Hypercontractivity, Sum-of-Squares Proofs, and their Applications

Boaz Barak
MSR New England

Fernando G.S.L. Brandão
Universidade Federal de Minas Gerais

Aram W. Harrow
University of Washington

Jonathan Kelner
MIT

David Steurer
MSR New England

Yuan Zhou
CMU

May 16 2012, Theory Seminar, Georgia Tech
Motivation

Unique Games Conjecture (UGC) [Khot’02]

For every $\epsilon > 0$, the following is \textbf{NP}-hard:

Given: system of equations $x_i - x_j = c \mod k$ \hspace{1cm} (say $k = \log n$)

Distinguish:

\textbf{YES:} \hspace{1cm} at least $1 - \epsilon$ of equations satisfiable

\textbf{NO:} \hspace{1cm} at most $\epsilon$ of equations satisfiable
Motivation

Unique Games Conjecture (UGC) [Khot’02]

Implications of UGC

For large class of problems, **BASIC SDP** achieves optimal approximation

*Examples: MAX CUT, VERTEX COVER, any MAX CSP*

[Khot-Regev’03, Khot-Kindler-Mossel-O’Donnell’04, Mossel-O’Donnell-Oleszkiewicz’05, Raghavendra’08]

*Is the conjecture true?*
In this work:

1) \textit{Evidence: }\exists \text{ polynomial-time algorithm } \text{ refuting UGC} \\
\textit{Show: } natural \ algorithm \ solves \ all \ known \ UG \ instances \ (including \ hard \ instances \ for \ other \ algorithms)

2) \textit{Evidence: } \forall \text{ polynomial-time algorithm } \text{ refuting UGC} \\
\textit{Show: } natural \ generalization \ of \ UG \ requires \ qpoly(n)-time \ (but \ still \ admits \ “same” \ subexponential \ algorithm \ as \ UG)
Semidefinite Programming (SDP) Hierarchies

[Sherali-Adams’90, Lovász-Schrijver’91,...]

How many significant eigenvalues can a small-set expander have?

(related to Locally Testable Codes)
Semidefinite Programming (SDP) Hierarchies

Result in this work: aka: Lasserre hierarchy

Sum-of-Squares (SoS) hierarchy [Parrilo’00, Lasserre’01]

All known UG instances in level-8 of this hierarchy

qualitative difference: basis independence of SoS hierarchy
Small-Set Expansion (SSE) & Operator Norms
(closely related to UG [Raghavendra-S.’09])

Result:

\[ P_\lambda = \text{projector into span of eigenfunctions of } G \text{ with eigenvalue } \geq \lambda \]

all sets of volume \( \leq \delta \) have expansion \( \geq 1 - \lambda^{\Theta(1)} \)

\[ \iff \text{2-to-4 operator norm of } P_\lambda \text{ is } \leq 1/\delta^{\Theta(1)} \text{ (hypercontractive)} \]

\[ \|P\|_{2\to4} = \max_{f:V\to\mathbb{R}} \|Pf\|_4/\|f\|_2 \]

\( f \) is \( \delta \)-sparse \( \iff \|f\|_4/\|f\|_2 > 1/\delta^{1/4} \)

Corollary: SSE-hard to certify hypercontractivity (even for projectors)
**Complexity of Hypercontractivity**

**Given:** projector $P$ into subspace of functions $f: V \rightarrow \mathbb{R}$ with $|V| = n$

**Promise:** $\|P\|_{2\rightarrow 4} = O(1)$ (hypercontractive)

**Certify:** $\|P\|_{2\rightarrow 4} = O(1)$ (for different constant $O(1)$)

**Results:**

- **subexponential** time $\exp(n^{1/2})$ suffices (can recover best algorithm for SSE by choice of norm)

- **quasipolynomial** time necessary (*) (builds on hardness of quantum separability) [Harrow-Montanaro’10]

(*) assuming $3\text{SAT}$ requires $2^{\Omega(n)}$ time
PROOF IDEAS
Result:

Level-8 SoS relaxation refutes UG instances based on long-code and short-code graphs

How to prove it?  (rounding algorithm?)

*Interpret* dual as proof system

*Lift* soundness proofs to this proof system

(SDP completeness & integral soundness)
**Sum-of-Squares Proof System** (informal)

**Axioms**

\[
\begin{align*}
P_1(z) & \geq 0 \\
& \vdots \\
P_m(z) & \geq 0
\end{align*}
\]

**Rules**

- Polynomial operations
- \( R(z)^2 \geq 0 \) for any polynomial \( R \)

Intermediate polynomials have *bounded degree* 

(c.f. bounded-width resolution, but basis independent)

["Positivstellensatz" \cite{Stengel}]
**Example**

In SoS proof system, \( \{z^2 \leq z\} \iff \{0 \leq z \leq 1\} \)

Axiom: \( z^2 \leq z \quad \text{Derive: } z \leq 1 \)

\[
1 - z = z - z^2 + (1 - z)^2 \\
\geq z - z^2 \quad \text{(non-negativity of squares)} \\
\geq 0 \quad \text{(axiom)}
\]
**Components of soundness proof** (for known UG instances)

**Non-serious issues:**
- Cauchy–Schwarz / Hölder
- Influence decoding
- Independent rounding

**Serious issues:**
- Hypercontractivity
- Invariance Principle

*can use variant of inductive proof, works in *Fourier basis*

*typically uses *bump functions*, but for UG, polynomials suffice*
Concrete component:

Level-4 SoS relaxation certifies small-set expansion of long-code graph

long-code graph

\[ G = \text{Cay}(\mathbb{F}_2^m, T) \] where \( T = \{ \text{points with Hamming weight } \varepsilon m \} \]
Small-Set Expansion (SSE)

Given: regular graph $G$ with vertex set $V$, parameter $\delta > 0$

Find: function $f \in \mathbb{R}^V$

- $\max \langle f, Gf \rangle$
- $f^2 = f$
- $\mathbf{E} f \leq \delta$

Hypercontractivity implies SSE

$P = \text{projector into span of eigenfunctions of } G \text{ with eigenvalue } \geq \lambda$

Suppose $\|P\|_{2 \rightarrow 4} \ll 1/\delta^{1/4}$ and $f$ is an optimal SSE solution.

Since $\|f\|_4/\|f\|_2 \geq \delta^{-1/4} \gg \|P\|_{2 \rightarrow 4}$, function $f$ is far from $\text{image}(P)$

Hence, $\langle f, Gf \rangle \leq (\lambda + o(1))\|f\|_2^2 \approx \lambda \cdot \delta$
\[ G = \text{long-code graph \text{Cay}(\mathbb{F}_2^m, T)} \text{ where } T = \{\text{points with Hamming weight } \epsilon m\} \]

\[ P = \text{projector into span of eigenfunctions of } G \text{ with eigenvalue } \geq \lambda = 0.1 \]

*SoS proof of hypercontractivity:*

\[
2^{O(1/\epsilon)} \|f\|_2^4 - \|Pf\|_4^4 \text{ is a sum of squares}
\]
\( G = \text{long-code graph} \ \text{Cay}(\mathbb{F}^m_2, T) \text{ where } T = \{\text{points with Hamming weight } \varepsilon m\} \)

\( P = \text{projector into span of eigenfunctions of } G \text{ with eigenvalue } \lambda \geq 0.1 \)

\textit{SoS proof of hypercontractivity:}

\[ \|Pf\|_4^4 \leq 2^{O(1/\varepsilon)}\|f\|_2^4 \]

\text{difference is sum of squares}

For long-code graph, \( P \) projects into \textit{Fourier polynomials} with degree \( O(1/\varepsilon) \)

\textbf{Stronger ind. Hyp.:}

\[ \mathbb{E} f^2 g^2 \leq 3^{d+e} \mathbb{E} f^2 \cdot \mathbb{E} g^2 \]

where \( f \) is a generic degree-\( d \) Fourier polynomial and \( g \) is a generic degree-\( e \) Fourier polynomial

\[ \mathbb{E} f^2 = \sum_{S, |S| \leq d} \hat{f}_S^2 \]
G = long-code graph Cay($\mathbb{F}_2^m, T$) where $T = \{\text{points with Hamming weight } \varepsilon m\}$

$P = \text{projector into span of eigenfunctions of } G \text{ with eigenvalue } \geq \lambda = 0.1$

SoS proof of hypercontractivity:

$$\|Pf\|_4^4 \lesssim 2^{O(1/\varepsilon)}\|f\|_2^4$$

For long-code graph, $P$ projects into *Fourier polynomials* with degree $O(1/\varepsilon)$

Stronger ind. Hyp.:

$$\mathbb{E} f^2 g^2 \lesssim 3^{d+e} \mathbb{E} f^2 \cdot \mathbb{E} g^2$$

where $f$ is a generic degree-$d$ Fourier polynomial and $g$ is a generic degree-$e$ Fourier polynomial

Write $f = f_0 + x_1 \cdot f_1$ and $g = g_0 + x_1 \cdot g_1$ (degrees of $f_1, g_1$ smaller than $d, e$)

$$\mathbb{E} f^2 g^2 = \mathbb{E} f_0^2 g_0^2 + \mathbb{E} f_1^2 g_0^2 + \mathbb{E} f_0^2 g_1^2 + \mathbb{E} f_1^2 g_1^2 + 4\mathbb{E} f_0 f_1 g_0 g_1 + 2\mathbb{E} f_0^2 g_1^2 + 2\mathbb{E} f_1^2 g_0^2$$

$$\lesssim \ldots$$

$$\lesssim 3^{d+e} (\mathbb{E} f_0^2 + \mathbb{E} f_1^2) \cdot (\mathbb{E} g_0^2 + \mathbb{E} g_1^2)$$

(ind. hyp.)
Let $P$ be projector into $d$ dimensional subspace of functions $f: V \to \mathbb{R}$

In time $\exp O(n^2/q)$, can distinguish $\|P\|_{2\to q} = O(1)$ and $\|P\|_{2\to q} \gg 1$

**Algorithm**

Enumerate subspace if dimension $< O(n^2/q)$

Otherwise, project standard basis vectors into the subspace and pick best

**Analysis**

\[
\text{Tr } P = d
\]

\[
\text{Tr } P = \sum_i (P1_i)_i \leq \sum_i \|P1_i\|_{\infty}
\]

\[
\text{Tr } P = n \cdot \sum_i \|P1_i\|_2^2
\]

Finally, use $\|P1_i\|_q \geq \|P1_i\|_{\infty}/n^q$
Summary

Level-8 of SoS hierarchy refutes all known UG instances
show soundness via SoS proof

New connections between hypercontractivity & small-set expansion
and between ... & quantum separability

Open Problems

New UG instances from 2-to-4 norm hardness?
Stronger hardness for 2-to-4 norms?
Show that level-8 of SoS hierarchy solves all UG instances!

Thank you!