Chapter 2
Interactive Proofs

Angsheng Li

Institute of Software
Chinese Academy of Sciences

Advanced Algorithms, U CAS
7th, March, 2016

Outline

1. Backgrounds
2. Probabilistic test
3. Interactive proof systems
4. Probabilistic tools
5. Public coins
6. IP=PSPACE

A mathematical proof

A prover P claims he has a proof π for a theorem T, the proof may be correct and may not be correct. To accept and publish the proof, verification from a verifier V is necessary.
In the procedure, we require that

- Verification for a verifier V is easy, no matter the proof π is easy or hard
- If the proof π is indeed a proof of Theorem T, V must accept the proof
- If the proof π is an incorrect proof, V rejects the proof π.

The procedure above is similar to the definition of an NP language.

Program checker

It is a program verification on the basis of input-by-input form.
Let T be a computation task. A *checker* for T is a probabilistic Turing machine M such that, for a program P claimed for T and input x,
Completeness If P is indeed a correct program for T, then the probability that M^P accepts $P(x)$ is at least $\frac{2}{3}$, and
Soundness If $P(x) \neq T(x)$, then the probability that M^P accepts $P(x)$ is less than $\frac{1}{3}$,
where M^P is the computation of M relative to P.
Remark Is this oracle Turing machine?

NP

Given a SAT instance ϕ,
If ϕ is satisfiable, then there if a certificate σ for the satisfaction of ϕ.
If ϕ is unsatisfiable, then any possible certificate σ is not a proof of the satisfaction of ϕ.
NP: Hard to compute, but easy to verify
NP: the class of languages that are verifiable in poly time, or even log space.

Interaction of deterministic functions

Let $f, g : \{0,1\} \rightarrow \{0,1\}$ be functions and $k \geq 0$. A k-round interaction of f and g on input $x \in \{0,1\}$, written

$$\langle f, g\rangle(x)$$

is defined as follows:

$$a_1 = f(x), \;\; a_2 = g(x, a_1)$$

$$a_{2i+1} = f(x, a_1, \cdots, a_{2i}), \quad a_{2i+2} = g(x, a_1, \cdots, a_{2i+1})$$

The output of f is:

$$\mathrm{Out}_f\langle f, g\rangle(x) = f(x, a_1. \cdots, a_k) \in \{0,1\}.$$

Deterministic proof system

We say that a language L has a k-round deterministic interactive proof system if there is a deterministic TM V that on input $x, a_1, \cdots, a_i$, runs in time poly in $n = |x|$, and can have a k-round interaction with ang function P such that

Completeness

$$x \in L \Rightarrow \exists P, \;\; \mathrm{Out}_V \langle V, P \rangle (x) = 1$$

Soundness

$$x \notin L \Rightarrow \forall P, \;\; \mathrm{Out}_V \langle V, P \rangle (x) = 0.$$

dIP: $k(n)$ - a poly of n.

dIP=NP

Completeness:
The verifier V asks for a *honest* prover P for the correct choices of the NP Turing machine.

Soundness:
For any answers of a prover, the verifier V cannot be convinced to accept a negative instance.

Probabilistic verifier

We allow the verifiers to be probabilistic Turing machines.
V flips coins.
Two ways to make a cup of tea: 1) put tea first, then add hot water, 2) put water first, then add tea
Alice claims: For a cup of tea, he knows the difference of the two ways of making a cup of tea. Bob doesn't believe.
How can Alice convince Bob his ability.
Bob prepares 10 cups of teas by the two ways, and remember the ways of all the teas. Ask Alice to test the ways of the preparation for each cup of the teas.
If Alice is correct for all the test, Bob is highly likely to be convinced, in which case, Bob does not know how can Alice test the teas. In this case, with high probability, Alice does have the ability to test the teas.
Otherwise, Bob rejects Alice.

Probabilistic verifier and IP

For an integer $k \geq 1$, we say that a language L is in IP[k], if: there is a probabilistic poly time Turing machine V that can have a k-round interaction with a prover $P : \{0,1\} \to \{0,1\}$ satisfying:

Completeness

$$x \in L \Rightarrow \exists P, \;\; \Pr[\mathrm{Out}_V \langle V, P \rangle (x) = 1] \geq \frac{2}{3}$$

Soundness

$$x \notin L \Rightarrow \forall P, \;\; \Pr[\mathrm{Out}_V \langle V, P \rangle (x) = 1] < \frac{1}{3}.$$

Define

$$\mathrm{IP} = \mathrm{IP}[n^{O(1)}].$$

Robustness of IP

For fixed $s > 0$,
$\frac{2}{3}$ in the completeness can be replaced by $1 - \frac{1}{2^{n^s}}$.
$\frac{1}{3}$ in the soundness can be replaced by $\frac{1}{2^{n^s}}$.
Proof. V runs m times.
V accepts if the number of times of acceptance is at least $\frac{m}{2}$.
Then:
If $x \in L$, then the probability that V accepts is at least $1 - 2^{-\Omega(m)}$.
If $x \notin L$, then the probability that V accepts is at most $2^{-\Omega(m)}$.

Remarks

1. *P* could have unbounded power
2. Parallel repetition amplifies both completeness and soundness exponentially
   for which probabilistic tools are needed
3. Private coins vs public coins

Linearity of expectation

For any random variables X and Y,

$$E[X+Y]=E[X]+E[Y].$$

Basic properties

1. If $a_1, a_2, \cdots, a_n$ are some numbers whose average is c, then there exists an i such that $a_i \geq c$.
2. If X is a random variable which takes values from a finite set and $E[X] = \mu$, then
$$\Pr[X \geq \mu] > 0.$$
3. If $a_1, a_2, \cdots, a_n \geq 0$ are numbers whose average is c, then the fractions of a_i's that are $\geq k \cdot c$ is at most $\frac{1}{k}$.

Markov inequality

Let X be a positive random variable. Then

$$\Pr[X \geq k \cdot E[X]] \leq \frac{1}{k}.$$

More properties

1. If $a_1, a_2, \cdots, a_n$ are numbers in the interval $[0, 1]$ whose average is ρ, then there are at least $\frac{\rho}{2}$ of the a_i's that are at least $\geq \frac{\rho}{2}$.
2. If $X \in [0, 1]$ and $E[X] = \mu$, then for any $c < 1$,

$$\Pr[X \leq c\mu] \leq \frac{1-\mu}{1-c\mu}.$$

Variance

The variance of a random variable X is:

$$\begin{aligned} \mathrm{Var}[X] &= E[(X - E[X])^2] \\ &= E[X^2] - (E[X])^2. \end{aligned} \tag{1}$$

The standard deviation of X is:

$$\sigma(X) = \sqrt[2]{\mathrm{Var}[X]}.$$

Chebyshev inequality

If X is a random variable with standard deviation σ, then for every $k > 0$,

$$\Pr[|X - E[X]| > k \cdot \sigma] \leq \frac{1}{k^2}.$$

Proof. Applying Markov to $(X - E[X])^2$.

Variance property

If $X_1, X_2, \cdots, X_n$ are pairwise independent, then

$$\mathrm{Var}[\sum_{i=1}^{n} X_i] = \sum_{i=1}^{n} \mathrm{Var}[X_i].$$

Chernoff bounds

Let $X_1, X_2, \cdots, X_n$ be mutually independent random variables over $\{0.1\}$, and let $\mu = \sum_{i=1}^{n} E[X_i]$. Then for every $\delta > 0$,

(1)

$$\Pr[\sum_{i=1}^{n} X_i \geq (1+\delta)\mu] \leq [\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}]^{\mu}.$$

(2)

$$\Pr[\sum_{i=1}^{n} X_i \geq (1-\delta)\mu] \leq [\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}]^{\mu}.$$

For every $c > 0$,

$$\Pr[|\sum_{i=1}^{n} X_i - \mu| \geq c \cdot \mu] \leq 2 \cdot e^{-\min\{c^2/4, c/2\} \cdot \mu}.$$

Graph non-isomorphism

Given graphs G_1, G_2, the prover P tries to convince the verifier V that $G_1 \ncong G_2$.
The verifier V:
– randomly picks $i \in \{1, 2\}$,
– let H be a random permutation of G_i,
– send H to P.
The prover P: send an i'.
V: If $i' = i$, accept, and reject otherwise.

Proofs

Completeness Assume $G_1 \ncong G_2$.
The honest prover P convinces V to accept with probability 1.
Soundness Assume $G_1 \cong G_2$.
For any prover P, V accepts with probability $\frac{1}{2}$.

Remarks:
i) Zero knowledge
ii) Private coins

Quadratic non-residuosity

Definition

We say that a is a quadratic residue mod p, if there is a b such that

$$a \equiv b^2 (\mathrm{mod}),$$

in which case, b is called the square root of $a \pmod{p}$.

QNR:
(a, p), p is prime and a is not a quadratic residue mod p.

Interactive proof system for QNR

V:
(i) Picks a random $r \pmod p$
(ii) picks a random bit b
(iii) If $b = 0$, sends $r^2 \pmod p$
If $b = 1$, sends $a \cdot r^2 \pmod p$

P: Answers b', which is expected to be b

V: Accepts if $b' = b$.

Proofs

Completeness $(a, p) \in \mathrm{QNR}$.
ar^2 and r^2 are different, since ar^2 is not a quadratic residue, but r^2 is. A honest prover P convinces V to accept with prob 1.
Soundness $(a, p) \notin \mathrm{QNR}$
$\{ar^2\}$ and $\{r^2\}$ are the same.
For any P, V accepts with prob $\frac{1}{2}$.

AM

Definition

(AM) For every k, the complexity class AM[k] to be the subset of IP[k] obtained by restricting the verifier's messages to be random bits.
An interactive proof system where the verifier has this form is called a public coin proof, or Arthur-Merlin proof, AM.

AM proceeds as follows:
V: picks random bits and sends to P

P: Responses with a message

V: makes a decision

MA

An interactive proof system of the form:

P: sends a message to V

V: picks random bits

V: makes a decision

Public interaction proof system for GNI

Given graphs G_1 and G_2, define

$$S = \{(H, \pi) \mid H \cong G_1 \text{via } \pi \text{ or } H \cong G_2 \text{ via } \pi\}.$$

Lemma

$$G_1 \cong G_2 \Rightarrow |S| = n!$$

$$G_1 \ncong G_2 \Rightarrow |S| = 2 \cdot n!$$

Can we use the gap between the two cases to construct an interactive prof system using public coins?

Pairwise independent hash functions

Definition

Let $\mathcal{H}_{n.k}$ be a collection of functions from $\{0,1\}^n$ to $\{0,1\}^k$. We say that $\mathcal{H}_{n,k}$ is pairwise independent if for every $x, x' \in \{0,1\}^n$ with $x \neq x'$ and for every $y, y' \in \{0,1\}^k$,

$$\Pr_{h \in_{\mathrm{R}} \mathcal{H}_{n.k}} [h(x) = y \; \& \; h(x') = y'] = \frac{1}{2^{2k}}.$$

Intuition: If $x \neq x'$, then $\langle h(x), h(x') \rangle$ is a uniform distribution of $\{0,1\}^k \times \{0,1\}^k$.

Efficient pairwise independent hash functions

For every n, define the collection $\mathcal{H}_{n.n}$ to be $h_{a,b}$ for $a, b \in \mathrm{GF}(2^n)$, where $h_{a,b}$ is the function from x to $ax + b$ for all $x \in \mathrm{GF}(2^n)$.

Theorem

$\mathcal{H}_{n,n}$ is a collection of pairwise independent hash functions.

Proof.

$h(x) = y \;\&\; h(x') = y' \iff ax + b = y \;\&\; ax' + b = y' \iff$ $a = \frac{y-y'}{x-x'},\ b = y - \frac{y-y'}{x-x'}x$, which hold with probability $\frac{1}{2^{2n}}$. □

A lower bound protocol

Assume: (i) $S \subseteq \{0,1\}^m$ is a set whose membership can be certified, (ii) both P and V knows a number K.
The prover P wants to convince the verifier V that $|S| \geq K$.
Require: V rejects with high probability if $|S| \leq \frac{K}{2}$.
Let k be such that

$$2^{k-2} < K \leq 2^{k-1}.$$

Let $\mathcal{H}_{n,k}$ be a collection pairwise independent hash functions.

The public coin protocol

V:
(i) picks h from $\mathcal{H}_{n,k}$ uniformly and randomly
(ii) Picks $y \in_{\mathrm{R}} \{0,1\}^k$
(iii) sends h, y to P.
P:
(i) tries to find an x in S such that $h(x) = y$,
(ii) sends x to V
V: If $x \in S$ and $h(x) = y$, then accept, and reject otherwise.

Basic lemma

Lemma

Let $\subseteq \{0,1\}^m$ *with* $|S| \leq 2^{k-1}$. *For* $p = \frac{|S|}{2^k}$,

(1) $\Pr[(\exists x \in S)[h(x) = y]] \leq p$

(2) $\Pr[(\exists x \in S)[h(x) = y]] \geq \frac{3}{4}p.$

Proof.

For (2). For $x \in S$, set $E_x : \; h(x) = y$. Then,

$$\begin{aligned} \Pr[(\exists x \in S)[h(x) = y]] &= \Pr[\vee E_x] \\ \geq \sum_{x \in S} \Pr[E_x] - \frac{1}{2} \sum_{x \neq x'} &\Pr[E_x \wedge E_{x'}] \\ = \frac{|S|}{2^k} - \frac{1}{2}\frac{|S|^2}{2^{2k}} &\geq \frac{3}{4}p. \end{aligned} \tag{2}$$

Proof of the protocol for GNI

Let $p^* = K/2^k$.
If $|S| \geq K$, then the probability that V accepts is at least

$$\frac{3}{4}\frac{|S|}{2^k} \geq \frac{3}{4}\frac{K}{2^k} = \frac{3}{4}p^*.$$

If $|S| < \frac{K}{2}$, then the probability that V accepts is at most

$$p = \frac{|S|}{2^k} < \frac{1}{2^k}\frac{K}{2} = \frac{1}{2}p^*.$$

Run V several times, and accepts if the fraction of acceptance is $\geq \frac{5}{8}p^*$.
Then by Chernoff bound,
If $|S| \geq K$, V acc with prob at least $\frac{2}{3}$.
If $|S| < \frac{K}{2}$, V acc with prob at most $\frac{1}{3}$.

IP $\subseteq$ PSPACE

QSAT

A quantified SAT (QSAT) instance is of the form:

$$\phi : \forall x \exists y (x \vee y) \wedge \forall z ((x \wedge z) \vee (y \wedge \neg z)) \vee \exists w (z \vee (y \wedge \neg w)).$$

Definition

A QSAT instance ϕ is called *simple*, if for any variable x, there is at most one $\forall$ variable between the start of x and the quantification of x.

Simplification of QSAT

Lemma

Any QSAT instance ϕ can be transformed in logarithmic space to an equivalent simple QSAT instance ψ.

Proof.

For a violating variable x of the form:

$$\cdots Qx \cdots \forall y \psi(x)$$

We replace it by:

$$\cdots Qx \cdots \forall y \exists x' ((x \wedge x') \vee (\neg x \wedge \neg x')) \wedge \psi(x')).$$

Note: negation occurs only for variables. □

Arithmetization

1. $\vee$: $+$
2. $\wedge$: $\times$
3. $\neg x$: $1 - x$
4. $\exists$: $\sum$
5. $\forall$: $\prod$

$$\phi : \ \forall x \exists y (x \vee y) \wedge \forall z ((x \wedge z) \vee (y \wedge \neg z)) \vee \exists w (z \vee (y \wedge \neg w)).$$

$$A_\phi = \prod_{x=0}^{1} \sum_{y=0}^{1} [(x+y) \prod_{z=0}^{1} [(xz + y(1-z)) + \sum_{w=0}^{1} (z + y(1-w))]].$$

A_ϕ

Lemma

For any QSAT instance ϕ, ϕ is true if and only if $A_\phi > 0$.

Proof.

By induction on the structure of ϕ. □

Lemma

If the length of ϕ is n, then $A_\phi \leq 2^{2^n}$.

Proof.

Each $\times$ and $\prod$ at most square the value, and each $+$ and $\sum$ at most double the value. □

Prime number theorem

For $n > 1$, let $\pi(n)$ be the number of primes between 1 and n, then

$$\pi(n) = \frac{n}{\ln n}(1 \pm o(1)).$$

Consequently, the number of primes between 2^n and 2^{3n} is at least 2^n.

Chinese remainder theorem

Suppose that $m_1, m_2, \cdots m_n$ are pairwise relatively prime natural numbers. Let $m = \prod_{i=1}^{n} m_i$. Then for every n-tuple $(a_1, a_2, \cdots, a_n)$ in $Z_{m_1} \times \cdots Z_{m_n}$, there is a unique $x < m$ such that for every i,

$$x \equiv a_i \pmod{m_i}.$$

Therefore, there is a one-to-one coding between Z_m and $Z_{m_1} \times \cdots Z_{m_n}$.

Lemma

Lemma

Let $A = A_\phi$ for a ϕ of length n. Then if $A > 0$, then there is a prime p such that

$$2^n < p < 2^{3n}$$

and

$$A \not\equiv 0 \pmod{p}.$$

Interactive protocol for QSAT

Given a QSAT instance ϕ, a prover P wants to convince the verifier V that $A = A_\phi > 0$.
P:
(i) sends V a number p with a certificate that p is a prime between 2^n and 2^{3n}, and
(ii) send V a number a which is expected to be $A \equiv a \pmod{p}$.
V: will check the correctness.
Suppose that

$$\phi = \forall x_1 \exists y_1 \cdots \forall x_l \exists y_l \psi(x_1, y_1, \cdots, x_l, y_l).$$

$$A = \prod_{x_1=0}^{1} \sum_{y_1=0}^{1} \cdots \prod_{x_l=0}^{1} \sum_{y_l=0}^{1} P(x_1, y_1, \cdots, x_l, y_l).$$

The protocol

V asks P for:

$$P_1(x_1) = \sum_{y_1=0}^{1} \cdots \prod_{x_l=0}^{1} \sum_{y_l=0}^{1} P(x_1, y_1, \cdots, x_l, y_l)$$

P: answers $Q_1(x_1)$ which is expected to be $P_1(x_1)$.
V: If $Q_1(0)Q_1(1) \not\equiv a \pmod{p}$, then reject. Otherwise, then:
(i) let r_1 be a random number $\leq p$,
(ii) let $a_1 = Q_1(r_1) \mod p$,
(iii) sends r_1 to P, asking for

$$P_2(y_1) = \prod_{x_2=0}^{1} \sum_{y_2=0}^{1} \cdots \prod_{x_l=0}^{1} \sum_{y_l=0}^{1} P(r_1, y_1, x_2, y_2 \cdots, x_l, y_l).$$

Therefore

$$a_1 = P_2(0) + P_2(1) \; (\mathrm{mod} p).$$

Protocol

Assume:
P answers $Q_2(y_1)$ to be expected to be $P_2(y_1)$.
V: if $Q_2(0) + Q_2(1) \not\equiv a_1(\mathrm{mod} p)$, then reject. Otherwise, then:
(i) pick a random number $r_2 \leq p$,
(ii) let $a_2 = Q_2(r_2)$,
(iii) sends r_2 to P, asking for

$$P_3(x_2) = \sum_{y_2=0}^{1} \cdots \prod_{x_l=0}^{1} \sum_{y_l=0}^{1} P(r_1, r_2, x_2, y_2 \cdots, x_l, y_l).$$

Get a response $Q_3(x_2)$ to be expected $P_3(x_2)$.
Continuing the procedure.

Completeness

If $A \equiv a \bmod p$, then the honest prover convinces the verifier V to accept with probability 1.

Polynomial identity test

Given a polynomial $p(x)$ of degree d, and a finite field F, if p is not identically zero, then

$$\Pr_{x \in_{\mathrm{R}} F}[p(x) = 0] \leq \frac{d}{|F|}.$$

Soundness

Assume $A \neq a \mod p$. Note, all the polynomials are of degree at most $d = 2n$.
Let

$$P_1(x_1) = \sum_{y_1=0}^{1} \prod_{x_2=0}^{1} \sum_{y_2=0}^{1} \cdots \prod_{x_l=0}^{1} \sum_{y_l=0}^{1} \psi(x_1, y_1, x_2, y_2, \cdots, x_l, y_l).$$

Known: $P_1(0)P_1(1) \neq a$.
P sends $Q_1(x_1)$ to V, which is expected to be $P_1(x_1)$
V: If $Q_1(0)Q_1(1) \neq a$, then V rejects now.
Otherwise, $Q_1(0)Q_1(1) = a$, implying $P_1 \not\equiv Q_1$. An error occurs.

Second round

The protocol proceeds with an error that $Q_1 \not\equiv P_1$.
V: pick a random r_1, asks P for

$$P_2(y_1) = \prod_{x_2=0}^{1} \sum_{y_2=0}^{1} \cdots \prod_{x_l=0}^{1} \sum_{y_l=0}^{1} \psi(r_1, y_1, x_2, y_2, \cdots, x_l, y_l).$$

Get $Q_2(y_1)$ from P.
By definition,

$$P_2(0) + P_2(1) = P_1(r_1)$$

V: checks
If $Q_2(0) + Q_2(1) \neq Q_1(r_1)$, then rejects.
With prob $\geq 1 - \frac{d}{p}$,

$$P_1(r_1) \neq Q_1(r_1).$$

This is again an error, such that with prob at least $1 - \frac{d}{p}$, the protocol continues with this error.

Third round

V: Picks a random r_2, asks P for

$$P_3(x_2) = \sum_{y_2=0}^{1} \cdots \prod_{x_l=0}^{1} \sum_{y_l=0}^{1} \psi(r_1, r_2, x_2, y_2, \cdots, x_l, y_l).$$

Gets an answer $Q_3(x_2)$.
By definition,

$$P_3(0)P_3(1) = P_2(r_2)$$

If $Q_3(0)Q_3(1) \neq Q_2(r_2)$, then rejects.
Otherwise, go on to the next round. In this case,

$$Q_3(0)Q_3(1) = Q_2(r_2) \neq P_2(r_2).$$

This is an error, which occurs with probability $\geq 1 - \frac{d}{p}$.

Final round

At each round, with probability at least $1 - \frac{d}{p}$, there is an error. If the error is kept in the last round, then V must find the error by checking the identity of the following form:

$$Q(0) + Q(1) \neq P(r_1, r_2, \cdots, r_{2l})$$

and then rejects.
Therefore, the probability that V rejects is at least

$$(1 - \frac{d}{p})^n \approx 1 - \frac{dn}{n} \approx 1.$$

New ideas and potential developments

- Interaction and randomness together increase the computational power
- Algebraic + probabilistic definitions of computational complexity classes
- Zero knowledge, potential new theory of cryptography
- New mathematics that are locally testable

Thinking

Story of IP: There is a long story for the discovery of IP

Questions

1. Why did not Chinese contribute anything in this new developments?
2. How can we achieve the first class of achievements in the future?