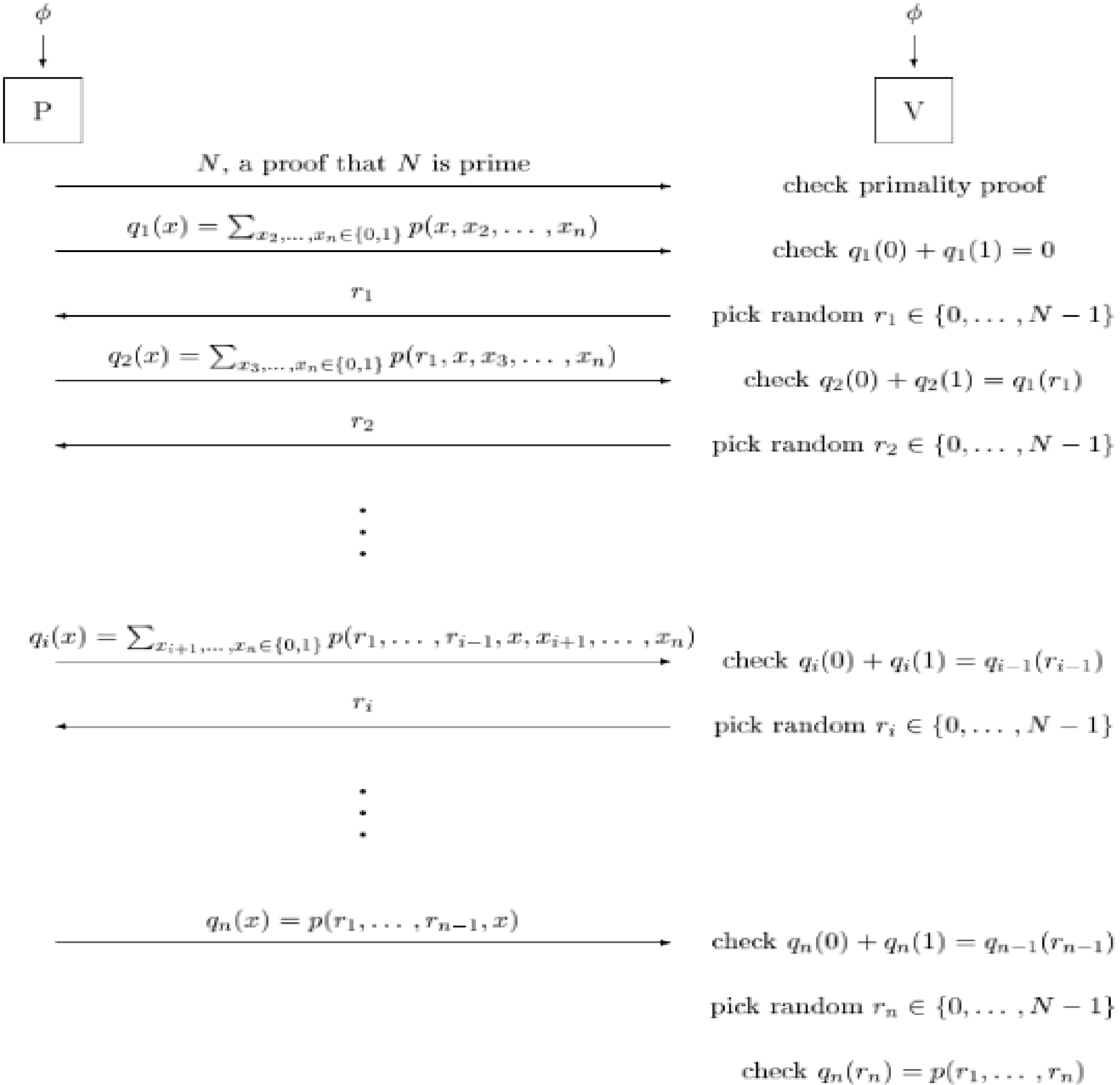
CS 579: Computational Complexity. Lecture 10

IP=PSPACE, Part 2

Alexandra Kolla

Today

- Proof: PSPACE $\subseteq$ IP.
- Discuss MIP, PCP.



ϕ → P

ϕ → V

N, a proof that N is prime → check primality proof

$q_1(x) = \sum_{x_2,\ldots,x_n \in \{0,1\}} p(x, x_2, \ldots, x_n)$ → check $q_1(0) + q_1(1) = 0$

r_1 ← pick random $r_1 \in \{0, \ldots, N-1\}$

$q_2(x) = \sum_{x_3,\ldots,x_n \in \{0,1\}} p(r_1, x, x_3, \ldots, x_n)$ → check $q_2(0) + q_2(1) = q_1(r_1)$

r_2 ← pick random $r_2 \in \{0, \ldots, N-1\}$

$\vdots$

$q_i(x) = \sum_{x_{i+1},\ldots,x_n \in \{0,1\}} p(r_1, \ldots, r_{i-1}, x, x_{i+1}, \ldots, x_n)$ → check $q_i(0) + q_i(1) = q_{i-1}(r_{i-1})$

r_i ← pick random $r_i \in \{0, \ldots, N-1\}$

$\vdots$

$q_n(x) = p(r_1, \ldots, r_{n-1}, x)$ → check $q_n(0) + q_n(1) = q_{n-1}(r_{n-1})$

pick random $r_n \in \{0, \ldots, N-1\}$

check $q_n(r_n) = p(r_1, \ldots, r_n)$

PSPACE - complete language:TQBF

- For 3CNF boolean formula we may think of the satisfiability problem as determining the truth value of the statement:

$$\exists x_1 \exists x_2 \ldots \exists x_n \phi(x_1, x_2, \ldots, x_n)$$

- Can generalize this idea to allow universal quantifiers, e,g. $\forall x_1 \exists x_2 (x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2})$

PSPACE - complete language: TQBF

- Consider the language of all true quantified boolean formulas:

  TQBF={Φ: Φ is a true quantified boolean formula }

- TQBF is PSPACE-complete
- Thus, if we have an interactive proof recognizing TQBF, we have it for all PSPACE.

Arithmetization of TQBF

- We consider that all quantified boolean formulas are given to us as:

  $\Phi = \forall x_1 \exists x_2 \forall x_3 \dots \forall x_n \phi(x_1, x_2, \dots, x_n)$

Where ϕ is 3 CNF formula.

- Similar ideas as #P⊆IP
- First, arithmetize the formula and then the prover convinces verifier that the arithmetized formula evaluates to 1.
- In what follows, random elements are drawn from field Fp, for large enough p

Arithmetization of TQBF

- Formula ϕ with m clauses on variables $x_1, \dots, x_n$.
- p large prime
- Translate ϕ to a polynomial F over the field (mod p) as follows:
- $z_1 \vee z_2 \vee z_3 \rightarrow 1 - (1 - z_1)(1 - z_2)(1 - z_3)$
- F is the product of all the m expressions corresponding to the m clauses.

Arithmetization of TQBF

- Each literal has degree 3, so F has degree at most 3m.
- For a zero-one assignment, F evaluates to zero if this assignment does not satisfy ϕ, and to 1 otherwise.
- Read quantifiers from left to right and consider the expression $\forall x_n \phi(x_1, x_2, \dots, x_n)$
- This expression has n-1 free variables and for each substitution of values to the variables its is either true or false.
- We are looking for a polynomial with the same behavior.

Arithmetization of TQBF

- Write new polynomial

$$\mathrm{G}(\mathrm{x}_1, \dots, \mathrm{x}_{\mathrm{n}-1}) = \mathrm{P}_{\forall x_n} F(x_1, x_2, \dots, x_n)$$
$$= \mathrm{F}(\mathrm{x}_1, \dots, \mathrm{x}_{\mathrm{n}-1}, 1) \cdot F(x_1, \dots, x_{n-1}, 0)$$

- In a similar manner, we want to find a polynomial representation of $\exists x_{n-1} \forall x_n \phi(x_1, x_2, \dots, x_n)$
- Write new polynomial

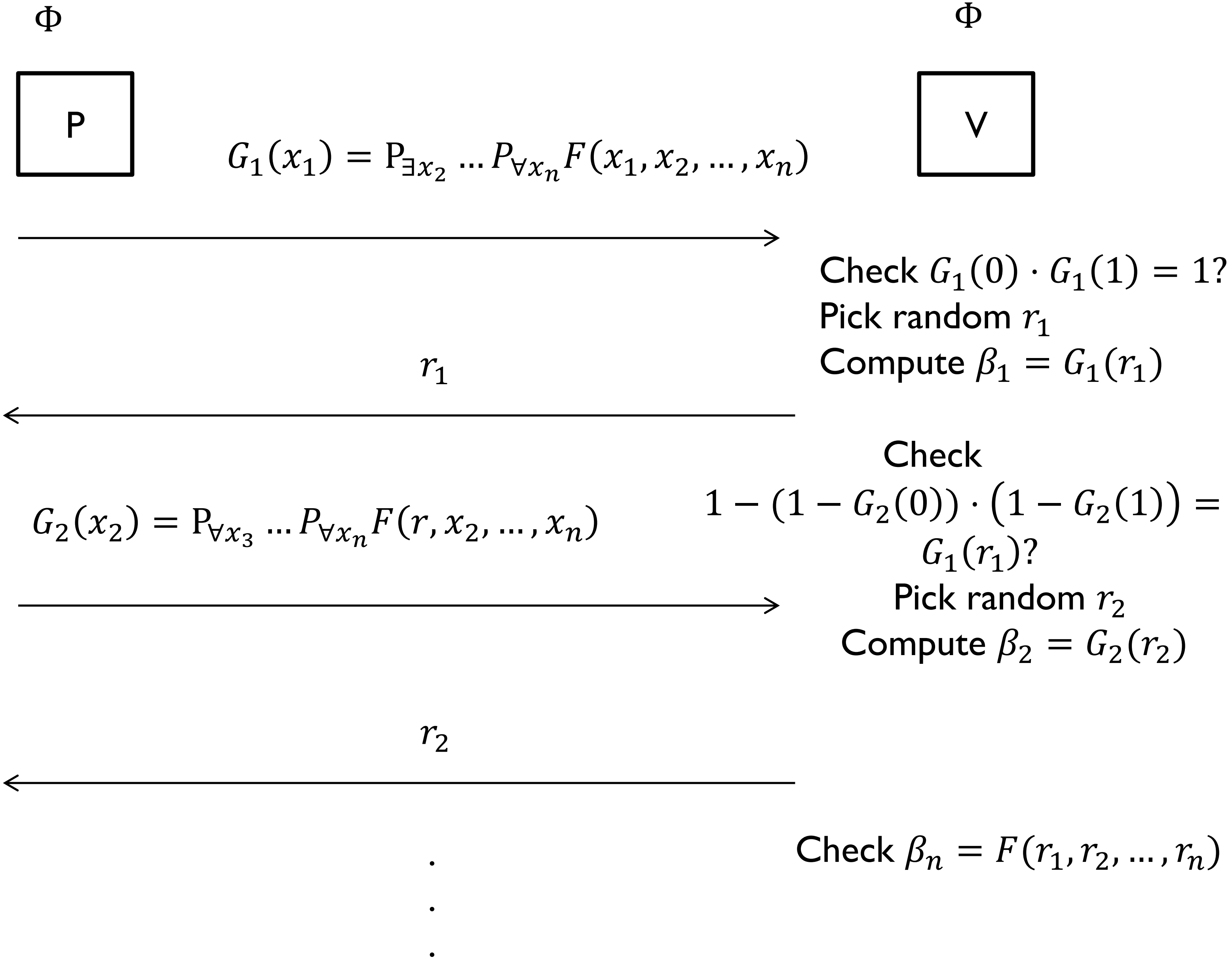
$$\mathrm{P}_{\exists x_{n-1}} G(x_1, x_2, \dots, x_{n-1})$$
$$= 1 - (1 - \mathrm{G}(\mathrm{x}_1, \dots, \mathrm{x}_{\mathrm{n}-2}, 0)) \cdot$$
$$(1 - G(x_1, \dots, x_{n-2}, 1))$$

Arithmetization of TQBF

- Denote the polynomial for $\exists x_{n-1} \forall x_n \phi(x_1, x_2, \dots, x_n)$
  $$\mathrm{P}_{\exists x_{n-1}} P_{\forall x_n} F(x_1, x_2, \dots, x_n)$$
- Turn 3CNF formula ϕ into F as in last lecture.
- Replace $\exists x_i$ with $\mathrm{P}_{\exists x_i}$
- Replace $\forall x_i$ with $\mathrm{P}_{\forall x_i}$
- Final expression always evaluates to 0 or 1. It evaluates to 1 iff the quantified boolean formula Φ is true.

Arithmetization of TQBF

- Final arithmetic expression:
  $\mathrm{P}_{\forall x_1}\mathrm{P}_{\exists x_2} \dots P_{\forall x_n} F(x_1, x_2, \dots, x_n)$
- Let’s try to (naively) mimic the protocol from last lecture.



Φ Φ

P V

$G_1(x_1) = \mathrm{P}_{\exists x_2} \ldots P_{\forall x_n} F(x_1, x_2, \ldots, x_n)$

Check $G_1(0) \cdot G_1(1) = 1?$

Pick random r_1

Compute $\beta_1 = G_1(r_1)$

r_1

Check

$1 - (1 - G_2(0)) \cdot \left(1 - G_2(1)\right) = G_1(r_1)?$

$G_2(x_2) = \mathrm{P}_{\forall x_3} \ldots P_{\forall x_n} F(r, x_2, \ldots, x_n)$

Pick random r_2

Compute $\beta_2 = G_2(r_2)$

r_2

Check $\beta_n = F(r_1, r_2, \ldots, r_n)$

.
.
.

Naïve protocol

- Problem is that the degree of the polynomial in the end can be exponential.
- Prover would have to send exponentially many coefficients but verifier will not be able to read them all.
- Need to ensure that the degree of any variable in any intermediate stage of the transformation never goes above two.

Revised solution

- At every stage of the transformation, we have some polynomial $J(x_1, x_2, \ldots, x_n)$ where some variables might have degree bigger than two.
- We can’t expect to transform it into J’ where the degree of all variables is at most two and they evaluate the same at every point.
- We only need J, J’ to agree on 0-1 assignments.

Revised solution

- Key observation $x^k = x, x = 0 \ \ or\ x = 1$ for all positive integers k.
- J' can be obtained by J by erasing all exponents.
- E.g. $J(x_1, x_2, x_3) = x_1^3 x_2^4 + 5x_1 x_2^3 + x_2^6 x_3^2$

replace by $J'(x_1, x_2, x_3) = 6x_1 x_2 + x_2 x_3$

- Define new operator Rx_i which reduces the exponent of x_i to 1 at all occurances.

Revised solution

- Formally, we have $Rx_iJ(x_1, x_2, \dots, x_n) = x_i \cdot J(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) + (1 - x_i) \cdot J(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$

- $J'(x_1, \dots, x_n) = Rx_1Rx_2 \dots Rx_nJ(x_1, \dots, x_n)$

Revised solution

- We now arithmetize the quantified boolean formula of the form $\Phi = \forall x_1 \exists x_2 \forall x_3 \ldots \forall x_n \phi(x_1, x_2, \ldots, x_n)$

into

- $\mathrm{E} = \mathrm{P}_{\forall x_1} R x_1 P_{\exists x_2} R x_1 R x_2 \ldots P_{\forall x_n} R x_1 \ldots R x_n F(x_1, \ldots, x_n)$