IP=PSPACE

Sumcheck protocol for #SAT

Definition of #SAT

$\#SAT = \{\langle \varphi, K \rangle : \varphi \text{ is a 3CNF formula and it has } \textit{exactly } K \text{ satisfying assignments}\}.$

Probably harder than any problem in NP or coNP…

Step 1: Arithmetization

There is a multivariate polynomial

$$P_\varphi(X_1, \ldots, X_n) = \prod_{j=1}^{m} p_j(X_1, \ldots, X_n)$$

Moreover, it satisfies the following:

1. It has degree at most $3m$.
2. It has a representation of size $O(m)$ (just keep the p_j's) and given, $X_1, \ldots, X_n$, P_φ can be evaluated in polynomial time.

It follows that

$$\langle \varphi, K \rangle \iff \sum_{b_1 \in \{0,1\}} \cdots \sum_{b_n \in \{0,1\}} P_\varphi(b_1, \ldots, b_n) = K$$

We devise a IP system to check the equation (RHS)

1.5: Preprocessing

- P: sends a prime p in $[2^n, 2^{2n}]$
- V: verifies that p is a prime

This reduces the problem to that of checking

$$\sum_{b_1 \in \{0,1\}} \cdots \sum_{b_n \in \{0,1\}} P_\varphi(b_1, \dots, b_n) = K \mod p$$

2. Sumcheck protocol

Goal check: $\sum_{b_1\in\{0,1\}} \cdots \sum_{b_n\in\{0,1\}} P_\varphi(b_1,\ldots,b_n) = K \mod p$

V: If $n=1$, check that $P_\varphi(1)+P_\varphi(0)=K$. If so accept; otherwise reject. If $n\geq 2$ proceed as follows:

P: Sends $s(X_1)$ that is supposed to equal $h(X_1) := \sum_{b_2\in\{0,1\}} \cdots \sum_{b_n\in\{0,1\}} P_\varphi(X_1, b_2 \ldots, b_n)$.

(Note that $s(X_1)$ is a univariate polynomial of degree $\leq 3m$ since P_φ has degree $3m$ and can therefore be transmitted efficiently.)

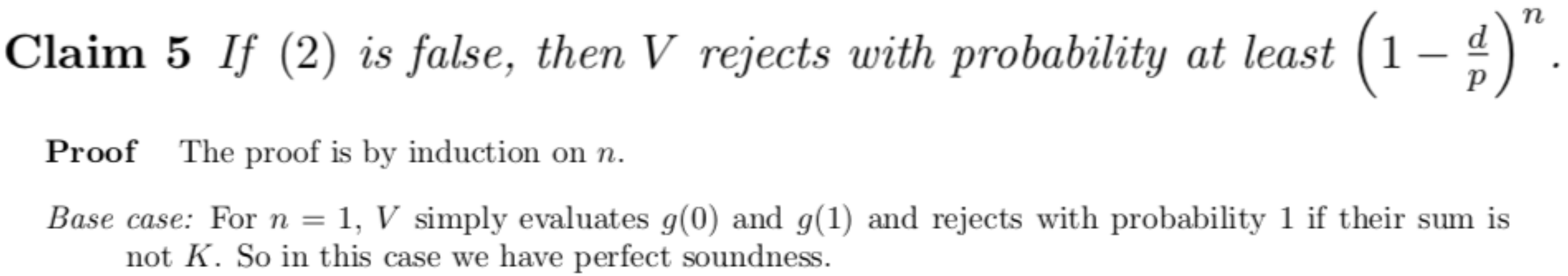
V: Reject if $s(0)+s(1)\neq K$; otherwise pick a *random* number $a\in\{0,\ldots,p-1\}$. Recursively use the same protocol to check that

$$s(a) = \sum_{b_2\in\{0,1\}} \cdots \sum_{b_n\in\{0,1\}} P_\varphi(a, b_2 \ldots, b_n) \qquad (= h(a))$$

Completeness

- Perfect, the prover simply sends the correct polynomial *h* in each step

Soundness

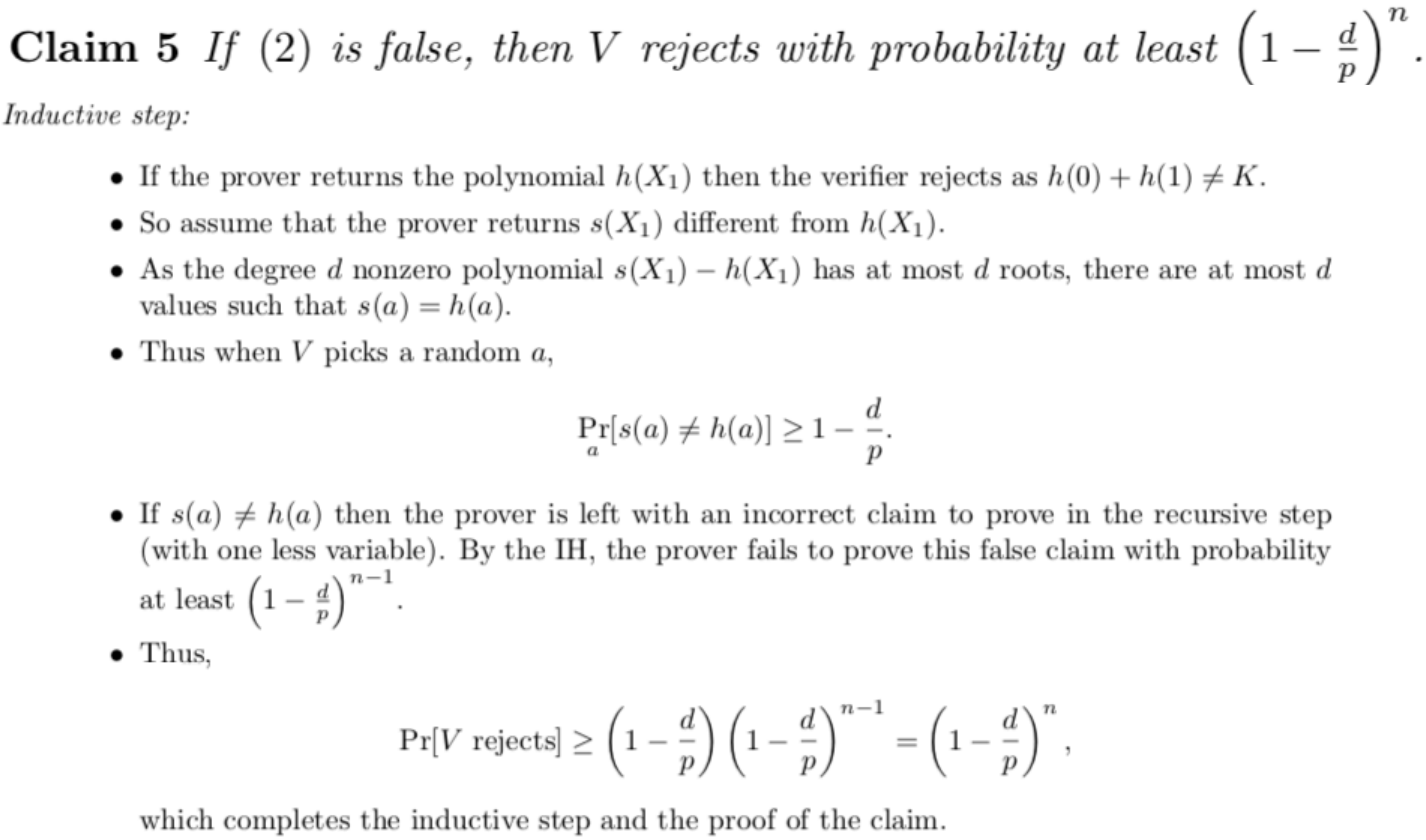


Claim 5 *If (2) is false, then V rejects with probability at least* $\left(1-\frac{d}{p}\right)^n$.

Proof The proof is by induction on n.

Base case: For $n = 1$, V simply evaluates $g(0)$ and $g(1)$ and rejects with probability 1 if their sum is not K. So in this case we have perfect soundness.

Soundness



Claim 5 *If (2) is false, then V rejects with probability at least* $\left(1-\frac{d}{p}\right)^n$.

Inductive step:

- If the prover returns the polynomial $h(X_1)$ then the verifier rejects as $h(0)+h(1) \neq K$.
- So assume that the prover returns $s(X_1)$ different from $h(X_1)$.
- As the degree d nonzero polynomial $s(X_1) - h(X_1)$ has at most d roots, there are at most d values such that $s(a) = h(a)$.
- Thus when V picks a random a,

$$\Pr_a[s(a) \neq h(a)] \geq 1 - \frac{d}{p}.$$

- If $s(a) \neq h(a)$ then the prover is left with an incorrect claim to prove in the recursive step (with one less variable). By the IH, the prover fails to prove this false claim with probability at least $\left(1-\frac{d}{p}\right)^{n-1}$.
- Thus,

$$\Pr[V \text{ rejects}] \geq \left(1-\frac{d}{p}\right)\left(1-\frac{d}{p}\right)^{n-1} = \left(1-\frac{d}{p}\right)^n,$$

which completes the inductive step and the proof of the claim.

Let’s get back to IP=PSPACE

Idea: do the same thing for PSPACE complete language

$\mathrm{TQBF} = \{\Psi : \Psi \text{ is a quantified } \textit{true} \text{ Boolean formula of the form } \forall x_1, \exists x_2, \ldots, Q_n x_n \varphi(x_1, \ldots, x_n)\}.$

Note that a formula $\Psi = \forall x_1, \exists x_2, \ldots, Q_n x_n \varphi(x_1, \ldots, x_n)$ can be arithmetized and $\Psi \in \mathrm{TQBF}$ if and only if

$$\prod_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \prod_{b_3 \in \{0,1\}} \cdots \sum_{b_n \in \{0,1\}} P_\varphi(b_1, \ldots, b_n) > 0.$$

So it looks like we can run the sum check protocol where the prover provides a K > 0 and we check if LHS = K.

There are two (smallish) problems. What are they?