

IP = PSPACE

Shamir's Theorem

Johannes Mittmann

Technische Universität München (TUM)

4th Joint Advanced Student School (JASS)

St. Petersburg, April 2 – 12, 2006

Course 1: Proofs and Computers



1 Introduction

2 Polynomial Space

- Quantified Satisfiability
- PSPACE-Completeness

3 Shamir's Theorem

- Arithmetization
- Reduction to a Finite Field
- Polynomials and Simple Expressions
- The Interactive Protocol

History

- Papadimitriou (1983):
 $\mathbf{IP} \subseteq \mathbf{PSPACE}$.
- Toda (1989): $\mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}}$.
- Nisan (Nov. 27, 1989):
 $\mathbf{PH} \subseteq \mathbf{MIP}$.
- Lund, Fortnow, Karloff, Nisan
(Dec. 13, 1989): $\mathbf{PH} \subseteq \mathbf{IP}$.
- Shamir (Dec. 26, 1989):
 $\mathbf{PSPACE} \subseteq \mathbf{IP}$.



Figure: Adi Shamir

Polynomial Space

$$\mathbf{PSPACE} = \bigcup_{k>0} \mathbf{SPACE}(n^k).$$

$$\mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE}.$$

Quantified Boolean Formulas

Definition

Let $X = \{x_1, x_2, \dots\}$ be an alphabet of *Boolean variables*. They can take the two *truth values* true and false.

A *quantified Boolean expression* (QBF) ϕ is defined inductively by

① a Boolean variable x_i ,

or an expression of the form

② $\neg\phi_1$ (*negation*),

③ $\phi_1 \vee \phi_2$ (*disjunction*),

④ $\phi_1 \wedge \phi_2$ (*conjunction*),

⑤ $\exists x_i \phi_1$ (*existential quantification*),

⑥ $\forall x_i \phi_1$ (*universal quantification*),

where ϕ_1 and ϕ_2 are quantified Boolean expressions.

Proposition

Let ϕ and ψ be QBFs. Then

$$1 \quad \neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi.$$

$$2 \quad \neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi.$$

$$3 \quad \neg(\exists x_i \phi) \equiv \forall x_i \neg\phi.$$

$$4 \quad \neg(\forall x_i \phi) \equiv \exists x_i \neg\phi.$$

$$5 \quad \neg(\neg\phi) \equiv \phi.$$

(De Morgan's Laws)

Proposition

Let ϕ and ψ be QBFs. Then

- 1 $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi.$
- 2 $\neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi.$
- 3 $\neg(\exists x_i \phi) \equiv \forall x_i \neg\phi.$
- 4 $\neg(\forall x_i \phi) \equiv \exists x_i \neg\phi.$
- 5 $\neg(\neg\phi) \equiv \phi.$
- 6 $\exists x_i (\phi \vee \psi) \equiv (\exists x_i \phi) \vee (\exists x_i \psi).$
- 7 $\forall x_i (\phi \wedge \psi) \equiv (\forall x_i \phi) \wedge (\forall x_i \psi).$

(De Morgan's Laws)

Proposition

Let ϕ and ψ be QBFs. Then

① $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi.$

② $\neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi.$

③ $\neg(\exists x_i \phi) \equiv \forall x_i \neg\phi.$

④ $\neg(\forall x_i \phi) \equiv \exists x_i \neg\phi.$

⑤ $\neg(\neg\phi) \equiv \phi.$

⑥ $\exists x_i (\phi \vee \psi) \equiv (\exists x_i \phi) \vee (\exists x_i \psi).$

⑦ $\forall x_i (\phi \wedge \psi) \equiv (\forall x_i \phi) \wedge (\forall x_i \psi).$

⑧ *If x_i does not appear free in ψ ,* $\forall x_i (\phi \vee \psi) \equiv (\forall x_i \phi) \vee \psi.$

⑨ *If x_i does not appear free in ψ ,* $\forall x_i (\phi \wedge \psi) \equiv (\forall x_i \phi) \wedge \psi.$

(De Morgan's Laws)

Proposition

Let ϕ and ψ be QBFs. Then

① $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi.$

(De Morgan's Laws)

② $\neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi.$

③ $\neg(\exists x_i \phi) \equiv \forall x_i \neg\phi.$

④ $\neg(\forall x_i \phi) \equiv \exists x_i \neg\phi.$

⑤ $\neg(\neg\phi) \equiv \phi.$

⑥ $\exists x_i (\phi \vee \psi) \equiv (\exists x_i \phi) \vee (\exists x_i \psi).$

⑦ $\forall x_i (\phi \wedge \psi) \equiv (\forall x_i \phi) \wedge (\forall x_i \psi).$

⑧ If x_i does not appear free in ψ , $\forall x_i (\phi \vee \psi) \equiv (\forall x_i \phi) \vee \psi.$

⑨ If x_i does not appear free in ψ , $\forall x_i (\phi \wedge \psi) \equiv (\forall x_i \phi) \wedge \psi.$

⑩ If x_j does not appear in ϕ , $\forall x_i \phi \equiv \forall x_j \phi[x_i \leftarrow x_j].$

Prenex Normal Form

$$\phi = \exists x_1 \forall x_2 \exists x_3 \dots Q_n x_n \psi, \quad Q_n \in \{\exists, \forall\}.$$

Prenex Normal Form

$$\phi = \exists x_1 \forall x_2 \exists x_3 \dots Q_n x_n \psi, \quad Q_n \in \{\exists, \forall\}.$$

Proposition

Any QBF ϕ can be transformed to an equivalent one in prenex normal form.

Quantified Satisfiability

$\text{QSAT} = \{ \langle \phi \rangle : \phi \text{ is a true QBF in prenex CNF} \}.$

PSPACE-Completeness

Theorem (Stockmeyer/Meyer 1973)

QSAT is **PSPACE**-complete.

PSPACE-Completeness

Theorem (Stockmeyer/Meyer 1973)

QSAT is **PSPACE**-complete.

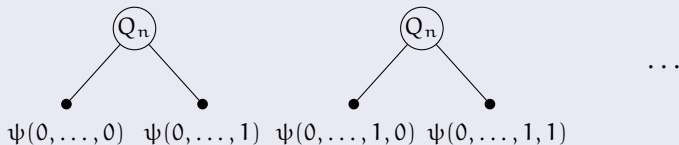
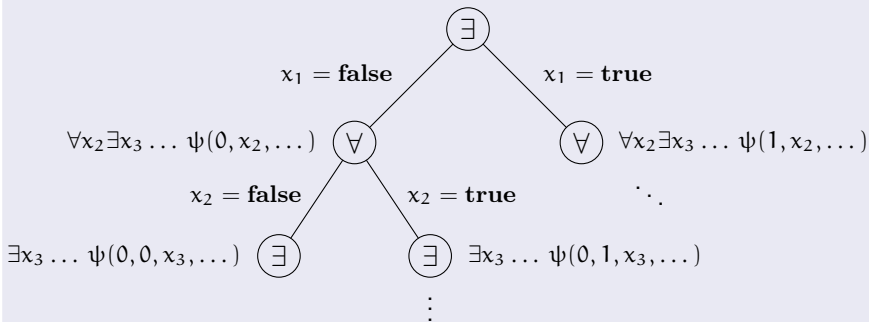
Proof.

It suffices to show:

- 1 QSAT \in **PSPACE**.
- 2 For all $L \in$ **PSPACE** : $L \leq_{\log}$ QSAT.

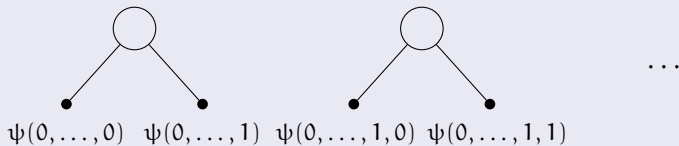
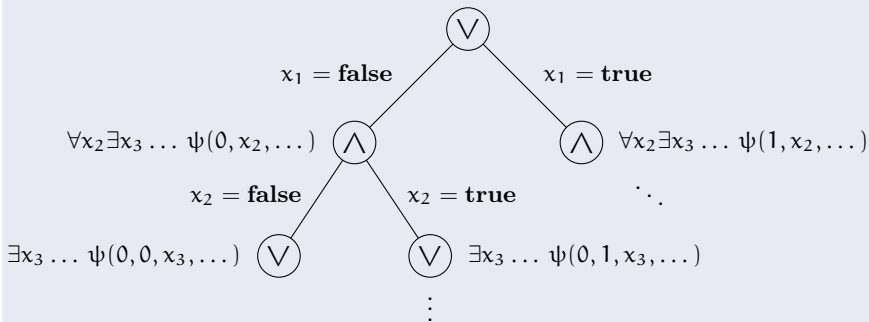
Proof sketch of (1).

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



Proof sketch of (1).

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



Algorithm: Truth(ϕ)

- 1: **if** ϕ is quantifier-free **then**
- 2: **return** truth value of ϕ
- 3: **end if**

- 4: denote $\phi = Q_1x_1 \dots Q_nx_n \psi(x_1, \dots, x_n)$

- 5: $b_0 \leftarrow \text{Truth}(Q_2x_2 \dots Q_nx_n \psi(\mathbf{false}, x_2, \dots, x_n))$
- 6: $b_1 \leftarrow \text{Truth}(Q_2x_2 \dots Q_nx_n \psi(\mathbf{true}, x_2, \dots, x_n))$

- 7: **if** $Q_1 = \exists$ **then**
- 8: **return** $b_0 \vee b_1$
- 9: **else**
- 10: **return** $b_0 \wedge b_1$
- 11: **end if**

Proof sketch of (2).

- Let $L \in \mathbf{PSPACE}$.

Proof sketch of (2).

- Let $L \in \mathbf{PSPACE}$.
- L is decidable by a Turing machine M .

Proof sketch of (2).

- Let $L \in \mathbf{PSPACE}$.
- L is decidable by a Turing machine M .
- For input x consider the configuration graph of M .

Proof sketch of (2).

- Let $L \in \mathbf{PSPACE}$.
- L is decidable by a Turing machine M .
- For input x consider the configuration graph of M .
- 2^m configurations, where $m = \mathcal{O}(n^k)$.

Proof sketch of (2).

- Let $L \in \mathbf{PSPACE}$.
- L is decidable by a Turing machine M .
- For input x consider the configuration graph of M .
- 2^m configurations, where $m = \mathcal{O}(n^k)$.
- Reachability method:

$\psi_i(X, Y)$ is true \iff configuration Y can be reached from
configuration X in $\leq 2^i$ steps,

for $i = 0, \dots, m$.

Proof sketch of (2).

- Let $L \in \mathbf{PSPACE}$.
- L is decidable by a Turing machine M .
- For input x consider the configuration graph of M .
- 2^m configurations, where $m = \mathcal{O}(n^k)$.
- Reachability method:

$\psi_i(X, Y)$ is true \iff configuration Y can be reached from configuration X in $\leq 2^i$ steps,

for $i = 0, \dots, m$.

- Required QBF: $\psi_m(A, B)$.

Proof sketch of (2).

- $\psi_0(A, B)$ can be written in DNF.

Proof sketch of (2).

- $\psi_0(A, B)$ can be written in DNF.
- Bad idea:

$$\psi_{i+1} = \exists Z [\psi_i(A, Z) \wedge \psi_i(Z, B)].$$

Proof sketch of (2).

- $\psi_0(A, B)$ can be written in DNF.
- Bad idea:

$$\psi_{i+1} = \exists Z [\psi_i(A, Z) \wedge \psi_i(Z, B)].$$

- Savitch's trick:

$$\psi_{i+1} = \exists Z \forall X \forall Y [((X = A \wedge Y = Z) \vee (X = Z \wedge Y = B)) \Rightarrow \psi_i(X, Y)].$$

Proof sketch of (2).

- $\psi_0(A, B)$ can be written in DNF.
- Bad idea:

$$\psi_{i+1} = \exists Z [\psi_i(A, Z) \wedge \psi_i(Z, B)].$$

- Savitch's trick:

$$\psi_{i+1} = \exists Z \forall X \forall Y [((X = A \wedge Y = Z) \vee (X = Z \wedge Y = B)) \Rightarrow \psi_i(X, Y)].$$

- Convert to prenex DNF.

Proof sketch of (2).

- $\psi_0(A, B)$ can be written in DNF.
- Bad idea:

$$\psi_{i+1} = \exists Z [\psi_i(A, Z) \wedge \psi_i(Z, B)].$$

- Savitch's trick:

$$\psi_{i+1} = \exists Z \forall X \forall Y [((X = A \wedge Y = Z) \vee (X = Z \wedge Y = B)) \Rightarrow \psi_i(X, Y)].$$

- Convert to prenex DNF.
- $L \leq_{\log} \overline{\text{QSAT}}$.

Proof sketch of (2).

- $\psi_0(A, B)$ can be written in DNF.
- Bad idea:

$$\psi_{i+1} = \exists Z [\psi_i(A, Z) \wedge \psi_i(Z, B)].$$

- Savitch's trick:

$$\psi_{i+1} = \exists Z \forall X \forall Y [((X = A \wedge Y = Z) \vee (X = Z \wedge Y = B)) \Rightarrow \psi_i(X, Y)].$$

- Convert to prenex DNF.
- $L \leq_{\log} \overline{\text{QSAT}}$.
- **PSPACE = coPSPACE.**



Shamir's Theorem

Theorem (Shamir 1992)

$$\mathbf{IP = PSPACE.}$$

Shamir's Theorem

Theorem (Shamir 1992)

$$\mathbf{IP = PSPACE.}$$

Proof.

\subseteq : Optimal prover strategy:

- Traverse the tree of all possible interactions between Alice and Bob.
- Compute the probabilities of acceptance.

Proof Outline

Proof.

\supseteq : It suffices to show

$$\text{QSAT} \in \text{IP},$$

since

- **IP** is closed under reductions, and
- $\text{QSAT} \in \text{PSPACE}$ -complete.

Proof Outline

Proof.

\supseteq : It suffices to show

$$\text{QSAT} \in \text{IP},$$

since

- **IP** is closed under reductions, and
- $\text{QSAT} \in \text{PSPACE}$ -complete.

Outline:

- Arithmetization: $\phi \mapsto A_\phi$.
- Reduction to \mathbb{F}_p .
- Polynomials and simple expressions.
- Interactive protocol that decides QSAT.

Arithmetization

Quantified Boolean expression $\phi \mapsto$ Arithmetization A_ϕ

Conversion rules:

QBF ϕ	Arithmetization A_ϕ
true	1
false	0
$x_i \in X$	$z_i \in \mathbb{Z}$
$\neg x_i$	$1 - z_i$
$\psi_1 \vee \psi_2$	$A_{\psi_1} + A_{\psi_2}$
$\psi_1 \wedge \psi_2$	$A_{\psi_1} \cdot A_{\psi_2}$
$\exists x_i \psi$	$\sum_{z_i=0}^1 A_\psi$
$\forall x_i \psi$	$\prod_{z_i=0}^1 A_\psi$

Example

$$\phi = \forall x_1 [\neg x_1 \vee \exists x_2 \forall x_3 (x_1 \wedge x_2) \vee x_3].$$

$$A_\phi = \prod_{z_1=0}^1 \left[(1 - z_1) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (z_1 \cdot z_2 + z_3) \right].$$

A_ϕ is called Σ - Π *expression*.

Lemma

Let ϕ be a closed QBF with negation only over variables. Then

$$\phi \text{ is true} \iff A_\phi > 0.$$

Lemma

Let ϕ be a closed QBF with negation only over variables. Then

$$\phi \text{ is true} \iff A_\phi > 0.$$

Proof.

Induction on the structure of a (not necessarily closed) QBF ϕ .

- $\phi = x_i$:

$$\begin{aligned} \phi \text{ is true} &\iff x_i = \text{true} \\ &\iff A_\phi = z_i = 1 > 0. \end{aligned}$$

Proof (continued).

- $\phi = \neg x_i$:

$$\phi \text{ is true} \iff x_i = \text{false}$$

$$\iff A_\phi = 1 - z_i = 1 - 0 > 0.$$

Proof (continued).

- $\phi = \neg x_i$:

$$\phi \text{ is true} \iff x_i = \text{false}$$

$$\iff A_\phi = 1 - z_i = 1 - 0 > 0.$$

- $\phi = \psi_1 \vee \psi_2$:

$$\phi \text{ is true} \iff \psi_1 \text{ is true} \quad \text{or} \quad \psi_2 \text{ is true}$$

$$\iff A_{\psi_1} > 0 \quad \text{or} \quad A_{\psi_2} > 0$$

$$\iff A_\phi = A_{\psi_1} + A_{\psi_2} > 0.$$

- ...



Problem: Exponential Arithmetizations

Example

$$\phi = \forall x_1 \forall x_2 \cdots \forall x_{k-1} \exists x_k (x_k \vee \neg x_k).$$

$$A_\phi = \prod_{z_1=0}^1 \prod_{z_2=0}^1 \cdots \prod_{z_{k-1}=0}^1 \sum_{z_k=0}^1 [z_k + (1 - z_k)] = 2^{2^{k-1}}.$$

Problem: Exponential Arithmetizations

Example

$$\phi = \forall x_1 \forall x_2 \cdots \forall x_{k-1} \exists x_k (x_k \vee \neg x_k).$$

$$A_\phi = \prod_{z_1=0}^1 \prod_{z_2=0}^1 \cdots \prod_{z_{k-1}=0}^1 \sum_{z_k=0}^1 [z_k + (1 - z_k)] = 2^{2^{k-1}}.$$

↪ exponentially many bits needed!

Problem: Exponential Arithmetizations

Example

$$\phi = \forall x_1 \forall x_2 \cdots \forall x_{k-1} \exists x_k (x_k \vee \neg x_k).$$

$$A_\phi = \prod_{z_1=0}^1 \prod_{z_2=0}^1 \cdots \prod_{z_{k-1}=0}^1 \sum_{z_k=0}^1 [z_k + (1 - z_k)] = 2^{2^{k-1}}.$$

↪ exponentially many bits needed!

Idea: reduction to a finite field.

Lemma

Let A_ϕ be a Σ - Π expression of length n . Then

$$A_\phi \leq 2^{2^n}.$$

Lemma

Let A_ϕ be a Σ - Π expression of length n . Then

$$A_\phi \leq 2^{2^n}.$$

Proof.

Induction on the structure of ϕ .

- $\phi = (\neg)x_i$:

$$A_\phi \leq 1 \leq 2^{2^1}.$$

Lemma

Let A_ϕ be a Σ - Π expression of length n . Then

$$A_\phi \leq 2^{2^n}.$$

Proof.

Induction on the structure of ϕ .

- $\phi = (\neg)x_i$:

$$A_\phi \leq 1 \leq 2^{2^1}.$$

- $\phi = \psi_1 \circ \psi_2$, $\circ \in \{\vee, \wedge\}$:

$$A_\phi \leq 2^{2^\ell} \cdot 2^{2^m} = 2^{2^\ell + 2^m} \leq 2^{2^n} \quad (\ell + m \leq n).$$

Lemma

Let A_ϕ be a Σ - Π expression of length n . Then

$$A_\phi \leq 2^{2^n}.$$

Proof.

Induction on the structure of ϕ .

- $\phi = (\neg)x_i$:

$$A_\phi \leq 1 \leq 2^{2^1}.$$

- $\phi = \psi_1 \circ \psi_2, \quad \circ \in \{\vee, \wedge\}$:

$$A_\phi \leq 2^{2^\ell} \cdot 2^{2^m} = 2^{2^\ell + 2^m} \leq 2^{2^n} \quad (\ell + m \leq n).$$

- $\phi = Qx_i \psi, \quad Q \in \{\exists, \forall\}$:

$$A_\phi \leq 2^{2^m} \cdot 2^{2^m} = 2^{2 \cdot 2^m} = 2^{2^{m+1}} \leq 2^{2^n} \quad (m < n). \quad \square$$

Number of Primes

Lemma

For $n \geq 3$,

$$\sqrt{n} \leq \pi(n) \leq n.$$

Number of Primes

Lemma

For $n \geq 3$,

$$\sqrt{n} \leq \pi(n) \leq n.$$

Proof.

$$\pi(n) \geq n \prod_{p \leq \sqrt{n}} \frac{p-1}{p} \geq n \prod_{i=2}^{\lfloor \sqrt{n} \rfloor} \frac{i-1}{i} = n / \lfloor \sqrt{n} \rfloor \geq \sqrt{n}. \quad \square$$

The Chinese Remainder Theorem

Theorem (Sun Tzu)

Let $a_1, \dots, a_k \in \mathbb{Z}$, and let $p_1, \dots, p_k \in \mathbb{N}_{>0}$ be pairwise coprime.

Then the system of simultaneous congruences

$$x = a_1 \pmod{p_1}$$

$$\vdots$$

$$x = a_k \pmod{p_k}$$

has a unique solution x modulo $\prod_{i=1}^k p_i$.

Reduction to \mathbb{F}_p

Proposition

For every Σ - Π expression $A \neq 0$ of length n , there exists a prime $p \in [2^n, 2^{3n}]$ such that

$$A \neq 0 \pmod{p}.$$

Proof.

- Denote by p_1, \dots, p_k all primes in $[2^n, 2^{3n}]$.

Proof.

- Denote by p_1, \dots, p_k all primes in $[2^n, 2^{3n}]$.
- $k = \pi(2^{3n}) - \pi(2^n) \geq \sqrt{2^{3n}} - 2^n > 2^n$.

Proof.

- Denote by p_1, \dots, p_k all primes in $[2^n, 2^{3n}]$.
- $k = \pi(2^{3n}) - \pi(2^n) \geq \sqrt{2^{3n}} - 2^n > 2^n$.
- Suppose

$$A = 0 \pmod{p_i} \quad \forall i.$$

Proof.

- Denote by p_1, \dots, p_k all primes in $[2^n, 2^{3n}]$.
- $k = \pi(2^{3n}) - \pi(2^n) \geq \sqrt{2^{3n}} - 2^n > 2^n$.
- Suppose

$$A = 0 \pmod{p_i} \quad \forall i.$$

- Chinese Remainder Theorem:

$$A = 0 \pmod{\prod_{i=1}^k p_i} > 2^{2^n}.$$

Proof.

- Denote by p_1, \dots, p_k all primes in $[2^n, 2^{3n}]$.
- $k = \pi(2^{3n}) - \pi(2^n) \geq \sqrt{2^{3n}} - 2^n > 2^n$.
- Suppose

$$A = 0 \pmod{p_i} \quad \forall i.$$

- Chinese Remainder Theorem:

$$A = 0 \pmod{\prod_{i=1}^k p_i} > 2^{2^n}.$$

- $A \leq 2^{2^n} \implies A = 0$, contradiction. □

Functional and Randomized Form

Definition

Let A be a Σ - Π expression.

The *functional form* A' is defined by eliminating the leftmost $\sum_{z_i=0}^1$ or $\prod_{z_i=0}^1$ symbol in A , and can be considered as a polynomial

$$q(z_i) \in \mathbb{Z}[z_i].$$

The *randomized form* of A is

$$A'(z_i = r),$$

where $r \in_{\mathbb{R}} \mathbb{F}_p$ is a random number supplied by the verifier.

Problem: Exponentially High Degree

Example

$$\phi = \forall x_1 \forall x_2 \dots \forall x_k (x_1 \vee x_2 \vee \dots \vee x_k).$$

$$A_\phi = \prod_{z_1=0}^1 \prod_{z_2=0}^1 \dots \prod_{z_k=0}^1 (z_1 + z_2 + \dots + z_k).$$

$$\implies \deg q(z_1) = 2^{k-1}.$$

Problem: Exponentially High Degree

Example

$$\phi = \forall x_1 \forall x_2 \dots \forall x_k (x_1 \vee x_2 \vee \dots \vee x_k).$$

$$A_\phi = \prod_{z_1=0}^1 \prod_{z_2=0}^1 \dots \prod_{z_k=0}^1 (z_1 + z_2 + \dots + z_k).$$

$$\implies \deg q(z_1) = 2^{k-1}.$$

\rightsquigarrow dense polynomial of exponentially high degree!

Problem: Exponentially High Degree

Example

$$\phi = \forall x_1 \forall x_2 \dots \forall x_k (x_1 \vee x_2 \vee \dots \vee x_k).$$

$$A_\phi = \prod_{z_1=0}^1 \prod_{z_2=0}^1 \dots \prod_{z_k=0}^1 (z_1 + z_2 + \dots + z_k).$$

$$\implies \deg q(z_1) = 2^{k-1}.$$

\rightsquigarrow dense polynomial of exponentially high degree!

Idea: elimination of universal quantifiers.

Simple Expressions

Definition

A QBF ϕ is called *simple*, if any occurrence of a variable is separated by at most one universal quantifier from its point of quantification.

Simple Expressions

Definition

A QBF ϕ is called *simple*, if any occurrence of a variable is separated by at most one universal quantifier from its point of quantification.

Example

$\phi = \forall x_1 \forall x_2 \exists x_3 [(x_1 \vee x_2) \wedge \forall x_4 (x_2 \vee x_3 \vee x_4)]$ is simple.

$\psi = \forall x_1 \forall x_2 [(x_1 \vee x_2) \wedge \forall x_3 (\neg x_1 \vee x_3)]$ is not simple.

Lemma

Let ϕ be a simple QBF of length n , and let $q(z_i)$ be the polynomial of the functional form of Λ_ϕ . Then

$$\deg q(z_i) \leq 2n.$$

Lemma

Let ϕ be a simple QBF of length n , and let $q(z_i)$ be the polynomial of the functional form of Λ_ϕ . Then

$$\deg q(z_i) \leq 2n.$$

Proof.

- The degree of quantifier-free subexpressions in z_i is bounded its size.

Lemma

Let ϕ be a simple QBF of length n , and let $q(z_i)$ be the polynomial of the functional form of Λ_ϕ . Then

$$\deg q(z_i) \leq 2n.$$

Proof.

- The degree of quantifier-free subexpressions in z_i is bounded its size.
- Summations cannot change the degree.

Lemma

Let ϕ be a simple QBF of length n , and let $q(z_i)$ be the polynomial of the functional form of Λ_ϕ . Then

$$\deg q(z_i) \leq 2n.$$

Proof.

- The degree of quantifier-free subexpressions in z_i is bounded its size.
- Summations cannot change the degree.
- Products can at most double the degree.

Lemma

Let ϕ be a simple QBF of length n , and let $q(z_i)$ be the polynomial of the functional form of Λ_ϕ . Then

$$\deg q(z_i) \leq 2n.$$

Proof.

- The degree of quantifier-free subexpressions in z_i is bounded its size.
- Summations cannot change the degree.
- Products can at most double the degree.
- In simple expressions this can happen at most once. □

Lemma

Any QBF ϕ can be transformed in logarithmic space to an equivalent simple expression.

Lemma

Any QBF ϕ can be transformed in logarithmic space to an equivalent simple expression.

Proof.

- Consider $\phi = \dots Qx_i \dots \forall x_j \psi(x_i)$, $Q \in \{\exists, \forall\}$.

Lemma

Any QBF ϕ can be transformed in logarithmic space to an equivalent simple expression.

Proof.

- Consider $\phi = \dots Qx_i \dots \forall x_j \psi(x_i)$, $Q \in \{\exists, \forall\}$.
- Transformation:

$$\begin{aligned}\phi' &= \dots Qx_i \dots \forall x_j \exists x_{i'} (x_i \Leftrightarrow x_{i'}) \wedge \psi(x_{i'}) \\ &= \dots Qx_i \dots \forall x_j \exists x_{i'} [(x_i \wedge x_{i'}) \vee (\neg x_i \wedge \neg x_{i'})] \wedge \psi(x_{i'}).\end{aligned}$$

Lemma

Any QBF ϕ can be transformed in logarithmic space to an equivalent simple expression.

Proof.

- Consider $\phi = \dots Qx_i \dots \forall x_j \psi(x_i)$, $Q \in \{\exists, \forall\}$.
- Transformation:

$$\begin{aligned} \phi' &= \dots Qx_i \dots \forall x_j \exists x_{i'} (x_i \Leftrightarrow x_{i'}) \wedge \psi(x_{i'}) \\ &= \dots Qx_i \dots \forall x_j \exists x_{i'} [(x_i \wedge x_{i'}) \vee (\neg x_i \wedge \neg x_{i'})] \wedge \psi(x_{i'}). \end{aligned}$$

- $\mathcal{O}(n^2)$ steps. □

Protocol Setup

Prover

Verifier

Choose $p \in [2^n, 2^{3n}]$.

Compute $a \leftarrow A_\phi \pmod{p}$.

$\xrightarrow{p, a}$

Verify $a \neq 0$,

$p \in [2^n, 2^{3n}]$, and

$p \in \text{PRIMES}$.

Split Step

$$A = A_1 + A_2 \quad \text{or} \quad A = A_1 \cdot A_2,$$

where A_2 starts with the leftmost $\sum_{z_i=0}^1$ or $\prod_{z_i=0}^1$ symbol:

$$A_2 = \sum_{z_i=0}^1 \dots \quad \text{or} \quad A_2 = \prod_{z_i=0}^1 \dots$$

Simplification Step

Prover

Verifier

Compute $q(z_i)$ of A' . $\xrightarrow{q(z_i)}$

Verify

$$a = q(0) + q(1) \pmod{p}, \text{ or}$$

$$a = q(0) \cdot q(1) \pmod{p}.$$
 \xleftarrow{r} Choose $r \in_{\mathcal{R}} \mathbb{F}_p$.
$$A \leftarrow A'(z_i = r) \pmod{p}.$$

$$a \leftarrow q(r) \pmod{p}.$$

Example (Round 1)

$$A \leftarrow A_\phi = \prod_{z_1=0}^1 \left[(1 - z_1) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (z_1 \cdot z_2 + z_3) \right],$$

$a \leftarrow 2.$

Example (Round 1)

$$A \leftarrow A_\phi = \prod_{z_1=0}^1 \left[(1 - z_1) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (z_1 \cdot z_2 + z_3) \right],$$

$$a \leftarrow 2.$$

$$A' = (1 - z_1) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (z_1 \cdot z_2 + z_3),$$

$$q(z_1) = z_1^2 + 1.$$

Example (Round 1)

$$A \leftarrow A_\phi = \prod_{z_1=0}^1 \left[(1 - z_1) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (z_1 \cdot z_2 + z_3) \right],$$

$$a \leftarrow 2.$$

$$A' = (1 - z_1) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (z_1 \cdot z_2 + z_3),$$

$$q(z_1) = z_1^2 + 1.$$

Verify $a = 2 = 2 \cdot 1 = q(0) \cdot q(1)$.

Example (Round 1)

$$A \leftarrow A_\phi = \prod_{z_1=0}^1 \left[(1 - z_1) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (z_1 \cdot z_2 + z_3) \right],$$

$$a \leftarrow 2.$$

$$A' = (1 - z_1) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (z_1 \cdot z_2 + z_3),$$

$$q(z_1) = z_1^2 + 1.$$

Verify $a = 2 = 2 \cdot 1 = q(0) \cdot q(1)$.

$$A \leftarrow A'(z_1 = 3) = (1 - 3) + \sum_{z_2=0}^1 \prod_{z_3=0}^1 (3z_2 + z_3),$$

$$a \leftarrow q(3) = 10.$$

Example (Round 2)

$$A \leftarrow A_2 = \sum_{z_2=0}^1 \prod_{z_3=0}^1 (3z_2 + z_3),$$

$$a \leftarrow a - a_1 = 10 - (-2) = 12.$$

Example (Round 2)

$$A \leftarrow A_2 = \sum_{z_2=0}^1 \prod_{z_3=0}^1 (3z_2 + z_3),$$

$$a \leftarrow a - a_1 = 10 - (-2) = 12.$$

$$A' = \prod_{z_3=0}^1 (3 \cdot z_2 + z_3),$$

$$q(z_2) = 9z_2^2 + 3z_2.$$

Example (Round 2)

$$A \leftarrow A_2 = \sum_{z_2=0}^1 \prod_{z_3=0}^1 (3z_2 + z_3),$$

$$a \leftarrow a - a_1 = 10 - (-2) = 12.$$

$$A' = \prod_{z_3=0}^1 (3 \cdot z_2 + z_3),$$

$$q(z_2) = 9z_2^2 + 3z_2.$$

Verify $a = 12 = 0 + 12 = q(0) + q(1)$.

Example (Round 2)

$$A \leftarrow A_2 = \sum_{z_2=0}^1 \prod_{z_3=0}^1 (3z_2 + z_3),$$

$$a \leftarrow a - a_1 = 10 - (-2) = 12.$$

$$A' = \prod_{z_3=0}^1 (3 \cdot z_2 + z_3),$$

$$q(z_2) = 9z_2^2 + 3z_2.$$

Verify $a = 12 = 0 + 12 = q(0) + q(1)$.

$$A \leftarrow A'(z_2 = 2) = \prod_{z_3=0}^1 (z_3 + 6),$$

$$a \leftarrow q(2) = 9 \cdot 4 + 3 \cdot 2 = 42.$$

Example (Round 3)

$$A \leftarrow \prod_{z_3=0}^1 (z_3 + 6),$$

$$a \leftarrow 42.$$

Example (Round 3)

$$A \leftarrow \prod_{z_3=0}^1 (z_3 + 6),$$

$$a \leftarrow 42.$$

$$A' = z_3 + 6,$$

$$q(z_3) = z_3 + 6.$$

Example (Round 3)

$$A \leftarrow \prod_{z_3=0}^1 (z_3 + 6),$$

$$a \leftarrow 42.$$

$$A' = z_3 + 6,$$

$$q(z_3) = z_3 + 6.$$

Verify $a = 42 = 6 \cdot 7 = q(0) \cdot q(1)$.

Example (Round 3)

$$A \leftarrow \prod_{z_3=0}^1 (z_3 + 6),$$

$$a \leftarrow 42.$$

$$A' = z_3 + 6,$$

$$q(z_3) = z_3 + 6.$$

Verify $a = 42 = 6 \cdot 7 = q(0) \cdot q(1)$.

$$A \leftarrow A'(z_3 = 5) = 5 + 6 = 11,$$

$$a \leftarrow q(5) = 5 + 6 = 11.$$

Example (Round 3)

$$A \leftarrow \prod_{z_3=0}^1 (z_3 + 6),$$

$$a \leftarrow 42.$$

$$A' = z_3 + 6,$$

$$q(z_3) = z_3 + 6.$$

Verify $a = 42 = 6 \cdot 7 = q(0) \cdot q(1)$.

$$A \leftarrow A'(z_3 = 5) = 5 + 6 = 11,$$

$$a \leftarrow q(5) = 5 + 6 = 11.$$

Verify $A = 11 = a$, and accept.



Correctness of the Interactive Proof

Theorem

- 1 *When ϕ is true and Alice is honest, Bob will always accept the proof.*
- 2 *When ϕ is false, Bob accepts the proof with negligible probability.*

Correctness of the Interactive Proof

Theorem

- 1 *When ϕ is true and Alice is honest, Bob will always accept the proof.*
- 2 *When ϕ is false, Bob accepts the proof with negligible probability.*

Proof of completeness.

- Alice is able to provide all the polynomials.
- Bob will always accept.

Proof of soundness.

- Suppose $A_\phi = 0$ and still Alice claims an $\alpha' \neq 0$.

Proof of soundness.

- Suppose $A_\phi = 0$ and still Alice claims an $\alpha' \neq 0$.
- Alice must supply a wrong polynomial $q'(z_i)$ in the i -th round.

Proof of soundness.

- Suppose $A_\phi = 0$ and still Alice claims an $a' \neq 0$.
- Alice must supply a wrong polynomial $q'(z_i)$ in the i -th round.
- $0 \neq q(z_i) - q'(z_i)$ has at most $2n$ roots.

Proof of soundness.

- Suppose $A_\phi = 0$ and still Alice claims an $a' \neq 0$.
- Alice must supply a wrong polynomial $q'(z_i)$ in the i -th round.
- $0 \neq q(z_i) - q'(z_i)$ has at most $2n$ roots.
- Probability of a false positive:

$$\Pr[\text{error in the } i\text{-th round}] \leq \frac{2n}{p} \leq \frac{2n}{2^n}.$$

Proof of soundness.

- Suppose $A_\phi = 0$ and still Alice claims an $\alpha' \neq 0$.
- Alice must supply a wrong polynomial $q'(z_i)$ in the i -th round.
- $0 \neq q(z_i) - q'(z_i)$ has at most $2n$ roots.
- Probability of a false positive:

$$\Pr[\text{error in the } i\text{-th round}] \leq \frac{2n}{p} \leq \frac{2n}{2^n}.$$

- After $m \leq n$ rounds:

$$\begin{aligned} \Pr[\text{error}] &= 1 - \prod_{i=1}^m \Pr[\text{no error in the } i\text{-th round}] \\ &\leq 1 - \left(1 - \frac{2n}{2^n}\right)^n. \end{aligned}$$



For further reading:



L. J. Stockmeyer and A. R. Meyer:

Word problems requiring exponential time.

Proc. 5th ACM Symp. on the Theory of Computing, pp. 1-9, 1973.



L. Babai:

E-mail and the unexpected power of interaction.

Structure in Complexity Theory Conf., pp. 30-44, 1990.



Adi Shamir:

$IP=PSPACE$.

Journal of the ACM, 39 (4), pp. 869-877, 1992.



Christos H. Papadimitriou:

Computational Complexity.

Addison Wesley, Reading, 1994.

Exercise

Exercise

Show that

$$\#P \subseteq IP.$$

Hint. Arithmetization of the $\#P$ -complete counting problem $\#SAT$.

Solution

Arithmetization:

3-CNF ϕ	Arithmetization A_ϕ
$x_i \in X$	$z_i \in \mathbb{Z}$
$\neg\psi$	$1 - A_\psi$
$\psi_1 \vee \psi_2$	$1 - (1 - A_{\psi_1})(1 - A_{\psi_2})$
$\psi_1 \wedge \psi_2$	$A_{\psi_1} \cdot A_{\psi_2}$

Then $\phi(x_1, \dots, x_n)$ has exactly K satisfying assignments, iff

$$K = \sum_{z_1=0}^1 \cdots \sum_{z_n=0}^1 A_\phi(z_1, \dots, z_n).$$