce some related concepts and show examples of matroid intersection.

Definition 1 (Matroid Intersection) *Given two matroids $M_1 = (E, \mathcal{I}_1)$ and $M_2 = (E, \mathcal{I}_2)$ over the* same *ground set E, the intersection of the two matroids is defined as $M_1 \cap M_2 = (E, \mathcal{I}_1 \cap \mathcal{I}_2)$.*

Example 1 (Bipartite matching) *Given $G = (A \cup B, E \subseteq A \times B)$, the bipartite matching problem can be formulated as the intersection of two matroids M_1, M_2 which have E as their ground set and*

$$\mathcal{I}_1 = \{S \subseteq E | \forall v \in A : |S \cap \delta(v)| \leq 1\}$$
$$\mathcal{I}_2 = \{S \subseteq E | \forall v \in B : |S \cap \delta(v)| \leq 1\}$$

where $\delta(v)$ is the set of all matched edges incident to v. Now, $\mathcal{I}_1 \cap \mathcal{I}_2$ is the set of all sets of edges that contain at most one edge incident to each vertex, hence the set of all matchings.

Example 2 (Arborescence) *Consider a directed graph G=(V,E); a set $T \subseteq E$ is called an* arborescence *if:*

- *T contains no undirected cycle.*
- *The in-degree of each vertex is at most 1.*

We can express arborescences as the edge sets contained in the intersection of two matroids, where E is the common ground set and:

- *$\mathcal{I}_1$ is the set of all edges that form a forest, i.e., (E, I_1) is a graphic matroid.*
- *$\mathcal{I}_2$ is the set of all edges which contains at most 1 edge in E_v, for all vertices v, where E_v is the set of incoming edges of v. Since G is directed, the different E_v-s are disjoint, and hence this set of edges forms a matroid called partition matroid.*

3 Matroid Intersection Polytope

The matroid intersection polytope with 2 matroids is:

$$\sum_{e \in S} x_e \leq r_1(S), \forall S \subseteq E$$
$$\sum_{e \in S} x_e \leq r_2(S), \forall S \subseteq E$$
$$x_e \geq 0, \forall e \in E$$

The polytope for the intersection between 3 or more matroids is not as easy to formulate and will be covered in the lecture of week 8.

Theorem 2 *Given 3 matroids M_1, M_2 and M_3 it is NP-hard to find a maximum cardinality independent set $\mathcal{I}_1 \cap \mathcal{I}_2 \cap \mathcal{I}_3$*

The theorem can be proven by providing a reduction to the Hamiltonian cycle problem which is well known to be NP-complete.

4 Matroid Intersection Theorem

Theorem 3 (Matroid Intersection Theorem) *For matroids* $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2)$

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{U \subseteq E} (r_1(U) + r_2(E \backslash U))$$

Proof $\Rightarrow$ (max $\leq$ min):
To see that max $\leq$ min for $U \subseteq E$ and $I \in \mathcal{I}_1 \cap \mathcal{I}_2$, we have

$$|I| = |I \cap U| + |I \cap (E \backslash U)| \leq r_1(U) + r_2(E \backslash U)$$

since $I \cap U$ is an independent set in $\mathcal{I}_1$ and $I \cap (E \backslash U)$ is an independent set in $\mathcal{I}_2$.

$\Leftarrow$ The main goal of this lecture is to prove the other direction. ■

Note that the matroid intersection theorem generalizes König's theorem:

$$\text{maximum matching} = \max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{U \subseteq E} (r_1(U) + r_2(E \backslash U)) = \text{minimum vertex cover}$$

Exercise 1 *(a) If $A \subseteq B$ then span$(A) \subseteq$ span(B)*

(b) If $e \in$ span(A) then span$(A + e) =$ span(A)

Proof The proof will use the submodularity of the rank function:

$$r(X) + r(Y) \geq r(X \cap Y) + r(X \cup Y)$$

(a) Suppose that $e \in \text{span}(A)$, by submodularity with $X = A + e$ and $Y = B$
$r(A + e) + r(B) \geq r((A + e) \cap B) + r((A + e) \cup B)$
$r(A + e) + r(B) \geq r((A + e) \cap B) + r(B + e)$
$r(A + e) + r(B) \geq r(A) + r(B + e)$
$r(B) \geq r(B + e)$ as $r(A) = r(A + e)$ for $e \in \text{span}(a)$
Since $r(B) = r(B + e) \Rightarrow e \in \text{span}(B)$, $e \in \text{span}(A) \Rightarrow e \in \text{span}(B)$ and $\text{span}(A) \subseteq \text{span}(B)$.

(b) By the previous proof we know that: $A \subseteq A + e \Rightarrow \text{span}(A) \subseteq \text{span}(A + e)$. Take $f \in \text{span}(A + e)$; we need to show that $f \in \text{span}(A)$. Let $X = A + e$ and $Y = A + f$; by submodularity of the rank function we have:
$r(A + e) + r(A + f) \geq r(A + e \cap A + f) + r(A + e \cup A + f)$
$r(A) + r(A + f) \geq r(A) + r(A + e + f)$
$r(A + f) \geq r(A + e + f) \Rightarrow r(A + f) = r(A + e + f)$
But $f \in \text{span}(A + e)$ and $e \in \text{span}(A)$ so $r(A + f) = r(A)$ and $f \in \text{span}(A)$. Note that we also get: $\text{span}(\text{span}(A)) = \text{span}(A)$

■

Exercise 2 *Consider the graph G with a k-coloring, i.e., the edge set E is partitioned into (disjoint) color classes $E_1 \cup E_2 \cup ... \cup E_k$. Formulate the question, whether there exists a colorful spanning tree (i.e., a spanning tree with edges of different colors), as a matroid intersection problem.*

Solution One matroid M_1 can obviously be specified as the graphic matroid which defines an acyclic subgraph in a graph. The second matroid M_2 can be considered to be the partition matroid which partitions the colorful edges such that only one edge of each color can be picked.

5 Strong Basis Exchange Property

The following is a well-known fact concerning matroids, often called the Strong Basis Exchange Property:

Lemma 4 *Given a matroid $M = (E, \mathcal{I})$, for any two bases B, B', $\forall x \in B \backslash B', \exists y \in B' \backslash B$, s.t. $B - x + y$ and $B' - y + x$ are independent and thus new bases.*

Proof Consider $x \in B \backslash B'$. Since B' is a base and $B' + x$ is dependent, there is a unique circuit $C \subseteq B' + x$. We have $x \in \text{span}(C - x) \Rightarrow x \in \text{span}((B \cup C) - x)$. As seen in the previous exercise $\text{span}((B \cup C) - x) = \text{span}(B \cup C) = E$ (because B is a base of E). Hence we have a new base $B'' \subseteq (B \cup C) - x$ because the rank of a set containing a base equals the cardinality of a base.
$B - x$ and B'' are independent with $|B''| > |B - x| \Rightarrow \exists y \in B'' \backslash (B - x)$ s.t. $B - x + y \in \mathcal{I}$
However $B'' \backslash (B - x) \subseteq (B \cup C - x) \backslash (B - x) \subseteq C - x$ and $y \in C - x$
So both $x, y \in C$ and therefore $B' + x - y \in \mathcal{I}$. ■

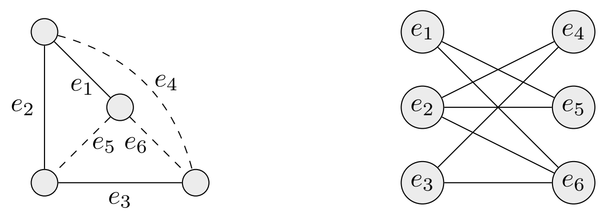
For example, the above implies we can switch 2 edges between 2 spanning trees over the same graph and obtain 2 new spanning trees. The Strong Basis Exchange Property will be used to design an algorithm which finds a maximum cardinality set in the intersection of two matroids.

6 Exchange Graph

A key object in the algorithm for finding a maximum cardinality set in the intersection of two matroids is the so-called exchange graph:

Definition 5 *Given a matroid $M = (E, \mathcal{I})$ and an independent set $I \in \mathcal{I}$, the exchange graph $D_M(I)$ is a bipartite graph with left hand side I, right hand side $E \backslash I$ and an edge (y, x) from $y \in I$ to $x \in E \backslash I$ if $I - y + x \in I$.*

Example 3 *A graphic matroid with the exchange graph $D(\{e_1, e_2, e_3\})$.*



Next, we will prove a couple of properties that we will use in the design of the matroid intersection algorithm.

Lemma 6 *Let $I, J \in \mathcal{I}$ s.t. $|I| = |J|$*
Then there is a perfect matching between $I \backslash J$ and $J \backslash I$ in $D_M(I)$

Proof We define a truncated matroid $M' = (S, \mathcal{I}' = \{I' \in \mathcal{I} : |I'| \leq |I|\})$; then I and J are bases in M'. We take $x \in J \backslash I$; by the strong basis exchange lemma there exists $y \in I \backslash J$ s.t. $J - x + y \in \mathcal{I}$ and $I - y + x \in \mathcal{I}$ are bases in M', which implies that (y, x) is an edge in $D_M(I)$.

We "match" y with x and replace I, J with $I, J - x + y$ and proceed inductively. As $I \backslash J$ decreases in each step we will eventually end up with a perfect matching. (Note that $|I \backslash J| = |I \backslash (J - x + y)| + 1$) ■

Example

$I = \{e_1, e_2, e_3\}, J = \{e_4, e_5, e_6\}$
The proof algorithm could develop as follows:
- select e_4 and match it to e_1 then update J to be $\{e_1, e_5, e_6\}$
- select e_5 and match it to e_2 then update J to be $\{e_1, e_2, e_6\}$
- finally select e_6 and match it to e_3.

Remark: The converse of the above lemma does not hold in general!

Lemma 7 *Let $I \in \mathcal{I}$ with exchange graph $D_M(I)$. Let J be a set with $|J| = |I|$ s.t. $D_M(I)$ has a unique matching between $I \backslash J$ and $J \backslash I$; then $J \in \mathcal{I}$.*

Proof Let N be a unique matching. Orient the edges of N from $E \backslash I$ to I (left to right) and the other edges are oriented from I to $E \backslash I$ (right to left). Now, the graph is acyclic, otherwise the matching would not be unique (i.e., switch matched edges on the alternating cycle) hence we can topologically sort the vertices.

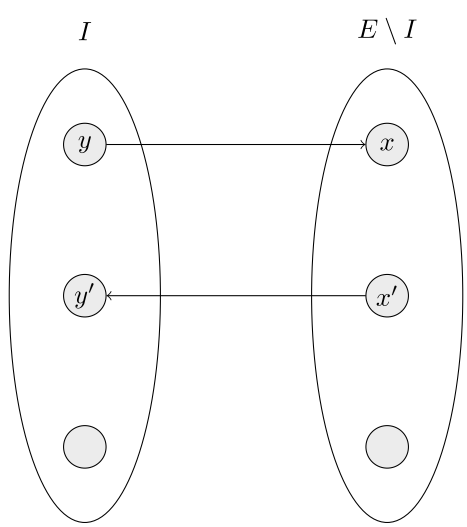
We number the edges $N = \{(y_1, x_1), ..., (y_t, x_t)\}$ s.t. there is no edge (y_i, x_j) with $j > i$. We suppose toward contradiction that $J \notin \mathcal{I}$ (not independent) and let C be a circuit of J. We take the smallest index i s.t. $x_i \in C$; then there is no edge $(y_i, x) \forall x \in C - x_i$ due to the ordering we performed (y_i must exist by construction). This mean that $I - y_i + x \notin \mathcal{I} \Rightarrow x \in \text{span}(I - x_i), \forall x \in C - x_i$ hence $C - x_i \subseteq (I - y_i)$. Now, $\text{span}(C - x_i) \subseteq \text{span}(\text{span}(I - y_i)) = \text{span}(I - y_i)$, but C is a circuit and hence $x_i \in \text{span}(C - x_i) \Rightarrow x_i \in \text{span}(I - y_i)$ with rank $r(C - x_i) = |C - x_i| = |C| - 1$. This implies $I - y_i + x_i \notin \mathcal{I}$ contradicting that there was an edge (y_i, x_i). ■

7 "Augmenting path" Matroid Intersection Algorithm

The Matroid Intersection Algorithm has the following main procedure: Given $I \in \mathcal{I}_1 \cap \mathcal{I}_2$ the algorithm produces $J \in \mathcal{I}_1 \cap \mathcal{I}_2$ s.t. $|J| = |I| + 1$, or it gives a certificate that I is an independent set of maximum cardinality in $|I_1 \cap \mathcal{I}_2|$ by exhibiting a set $U \subseteq E$ s.t. $|I| = r_1(U) + r_2(E \backslash U)$.

In order to fully define the Matroid Intersection Algorithm, we need to define its exchange graph:

Definition 8 (Matroid Intersection Exchange Graph) *For $I \in \mathcal{I}_1 \cap \mathcal{I}_2$, the exchange graph $D_{M_1,M_2}(I)$ is the* directed *bipartite graph with left hand side I and right hand side $E \backslash I$ with edges (y, x) if $I - y + x \in \mathcal{I}_1$ and edges (x, y) if $I - y + x \in \mathcal{I}_2$.*



Remark D_{M_1,M_2} is the *union* of $D_{M_1}(I)$ and the reverse of $D_{M_2}(I)$

The algorithm for finding a maximum cardinality independent set in the intersection of two matroids works as follows: it is an iterative algorithm, and at every iteration we have a tentative independent set I in the intersection of $\mathcal{I}_1$ and $\mathcal{I}_2$ (in the absence of an initial one, finding a set of cardinality 1 is easy). The algorithm repeats the following:

- Given I, construct $D_{M_1,M_2}(I)$. Let $X_1 = \{e \in E \backslash I : I + e \in \mathcal{I}_1\}$, $X_2 = \{e \in E \backslash I : I + e \in \mathcal{I}_2\}$. Try to find a *shortest* path P from X_1 to X_2 in $D_{M_1,M_2}(I)$, which can be found (if it exists) by considering X_1 and X_2 as two nodes in the exchange graph (i.e., collapse them into two nodes) and applying breadth-first search unto the resulting graph, starting from X_1.
- If there is such a shortest path P, set $I' = I \triangle V(P)$ and iterate.
- Otherwise, if there is no such path between X_1 and X_2, output I.

7.1 Optimality

In order to prove that the algorithm returns a maximum cardinality independent set in the intersection of the two matroids, we have to prove that:

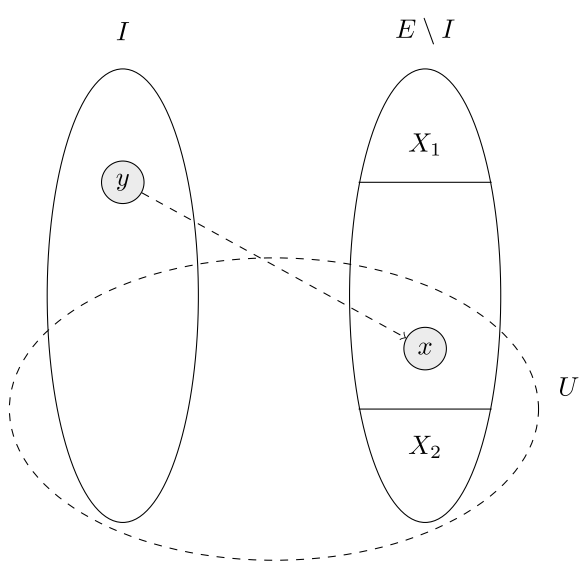
- If we find a shortest path between X_1 and X_2, $I' \in \mathcal{I}_1 \cap \mathcal{I}_2$.
- If there is no such path, then I is a maximum cardinality set in $\mathcal{I}_1 \cap \mathcal{I}_2$.

We proceed to prove the above:

Lemma 9 *If no $X_1 - X_2$ path in $D_{M_1,M_2}(I)$ then I is a maximum cardinality independent set of $\mathcal{I}_1 \cap \mathcal{I}_2$.*

Proof Note that if $X_1 = \emptyset$ then I is base of M_1 and hence optimal. The same applies to M_2 so we assume $X_1 \neq \emptyset \neq X_2$.

Let U be those nodes that can reach a vertex in x_2 in $D_{M_1,M_2}(I)$. The existence of no $X_1 - X_2$ path implies that $X_2 \subseteq U, X_1 \cap U = \emptyset, \delta^-(U) = \emptyset$.



Claim 10 $r_1(U) \leq |I \cap U|$.

Proof If $r_1(U) > |I \cap U|$, $\exists x \in U \backslash (I \cap U)$ s.t. $(I \cap U) + x \in \mathcal{I}_1$. Note that $I + x \notin \mathcal{I}_1$ since $x \in U$ and $X_1 = \emptyset$. Since $(I \cap U) + x \in \mathcal{I}_1$ but $I + x \notin \mathcal{I}_1$, there must exist a $y \in I \backslash U$ s.t. $I - y + x \in \mathcal{I}_1$. Then (y, x) would be an edge in $D_{M_1,M_2}(I)$ which contradicts $\delta^-(U) = \emptyset$ (c.f. figure). ■

Claim 11 $r_2(E \backslash U) \leq |I \backslash U|$.

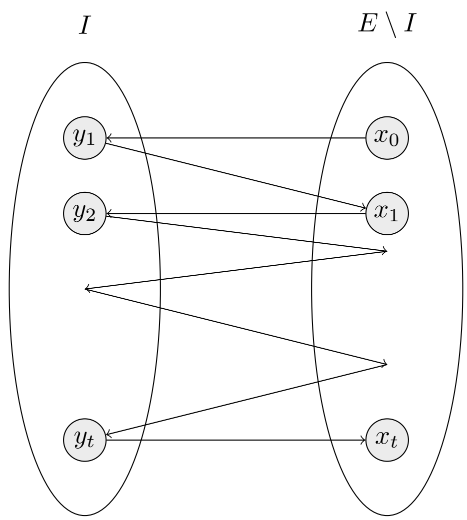
Proof If $r_2(E \backslash U) > |I \backslash U|$ then $\exists x \in (E \backslash U) \backslash (I \backslash U)$ s.t. $I \backslash U + x \in \mathcal{I}_2$ but then $\exists y \in I \cap U$ s.t. $I - y + x \in \mathcal{I}_2$. This would result in (x, y) being an arc in D_{M_1,M_2} contradicting that $x \notin U$.■

Thus $|I| = |I \cap U| + |I \backslash U| \geq r_1(U) + r_2(E \backslash U)$, and therefore I is the maximum cardinality independent set in $\mathcal{I}_1 \cap \mathcal{I}_2$ with $|I| = r_1(U) + r_2(E \backslash U)$. ■

The above lemma also implies the Matroid Intersection Theorem, since it establishes that whenever we cannot find an augmenting path, we can assert that $|I| = r_1(U) + r_2(E \backslash U)$:
Proof of $\Leftarrow$ of matroid intersection theorem:

Finally we have: $|I| = |I \cap U| + |I \backslash U| \geq r_1(U) + r_2(E \backslash U)$.

Combined with the other direction proved earlier we finally have: $|I| = |I \cap U| + |I \backslash U| = r_1(U) + r_2(E \backslash U)$. ■



Lemma 12 *If P is a shortest path $X_1 - X_2$ in D_{M_1,M_2} then $I' = I \Delta V(P)$ is in $\mathcal{I}_1 \cap \mathcal{I}_2$.*

Proof Let $P = x_0, y_1, x_1, ...y_t, x_t$ be the shortest path from X_1 to X_2. Let $J = \{x_1, .., x_t\} \cup (I \backslash \{y_1, ..., y_t\})$; we have $J \subseteq E, |J| = |I|$ s.t. the arcs from both paths form a unique matching from $I \backslash J$ to $J \backslash I$ i.e., from $\{y_1, ..., y_t\}$ to $\{x_1, ..., x_t\}$since otherwise P would have a shortcut and would not be a shortest path. Hence, by Lemma 6 $J \in \mathcal{I}_1$.

Now, $x_i \notin X_1$ for $i \geq 1$, otherwise the path P would be longer than the shortest $X_1 - X_2$ path. This means that $I + x_i \notin \mathcal{I}_1 \rightarrow r_1(I \cup J) = r_1(I) = r_1(J) = |I| = |J|$, so $\nexists x \in I \backslash J$ s.t. $J + x$ would be independent; however $I + x_0$ is independent and $|I + x_0| = |J| + 1$ hence $J + x_0 \in \mathcal{I}_1$ and $I' = (I \backslash \{y_1, ..., y_t\}) \cup \{x_0, ..., x_t\} \in \mathcal{I}_1$. Finally, by symmetry $I' \in \mathcal{I}_2$. ■

Running Time With $r = \max(r_1(E), r_2(E))$ we construct D_{M_1,M_2} in $O(rn)$ calls to the oracle. The augmenting path can be found in time $O(rn)$ which we have to do at most r times before we obtain an independent set. Thus the algorithm runs in $O(r^2 n)$ time.