Around the PCP theorem

in the footsteps of giants

Bruno Sévennec

UMPA - ENS Lyon

2020-05-28

Outline

- Classes P and NP
- Classes PCP(r(n),q(n))
- The PCP theorem(s)
- Outline of proof of a "toy" PCP theorem

P decision problems

Definition

A decision problem ($x \in L$? for a subset L of $\{0,1\}^*$) is in P (Polynomial time) if there is a Turing machine M deciding each instance in time polynomial with respect to the input size. Thus M always halts in polynomial time, and computes the characteristic function of L.

Examples in P

- Coprimeness of natural integers (Euclid)
- Correctness of a proposed formalized proof of a mathematical statement, e.g. in PA (or ZFC, or ZF+DC)
- 2SAT : satisfiability of a 2CNF boolean formula such as $(x_0 \vee \neg x_4) \wedge (x_{10} \vee x_2) \wedge \cdots \wedge (\neg x_{117} \vee \neg x_{42})$
- LP : Non-emptiness of an intersection of rational halfspaces in $\mathbb{R}^n$ (Kachiyan 1979)
- Primeness of natural integers (AKS primality test 2002)

NP decision problems

Definition

A decision problem (i.e. subset L of $\{0,1\}^*$) is in NP (Non-deterministic Polynomial time) if there is a polynomial P and a polynomial time Turing machine M that for each x accepts **some** "witness", or "certificate", u of size $\leq P(|x|)$ (seen as a proposed proof that $x \in L$) if and only if $x \in L$. More formally, $x \in L \Leftrightarrow \exists u \in \{0,1\}^{P(|x|)}, M(x,u) = 1$.

Note

This could as well have been called "Polynomially Checkable Proof" ;)

Remark

Contrary to P there is a huge dissymmetry between true and false instances, because $x \notin L \Leftrightarrow \forall u \in \{0,1\}^{P(|x|)}, M(x,u) = 0$. Hence a class coNP, conjectured to be $\neq$ NP. Obviously $P \subset NP \cap coNP$ (no witness needed).

Examples in NP

- $3SAT$: Satisfiability of a 3CNF boolean formula
- $\neg PRIME$: Compositeness of natural numbers is in NP
- $PRIME$: Primeness of natural numbers is in NP (A polynomial size certificate is not so obvious. It recursively uses that an odd n is prime iff $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic of order $n-1$. A generator a together with prime factorization $n-1=\prod p_i^{r_i}$ begins the certificate, which continues with primeness certificates for the p_i etc. The machine checks e.g. that $a^{n-1}\equiv 1 \mod n$ but $a^{(n-1)/p_i}\not\equiv 1 \mod n$ using fast exponentiation)
- $3COL$: 3-colorability of a finite graph is in NP

Note

Problems in NP are decidable, hence truth of PA statements is not in NP.

NP completeness

Theorem

(Cook 1971) Every NP problem is polynomial-time-reducible to 3*SAT.*

3SAT is the first "NP-complete" decision problem.

Definition

A decision problem $x \in L$ is *NP-hard* if any NP problem is polynomial-time-reducible to it, and *NP-complete* if it is moreover in NP.

Note

The following special case of SDP (SemiDefinite Programming) is apparently not known to be in NP : Given non-negative integers $a_1, \dots, a_k, b_1, \dots, b_k$, decide if $\sqrt{a_1} + \dots \sqrt{a_k} \geq \sqrt{b_1} + \dots \sqrt{b_k}$.
The problem is with the precision needed to decide (on the other hand it is, like SDP, polynomial-time-decidable if a small additive error is allowed).

PCP classes

Definition

A language/decision problem $L \subset \{0,1\}^*$ is in the class $PCP(r(n), q(n))$ if there is a polynomial-time *probabilistic* Turing machine V ("verifier") which on inputs x and π from $\{0,1\}^*$ ("statement" and "proof") accepts ($V(x,\pi) = 1$) or rejects ($V(x,\pi) = 0$) as follows

1. It flips $r(|x|)$ random (fair) coins.
2. From these, it reads only $q(|x|)$ bits $\pi' = (\pi_i)_{i \in I}$ from π.
3. $\forall x \in L$, $\exists \pi$, $\mathbb{E}[V(x,\pi')] = 1$ (π is always accepted).
4. $\forall x \notin L$, $\forall \pi$, $\mathbb{E}[V(x,\pi')] \leq 1/2$ (π is rejected at least half of the time).

Remark

A crucial point is that the length of "proofs" π is a priori *arbitrary*, even though in fact one can assume the proof to be of length $\leq 2^{r(|x|)} q(|x|)$, the maximum number of bits of π read in all possible runs with input (x,π).

Note

There are also variants Σ-$PCP_{c,s}(r(n), q(n))$ with parameters c, s (completeness, resp. soundness) giving bounds on the probability of accepting valid resp. invalid proofs, and a bigger alphabet Σ instead of $\{0, 1\}$. The previous definition corresponds to $\{0, 1\}$-$PCP_{1,1/2}(r(n), q(n))$.

Note

Randomness plays a very important role in computational complexity, and its power is not yet completely understood. For example, no polynomial time deterministic algorithm is known to output a prime number with n digits, whereas an obvious probabilistic sampling followed by a polynomial time primality test runs in polynomial expected time (see polymath4 project, 2009).

The PCP theorem, proof-checking version

Theorem (Arora, Lund, Motwani, Szegedy, Sudan 1992)

There is a universal constant Q such that $NP \subseteq PCP(O(\log n), Q)$.

Note

The proof was subsequently improved by many people, culminating with Irit Dinur's "much simpler" proof in 2007, which earned her the 2019 Gödel Prize. In 2001, the same prize was already awarded to ALMSS + Feige, Goldwasser, Lovász, Safra for work on PCP and hardness of approximation.

Remarks

Taking $Q = 16$ is enough for the above statement to hold (see Nelson's lecture 22). The implicit constant in $O(\log n)$ depends on the NP problem considered. The length of the proofs examined by the resulting verifiers is *polynomial* in n.

PCP theorem can (a bit tautologically, but perhaps suggestively) be viewed as a hardness result for a "gap problem" :

Corollary

Given a PCP verifier V for some NP-complete problem, e.g. 3SAT, it is NP-hard to decide between $\omega(V, x) = 1$ and $\omega(V, x) \leq 1/2$, where

$$\omega(V, x) = \max_{\pi \in \{0,1\}^*} \mathbb{E}[V(x, \pi)]$$

is the maximum probability of acceptance of a proof of x.

The PCP theorem, game version

Definition

A 2-provers 1-round (2P1R) game G is given by finite sets X_1, X_2 of questions, A_1, A_2 of answers, functions $f_1 : X_1 \to A_1$, $f_2 : X_2 \to A_2$ (strategies of the provers), a probability μ on $X_1 \times X_2$ and a predicate

$$V : X_1 \times X_2 \times A_1 \times A_2 \to \{0, 1\}$$

for acceptance of answers.

The *value* of G is then

$$\omega(G) = \max_{f_1, f_2} \mathbb{E}_{x_1, x_2}[V(x_1, x_2, f_1(x_1), f_2(x_2))].$$

Theorem (PCP, game version)

There is a constant $\varepsilon_0 > 0$ *such that for any* $L \subset \{0,1\}^*$ *in NP, there is a polynomial-time-computable mapping* $x \mapsto G_x$ *from* $\{0,1\}^*$ *to 2P1R games such that* $\omega(G_x) = 1$ *for* $x \in L$ *and* $\omega(G_x) \leq 1 - \varepsilon_0$ *otherwise.*

Note

This could be amplified using the "parallel repetition theorem" discovered by Raz (1998)...

Outline of proof of a "toy" PCP theorem

Theorem

There is a constant q such that $NP \subseteq PCP(poly(n), q)$.

The proofs examined by such verifiers could be huge (of size 2^{cn^k}), but only a constant number of bits of them will be examined.

It is enough to construct a verifier with the required properties for *one* NP-complete decision problem.

The chosen decision problem will be the satisfiability of systems of quadratic equations over the field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

To show NP-completeness, observe that since

$$a \vee b \vee c = a + b + c + ab + bc + ca + abc$$

in $\mathbb{F}_2 = \{0, 1\}$, any instance of 3SAT can be viewed as a system of *cubic* equations over $\mathbb{F}_2$.

The classical trick of introducing auxiliary variables $x_{ij} = x_i x_j$ for intermediate products gives an equi-satisfiable system of quadratic equations, whose size is polynomial in the size of the $3SAT$ instance.

So we consider systems of equations

$$Q_i(x) + L_i(x) = c_i, \quad i = 1, \dots, m, \quad x \in \mathbb{F}_2^n \qquad (\mathcal{Q})$$

where Q_i, L_i are homogeneous polynomials of degree 2 resp. 1, aka quadratic and linear forms in x, and c_i are constants in $\mathbb{F}_2$.

The verifier will examine proofs of satisfiability consisting of a pair of functions

$$\Pi^1 : \mathbb{F}_2^n \to \mathbb{F}_2, \qquad \alpha \mapsto \Pi^1_\alpha$$

$$\Pi^2 : \mathbb{F}_2^n \otimes \mathbb{F}_2^n = \mathbb{F}_2^{n^2} \to \mathbb{F}_2, \qquad \beta \mapsto \Pi^2_\beta.$$

Such a proof will be correct iff there is an $x \in \mathbb{F}_2^n$ such that for all $\alpha \in \mathbb{F}_2^n$, $\beta \in \mathbb{F}_2^{n^2}$

$$\Pi^1_\alpha = \alpha \cdot x, \quad \Pi^2_\beta = \beta \cdot (x \otimes x),$$

and moreover x satisfies the system $Q_i(x) + L_i(x) = c_i$ for $i = 1, \dots, m$.

Remark

This resembles the previously encountered "long encoding" of x. Here $x \in \mathbb{F}_2^n$ is represented as a string of $2^n + 2^{n^2}$ bits.

Writing $L_i(x) = \alpha^i \cdot x$, $Q_i(x) = \beta^i \cdot (x \otimes x)$, this satisfaction is checked by

- Choosing $(a_1, \ldots, a_m) \in \mathbb{F}_2^m$ uniformly at random
- Computing $\alpha = \sum_i a_i \alpha^i$, $\beta = \sum_i a_i \beta^i$, $c = \sum_i a_i c_i$
- Querying Π^1_α, Π^2_β
- Accepting iff $\Pi^1_\alpha + \Pi^2_\beta = c$

By the magic of $\mathbb{F}_2$-linear algebra, this falsely accepts with probability $\leq 1/2$.

But the verifier still has to (randomly) check that $\alpha \mapsto \Pi^1_\alpha$, $\beta \mapsto \Pi^2_\beta$ are *linear*, and moreover of the form

$$\Pi^1_\alpha = \alpha \cdot x, \quad \Pi^2_\beta = \beta \cdot (x \otimes x)$$

for some x. Given linearity, this is ensured by checking that

$$\Pi^2_{\alpha \otimes \alpha'} = \Pi^1_\alpha \Pi^1_{\alpha'}$$

for $\alpha, \alpha' \in \mathbb{F}_2^n$ uniformly random, and one can show that the probability of falsely accepting is $\leq 3/4$. This leads us to...

Linearity testing

Theorem (Blum,Luby,Rubinfeld 1993)

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2$ be an arbitrary function, and equip $\mathbb{F}_2^n$ and its square with the uniform probability. Then if $\mathbb{P}_{x,y}[F(x+y) = F(x) + F(y)] \geq \rho > 1/2$, there is a linear form L such that $\mathbb{P}_x[F(x) = L(x)] \geq \rho$.
L is unique if $\rho > 3/4$.

Note ("local decoding")

When $\rho > 3/4$, even if F is not exactly linear, $L(x)$ can be efficiently recovered at *all* points x by evaluating $F(x+r) - F(r)$ for random r. This is easily seen to equal $L(x)$ with probablility $\geq 2\rho - 1 > 1/2$, i.e. $\geq 1 - 2\delta$ if $\rho = 1 - \delta$.

Proof : Fourier(-Walsh) analysis on $\mathbb{F}_2^n$.
Euclidean space of functions $f : \mathbb{F}_2^n \to \mathbb{R}$ with scalar product

$$\langle f, g \rangle = \mathbb{E}_x[f(x)g(x)].$$

Orthonormal basis :

$$\chi_\alpha(x) = (-1)^{\alpha \cdot x}, \quad \alpha \in \mathbb{F}_2^n,$$

(all characters, i.e. group homomorphisms $\mathbb{F}_2^n \to \mathbb{C}^*$)

We will use that $\chi_0 \equiv 1$ is orthogonal to all others, and $\chi_\alpha \chi_\beta = \chi_{\alpha+\beta}$.

Replace F by $f = (-1)^F : \mathbb{F}_2^n \to \{\pm 1\}$. Then

$$\mathbb{E}_{x,y}[f(x+y)f(x)f(y)] = 2\mathbb{P}_{x,y}[f(x+y) = f(x)f(y)] - 1$$

and

$$\langle f, g \rangle = \mathbb{E}_x[f(x)g(x)] = 2\mathbb{P}_x[f(x) = g(x)] - 1$$

for any $g : \mathbb{F}_2^n \to \{\pm 1\}$. Writing $f = \sum_\alpha f_\alpha \chi_\alpha$,

$$\begin{aligned} f(x+y)f(x)f(y) &= \sum_{\alpha,\beta,\gamma} f_\alpha f_\beta f_\gamma \chi_\alpha(x+y)\chi_\beta(x)\chi_\gamma(y) \\ &= \sum_{\alpha,\beta,\gamma} f_\alpha f_\beta f_\gamma \chi_{\alpha+\beta}(x)\chi_{\alpha+\gamma}(y) \end{aligned}$$

$$\mathbb{E}_{x,y}[f(x+y)f(x)f(y)] = \sum_\alpha f_\alpha^3 \leq \max_\alpha f_\alpha \sum_\alpha f_\alpha^2 = \max_\alpha f_\alpha$$

Conclusion : $\mathbb{P}_{x,y}[f(x+y) = f(x)f(y)] \geq \rho$ implies

$$f_\alpha = \langle f, \chi_\alpha \rangle \geq 2\rho - 1$$

for some α so $\mathbb{P}_x[F(x) = \alpha \cdot x] = \mathbb{P}_x[f(x) = \chi_\alpha(x)] \geq \rho$ as claimed.

If $\rho > 3/4$ and $\mathbb{P}_x[F(x) = \beta \cdot x] \geq \rho$, then by "union bound"

$$\mathbb{P}_x[\alpha \cdot x = \beta \cdot x] > 1/2$$

so $\alpha = \beta$ because hyperplanes are "half spaces" over $\mathbb{F}_2$.

□

Wrapup

There is $\delta_0 > 0$ and a $PCP_{1,1-\delta_0}(O(n^2), 13)$ verifier for satisfiability a system of quadratic equations over $\mathbb{F}_2$

$$\alpha^i \cdot x + \beta^i \cdot (x \otimes x) = c_i, \quad x \in \mathbb{F}_2^n,\ i = 1, \ldots, m$$

which performs the following tests on a proof $(\Pi^1, \Pi^2) \in \mathbb{F}_2^{2^n + 2^{n^2}}$, rejecting it if one test fails :

1. Linearity test on Π^1 : verify if $\quad \Pi^1_\alpha + \Pi^1_{\alpha'} = \Pi^1_{\alpha+\alpha'}$ for uniformly random $\alpha, \alpha' \in \mathbb{F}_2^n$.
2. Linearity test on Π^2 (same form).
3. Consistency of tensor product : for uniformly random $\alpha, \alpha' \in \mathbb{F}_2^n$, $\beta \in \mathbb{F}_2^{n^2}$, verify if $\quad \Pi^2_{\alpha\otimes\alpha'+\beta} = \Pi^1_\alpha \Pi^1_{\alpha'} + \Pi^2_\beta$.
4. Satisfaction of the quadratic system : for uniformly random $a \in \mathbb{F}_2^m$, compute $\alpha = \sum_i a_i \alpha^i$, $\beta = \sum_i a_i \beta^i$, $c = \sum_i a_i c_i$, and verify if $\Pi^1_\alpha + \Pi^2_\beta = c$.

Repeating this verifier's test k_0 times with $(1-\delta_0)^{k_0} \leq 1/2$, we have obtained $NP \subseteq PCP(O(n^2), 13\, k_0)$.

□□

Thanks !

Bibliography

S. Arora, B. Barak, Computational Complexity: A Modern Approach (2009).

B. Chazelle, The PCP theorem, Séminaire Bourbaki n^o 895, 2001.

O. Goldreich, P, NP, and NP-Completeness: The Basics of Complexity Theory (2010).

O. Goldreich, Computational Complexity: A Conceptual Perspective (2008).

V. Guruswami, R. O'Donnell, Proof of the PCP Theorem, course notes, 2005

V. Guruswami, R. O'Donnell, A history of the PCP Theorem, 2005.

P. Harsha, PCPs, codes and inapproximability, course notes, 2007.

T. Vidick, Around the quantum PCP conjecture, lectures 1-4, 2014

J. Nelson, CS 125: Algorithms & Complexity, lectures 22,23,wrapup, 2016.

L. Trevisan, Mini Crash Course: The Classical PCP Theorem, youtube video, 2014.

H. Yuen, MIP* Wiki, 2020.