Probabilistic Checkable Proofs

How to verify a proof by reading a constant number of bits

Bundit Laekhanukit
ITCS@SUFE

Given a mathematical proof,

can we verify it by skimming?

Recall : Classical NP-Proof System for NP language L.

Claim: $x \in L$

Prover

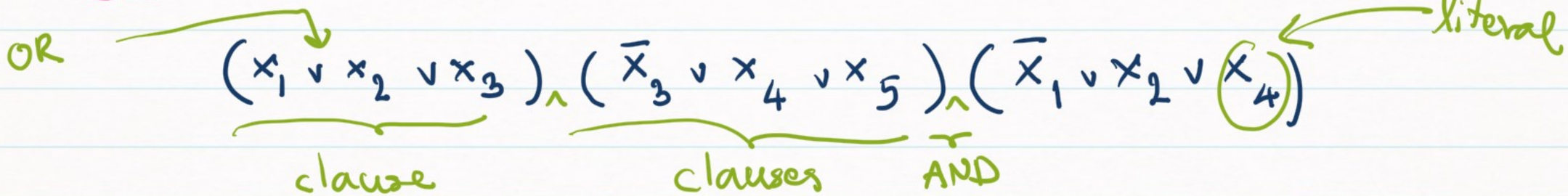
Verifier

witness y

- Read y and decide in time $\text{poly}(\|x\|)$ whether to accept or reject.

Let's consider 3-SAT :

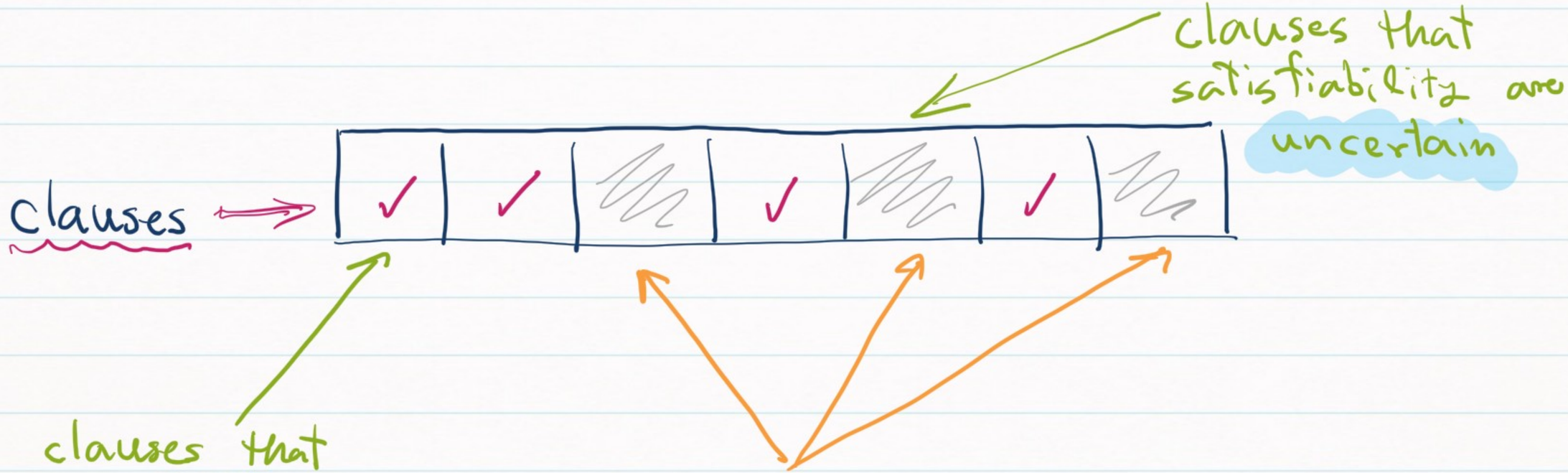
INPUT : 3-CNF formula ϕ -- Boolean formula of a form



GOAL : Decide whether $\exists$ an assignment z s.t. $\phi(z) = \text{TRUE}$

Let's take a feasible solution z as a witness.

How many bits do we need to read ?



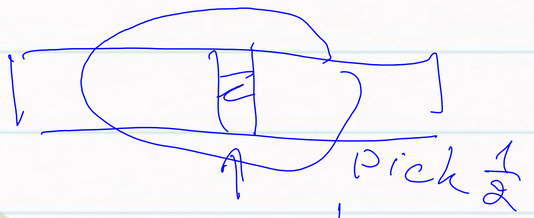
Suppose we read $n-1$ bits from the assignment z.
But, we miss to read z_j (assignment to x_j)

$\Rightarrow$ The satisfiability of some clauses are uncertain

Second attemp.

Yes If $\exists$ a satisfying assignment $\Rightarrow$ Accept w.p. 1

No If $\nexists$ satisfying assignment $\Rightarrow$ Accept w.p. $\frac{1}{2}$

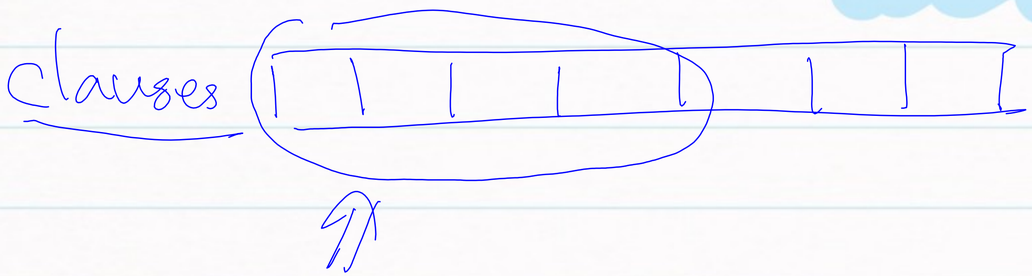


≥ 1 clause is not satisfied

$\Rightarrow$ Pr[picked unsat clause] $\geq \frac{1}{2}$

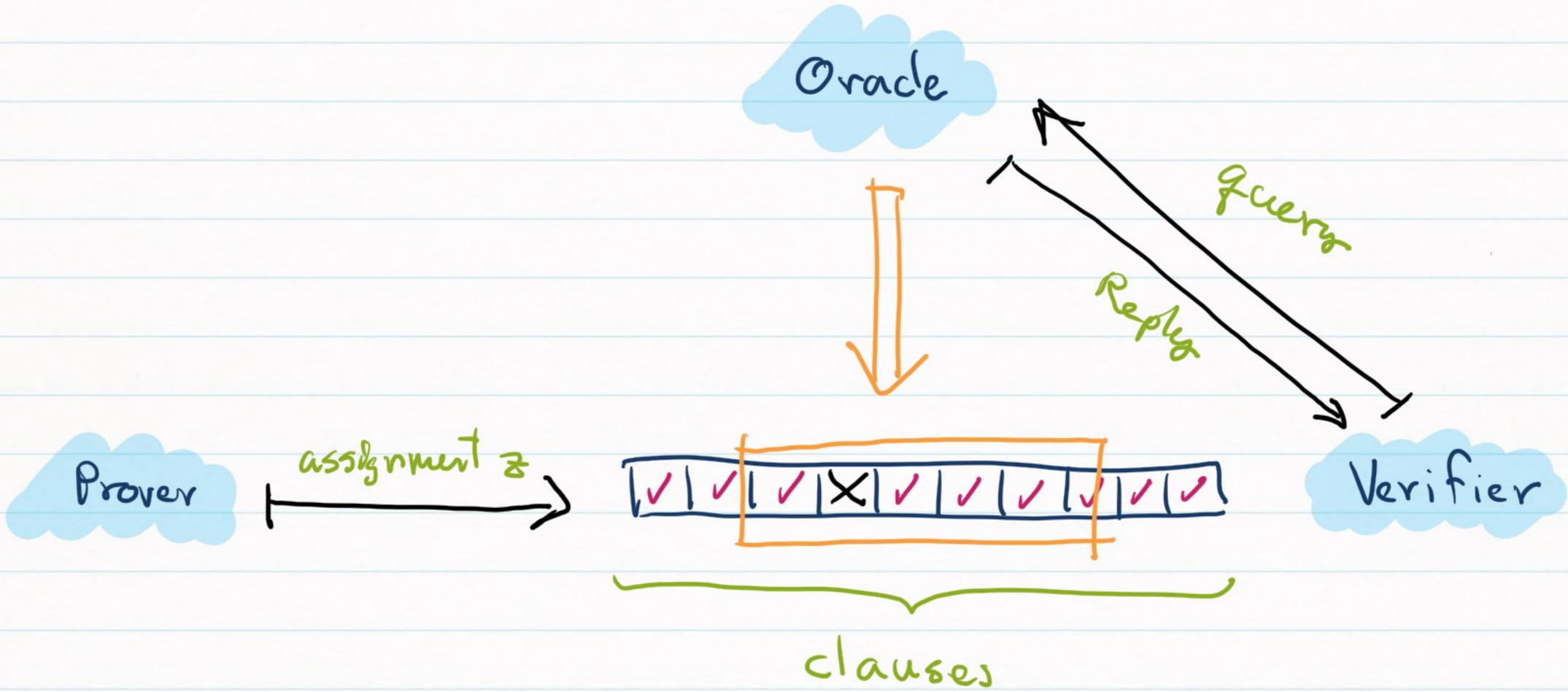
Assume we have an oracle $\mathcal{O}$ that can evalute clauses for us

Can we use a constant # of queries?



fix (but cannot see it)

- Pick a bunch of clauses, say $\frac{1}{2}$ of the clauses.
- Ask oracle if the given assignment satisfies all the clauses we picked.



Ask oracle to bulk evaluate $\frac{m}{2}$ clases

$\Rightarrow$ Pr [found UNSAT clause] = $\frac{1}{2}$

Probabilistic Checkable Proof (PCP)

Prover

- prepare proof π

One-shot

π

have random access to π

Verifier

- asks Prover to encode assignment
- asks Oracle to read $\pi_i, \pi_j, \ldots$ randomly

Oracle

Formulate the Idea

Proof of size $\binom{m}{m/2} \approx 2^m$

- Ask Prover to evaluate every $\frac{m}{2}$ clauses.
- Randomly read $O(1)$ positions.
- Hard part is to ensure that

  Prover CANNOT lie.

⇨ need consistency check.

Implementing the idea

- Transform 3SAT $\phi \mapsto$ Quadratic Eq.

$x_i \in \{0,1\}$

$\overline{x_i} \Rightarrow (1 - x_i)$

$x_i \wedge x_j \Rightarrow x_i \cdot x_j$

$x_i \vee x_j \Rightarrow (1 - (1-x_i)(1-x_j))$

$a \vee b = \overline{(\bar{a} \wedge \bar{b})}$

$(x_1 \vee x_2 \vee x_3) \Rightarrow$ deg-3 equation

dummy.

$x_1 \cdot x_2 \cdot x_3 \Rightarrow x_1 \cdot y_{23}$

$\rightarrow$ add eq. $(y_{23} - x_2 \cdot x_3 = 0)$

Quadratic Equations Problem (QEP)

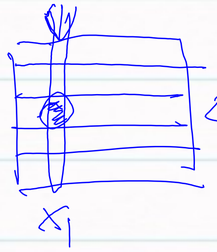
- **Input**:

$$\begin{aligned} e_1(x_1, \dots, x_n) &= c_1 \\ e_2(x_1, \dots, x_n) &= c_2 \\ &\vdots \\ e_m(x_1, \dots, x_n) &= c_m \end{aligned}$$

} call Σ

- **Goal**: Decide whether the system has a solution.

Write all truth table



Fix x

← Read the row instead ⇒ has info of all vars.

Interesting Facts (of functions over $\mathbb{F}_2$)

$\exists\ 2^{n^2}$ quadratic functions

- $c(x)$ is Quadratic

$$\Rightarrow c(x) = \sum_{i,j} P_{ij}\, x_i x_j \quad , \quad P : n \times n \text{ matrix}$$

Fix assignment z

$$\rightarrow f_z(P) = \sum_{i,j} P_{i,j} \boxed{x_i x_j}$$ is Linear

$P_{i,j}$: variable, $x_i x_j$: coefficient

- **Linearity**: $f_z(p) + f_z(q) = f_z(p+q)$
- **Quadraticity**: l_1, l_2 are linear $\Rightarrow f_z(l_1) \cdot f_z(l_2) = f_z(l_1 l_2)$
- **Self Producability**: $f_z(a+b) + f_z(b) = f_z(a)$

Exponential-Sized PCP for 3-SAT

QEP

* φ has a solution $\Leftrightarrow \exists z : E(z) = \sum_i (c_i - e_i(z)) = 0$

Quadratic Function at z

If $E(z) \neq 0 \Rightarrow$ $I \underset{Rand}{\subseteq} [m]$, $E_I(z) = \sum_{i \in I} (c_i - e_i(z)) \neq 0$ w.p. $\frac{1}{2}$

say false half coord $\forall I$

also quadratic function at z

Prover

- Compute $\pi = [f_z(p)]_{p \in Quad}$

π

Evaluation of all quadratic functions at z

Verifier

- Pick P_I, $I \underset{Rand}{\subseteq} [m]$
- Accept if $\pi(P_I) = 0$

Honest Prover $\Rightarrow$ $\pi = [f_p(z)]_p$

$\Rightarrow$ • **Completeness** $\exists z : E(z) = 0 \Rightarrow$ Accept w.p. 1

• **Soundness** $\forall z : E(z) \neq 0 \Rightarrow$ Accept w.p. $\frac{1}{2}$

What if the prover cheats ?

That is, π is NOT evaluation of

all quadratic functions at z.

PCP - Verifier for QEP

queries = 3 + 9 + 1 = 13
⇒ constant # of queries.

① **Consistency Check** – Test whether π is VALID.

- **Linearity Test**: Pick random $p, q \in Quad$ (3 positions)
  Check if $\pi[p] + \pi[q] = \pi[p+q]$

- **Quadraticity Test**: Pick random $l_1, l_2 \in Linear$
  Check if $\tilde{\pi}(l_1) \cdot \tilde{\pi}(l_2) = \tilde{\pi}(l_1, l_2)$
  where $\tilde{\pi}(a) = \pi[a+b] + \pi[b] \approx f_2(a)$ (Read 3 positions each)
  Self Reproducing Test

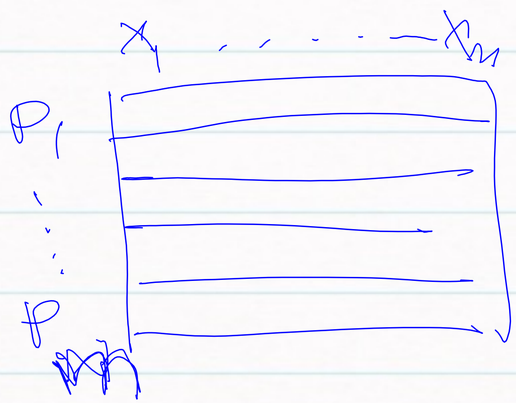
Reject fake π w.p. 0.99

② **Evaluation Test**: Pick random $I \overset{rand}{\subseteq} [m]$
Accept if $\pi[P_I] = 0$ (1 position)

Reject $E(z) \neq 0$ w.p. $\frac{1}{2}$

⇒ Accept false proof w.p. $\frac{1}{2} - \varepsilon$

What is the size of truth table of $f_z(p)$



not $n+m$ bits

$2^{n+m} \approx 2^{N^2}$

N = size of SAT instance

chars

$\Rightarrow$ This protocol gives (1) $c(i)$ queries

(2) Soundness $\frac{1}{2}$

But, size of the proof is expo(n)

* proof of size poly(n) exists