Constant rate PCPs with sublinear query complexity

Eli Ben-Sasson (Technion)    Yohay Kaplan (Technion)
Swastik Kopparty (Rutgers)   Or Meir (IAS)
Appendix by Henning Stichtenoth (Sabanci U.)

October 2013
Theorem (PCP [AS, ALMSS])

Every NP-claim has a short proof, can be verified by querying a few bits.

Two main applications, both benefit from shorter proofs:
- Hardness of approximation of CSP [FGLSS96]
  - Focus: query complexity vs. soundness
  - Shorter proofs imply inapprox. for larger class of algorithms
  - Query complexity is arity of CSP constraints
- Succinct verification of computational integrity [BFLS91]
  - Focus: efficiency of prover and verifier
  - Proof length is a lower bound on prover running time
  - Query complexity is lower bound on verifier running time
Introduction

Theorem (PCP [AS98,ALMSS98])

Every NP-claim has a short proof, can be verified by querying a few bits.

- [AS98,ALMSS98]: Short is $\ell = \text{poly}(n)$ (for claim of size $n$), few is $q = O(1)$.
- State of the art [BS05,D06]: $\ell = n \cdot \log^{O(1)} n$, $q = O(1)$
- No prior PCP with $\ell = O(n)$, $q = o(n)$ for any NP-complete $L$.

Theorem (Main: Constant rate PCPs with sublinear q. complexity)

For every $\epsilon > 0$ there exist (non-uniform) PCPs for $\text{CircutSAT}_n$ (instances are circuits with $n$ gates), with $\ell = 2^{c/\epsilon} \cdot n = O_\epsilon(n)$ and $q = n^\epsilon$
Two Corollaries and one Conjecture

Theorem (Main: Constant rate PCPs with sublinear q. complexity)

(Non-uniform) PCPs for CircuitSAT\(_n\) with \(\ell = O_\varepsilon(n)\) and \(q = n^\varepsilon\)

Corollary (log-rate PCPs for NP with subconst. q. complexity)

For any NDTM \(M\) running in time \(n^c\), the language \(L_M\) decided by \(M\) has non-uniform PCPs with \(\ell = O(n^c \log n)\) and \(q = n^\varepsilon\).

Corollary (Hardness of approximation)

If CircuitSAT\(_n\) does not have \(2^{o(n)}\)-size circuits, then \(\max - n^\varepsilon - CSP_n\) has no \(0.1\)-approx. alg. running in time \(2^{o(n)}\).

Conjecture (Succinct computational integrity)

Every \(L \in \text{NTIME}(T(n))\) has PCP with prover time \(O(T(n) \log T(n))\), verifier time \(T(n)^\varepsilon\).
Rest of talk — Main ideas in the proof

- PCP constructions have many moving parts,
- Won't present proof, rather examine 3 new parts in it,
  - Transitive Algebraic Geometry (AG) codes
  - Automorphism-based Schreier graphs
  - AG-generalization of Alon’s Combinatorial Nullstellensatz
- Compare new parts to “old” and “simple” PCP construction, based on bivariate low-degree polynomials
- For simplicity aim for query complexity $\sqrt{n}$ (i.e., $\epsilon = 1/2$)
Bivariate Reed-Muller (RM) PCP with $\sqrt{n}$ queries

- NP-claim given by circuit $\phi$ with $n$ NAND gates, fan-in 2
- RM-PCP proof contains a low-degree extension of $A$:
  - gates $\rightarrow \{0, 1\}$
  
  1. Let $F$ be of size $10\sqrt{n}$ and $H \subset F$, $|H| = \sqrt{n}$
  2. Identify gates with $H \times H$, now assignment is $A : H \times H \rightarrow \{0, 1\}$
  3. Prover writes $f : F \times F \rightarrow F$, supposedly the interpolation of $A$.

- Problem: Bitlength of $f$ is $\geq n \cdot \log |F| = \Omega(n \cdot \log n)$.

- Attempted solution:
  - Pack $\log |F|$ bits of $A$ in each symbol, like done for constant-rate LDCs [KSY11] and LTCs [V12]
  - Fails because need to unpack bits to check different constraints.

- New: Use tensor AG codes! Behave like polynomials (degree, distance, etc.) but with constant alphabet size. (Disclaimer: Restrictions apply, consult algebraist geometer before use.)
Algebraic Constraint Satisfaction Problems (ACSP)

- NP-claim given by circuit $\phi$ with $n$ NAND gates, fan-in 2
- RM-PCP proof contains a low-degree extension of $A : H \times H \rightarrow \{0, 1\}$
- Check each gate $(x, y)$ for consistency with its inputs
  - Let $N_1(x, y)$ be first input-gate to $(x, y)$, $N_2(x, y)$ second input-gate.
  - NAND constraint: $A(X, Y) - (1 - A(N_1(X, Y)) \cdot A(N_2(X, Y))) = 0$
- Problem: $\deg_X(A) = \sqrt{n}$ and $\deg_X(N_i) = \sqrt{n}$ (same with $Y$-degree)
  - Hence $\deg_X(A(N_1)) = n$, same with $Y$-degree
  - Hence $|F|$ must be greater than $n$
  - So proof has size $\geq n^2$
- Solution: Construct circuit where $\deg(N_i) = 1$ by embedding $\phi$ in affine graph
Affine graphs for RM-PCP

- [BS05], following [PS94]: Reduce \( \phi \) to circuit \( \phi' \) in which \( \deg(N_i) = 1 \)
  1. Embed \( \phi \) in a universal circuit \( U \), using vertex disjoint paths
  2. Embed \( U \) in an affine graph \( G \), hence \( N_i \) is an affine function.
     - Affine graph: Schreier graph with \( V = \mathbb{F}^2 \) and edge-generating set a subgroup of the affine group.

- Problem: Resulting \( \phi' \) is of size \( n \log n \).
- New: Use hypercube instead
  - Vertices are \( \mathbb{F} \times \mathbb{F} \)
  - Edges: \((x, y)\) adjacent to \( \{(x + x', y), (x, y + y') | x', y' \in H\} \)
  - Affine graph generated by \( O(\sqrt{n}) \) affine functions, and vertex set size \( O(n) \)

- This works fine for RM, what about AG?
Schreier graphs for AG-PCP

- Question: Why use affine graphs with RM-PCP?
- Answer: Because RM-codes invariant under affine transformation, so 
  \[ \deg_X(A(N)) = \deg_X(A) \]
- In other words: Affine graph is a Schreier graph that uses, as generating set, only automorphisms of the RM code!
- **New:** In AG-PCP, use Schreier graph with generating set that is contained in the automorphisms of the AG-code
- In particular, to embed hypercube need a *transitive* AG-code
- Many results on \( \text{Aut}(C) \) and “local” code properties [YR03, AKKLR05, KS08, KW06, BS11, BGMSS12, BGKSS13, …].
- **New:** AG codes with a sufficiently rich automorphism group leads to better PCPs!
Asymptotically good transitive AG codes

- Need codes satisfying
  - constant rate, relative distance, and alphabet size
  (needed to achieve constant rate PCP)
  - polynomial-like “multiplication property” [M10]
  (needed to facilitate arithmetization)
  - Invariant under action of a transitive group
  (needed to allow reduction of \( \phi \) to hypercube)
- Do they exist?

**Theorem (Stichtenoth, 2006)**

For infinitely many \( k_1 < k_2 < \ldots \), exists transitive AG code of dimension \( \dim(C_i) = k_i \) and constant rate, relative distance, and alphabet-size.

Problem: family is sparse, i.e., \( k_i / k_{i-1} \to \infty \)

**Theorem (Stichtenoth, New dense family of transitive AG codes)**

For inf. many \( k_1 < k_2 < \ldots \), \( k_i / k_{i-1} = O(1) \), exists transitive AG code of dimension \( k_i \), constant rate, relative distance, and alphabet-size.
Zero testing and Sum-check

Zero testing problem: Verify that $P(X, Y)$ vanishes on $H \times H$. We provide two different solutions

- “Combinatorial” \cite{M10}: All tensor codes have a sum-check protocol
- “Algebraic”: Generalize Alon’s combinatorial nullstellensatz to AG
AG combinatorial nullstellensatz

Verify that $P(X, Y)$ vanishes on $H \times H$.

- Univariate (simpler) case: Given $f \in C$, verify $f(x) = 0$ for all $x \in H$.
- Reed-Solomon: $P(X)|_H = 0$ iff $\exists \hat{P}(X), P(X) = \hat{P}(X) \cdot \text{Zero}_H(X)$, where $\text{Zero}_H(X) = \prod_{\alpha \in H}(X - \alpha)$
- [BS05] used this in RS-PCP, generalization to RM-PCP is

**Theorem (Combinatorial Nullstellensatz [Alon99])**

Low-degree $P(X, Y)$ vanishes on $H \times H$ iff there exist low-degree $B, C$ s.t.

$$P(X, Y) = B(X, Y) \cdot \text{Zero}_H(X) + C(X, Y) \cdot \text{Zero}_H(Y)$$

- What if $C$ is AG-code? Is there a function vanishing precisely on $H$?

**Theorem (New AG Combinatorial Nullstellensatz)**

For $H \subset D$ there exist $Z_H, Z'_H$ such that “low-degree” $f : D \times D \to \mathbb{F}$ vanishes on $H \times H$ iff exist “low-degree” $g, h : D \times D \to \mathbb{F}$ s.t.

$$f(X, Y) \cdot Z'_H(X, Y) = g(X, Y) \cdot Z_H(X) + h(X, Y) \cdot Z_H(Y)$$
Concluding remarks

Theorem (Main: Constant rate PCPs with sublinear q. complexity)

For every $\epsilon > 0$ there exist (non-uniform) PCPs for $\text{CircuitSAT}_n$ (instances are circuits with $n$ gates), with $\ell = 2^{c/\epsilon} \cdot n = O_\epsilon(n)$ and $q = n^\epsilon$

- Construction uses tensors of transitive AG codes
- Such codes are useful because
  - are asymptotically good
  - transitivity facilitates efficient ACSPs via universal Schreier graphs
  - have a combinatorial nullstellensatz theorem

Questions

1. Remove non-uniformity assumptions, requires (only) explicit polynomial time construction of transitive AG codes
2. Are there PCPs with constant rate and $q = O(1)$?, perhaps $q = \log n$?