separable states, unique games and monogamy

Aram Harrow (MIT)

TQC 2013
arXiv:1205.4484

<u>based on work with</u>

Boaz Barak (Microsoft)
Fernando Brandão (UCL)
Jon Kelner (MIT)
David Steurer (Cornell)
Yuan Zhou (CMU)

motivation:

approximation problems with intermediate complexity

1. **Unique Games (UG):**
   Given a system of linear equations: $x_i - x_j = a_{ij} \bmod k$.
   Determine whether $\geq 1-\epsilon$ or $\leq \epsilon$ fraction are satisfiable.

2. **Small-Set Expansion (SSE):**
   Is the minimum expansion of a set with $\leq \delta n$ vertices
   $\geq 1-\epsilon$ or $\leq \epsilon$?

3. **2->4 norm:**
   Given $A \in \mathbb{R}^{m \times n}$. Define $\|x\|_p := (\Sigma_i |x_i|^p)^{1/p}$
   Approximate $\|A\|_{2\to4} := \sup_x \|Ax\|_4 / \|x\|_2$

4. **h_{Sep}:**
   Given M with $0 \leq M \leq I$ acting on $C^n \otimes C^n$, estimate $h_{Sep}(M) = \max\{\mathrm{tr}\, M\rho : \rho \in \mathrm{Sep}\}$

5. **weak membership for Sep:** Given ρ such that either
   $\rho \in \mathrm{Sep}$ or $\mathrm{dist}(\rho, \mathrm{Sep}) > \varepsilon$, determine which is the case.

unique games motivation

CSP = constraint satisfaction problem

Example: MAX-CUT

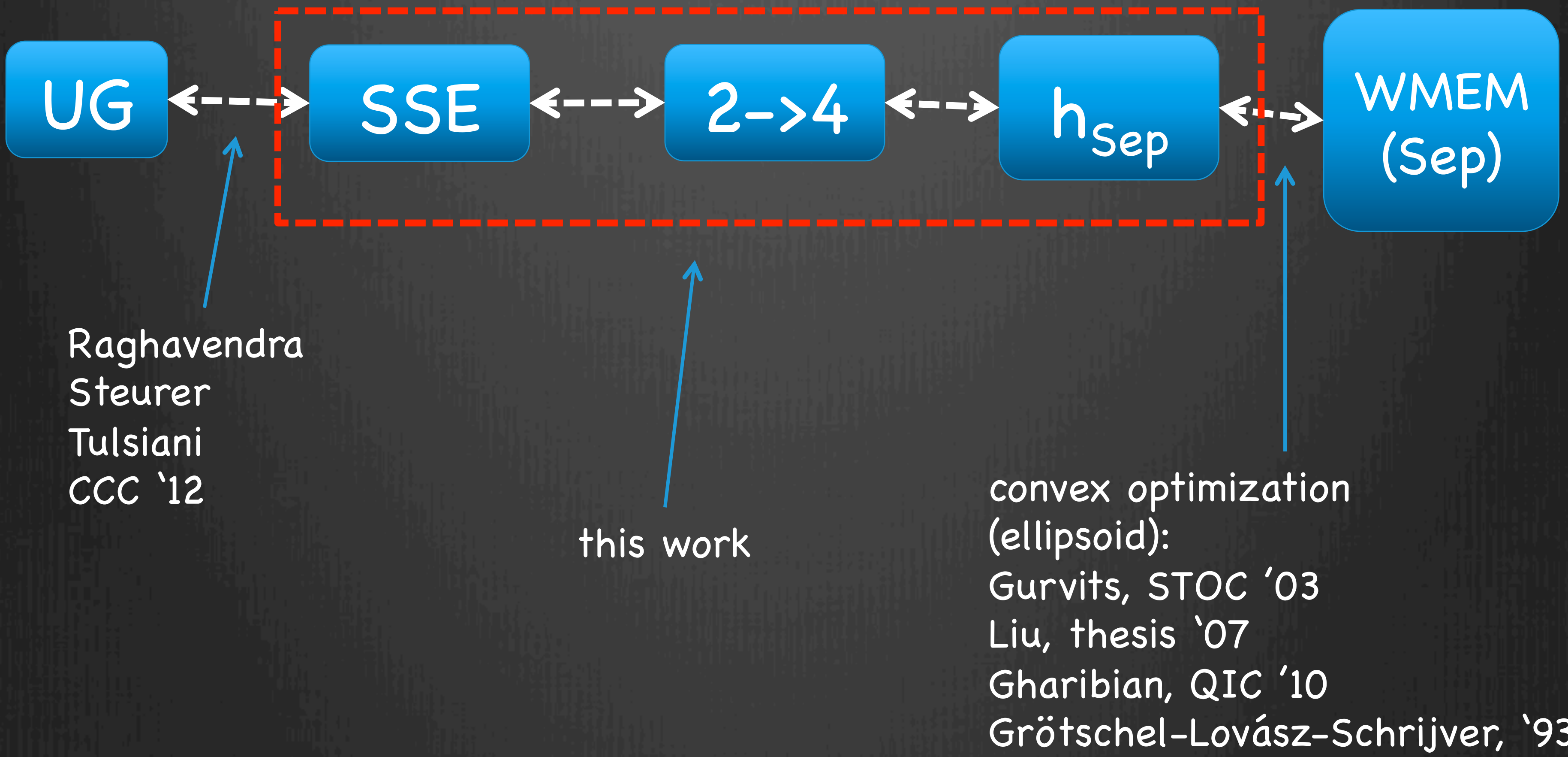
- trivial algorithm achieves ½-approximation
- SDP achieves 0.878…-approximation
- NP-hard to achieve 0.941…-approximation

If UG is NP-complete, then 0.878… is optimal!

Theorem: [Raghavendra '08]
If the unique games problem is NP-complete, then for every CSP, $\exists\ \alpha > 0$ such that

- an α-approximation is achievable in poly time using SDP
- it is NP-hard to achieve a $\alpha + \varepsilon$ approximation

TFA≈E


UG
SSE
2->4
h_{Sep}
WMEM (Sep)
Raghavendra
Steurer
Tulsiani
CCC '12
this work
convex optimization
(ellipsoid):
Gurvits, STOC '03
Liu, thesis '07
Gharibian, QIC '10
Grötschel-Lovász-Schrijver, '93

the dream

SSE <---> 2->4 <---> h_{Sep}

hardness

algorithms

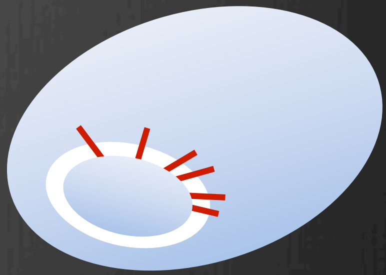
...quasipolynomial (=exp(polylog(n)) upper and lower bounds for unique games

progress so far

small-set expansion (SSE) ≈ 2->4 norm

G = normalized adjacency matrix

$P_{\geq \lambda}$ = largest projector s.t. $G \geq \lambda P$



Theorem:

All sets of volume $\leq \delta$ have expansion $\geq 1 - \lambda^{O(1)}$

iff

$\|P_{\geq \lambda}\|_{2\to 4} \leq n^{-1/4} / \delta^{O(1)}$

Definitions

volume = fraction of vertices weighted by degree

expansion of set S = Pr [e leaves S | e has endpoint in S]

2->4 norm ≈ h_{Sep}

$$A = \sum_{i=1}^{m} |i\rangle \langle a_i|$$

$$M = \sum_i |a_i\rangle\langle a_i| \otimes |a_i\rangle\langle a_i|$$

Easy direction:

h_{Sep} ≥ 2->4 norm

$$\|Ax\|_4^4 = \sum_i \langle a_i, x\rangle^4 = \mathrm{tr} M \rho$$

$$\rho = |x\rangle\langle x| \otimes |x\rangle\langle x|$$

$$\|A\|_{2\to 4}^4 = h_{\mathrm{Sep}}(M)$$

Harder direction:

2->4 norm ≥ h_{Sep}

Given an arbitrary M, can we make it look like $\sum_i |a_i\rangle\langle a_i| \otimes |a_i\rangle\langle a_i|$?

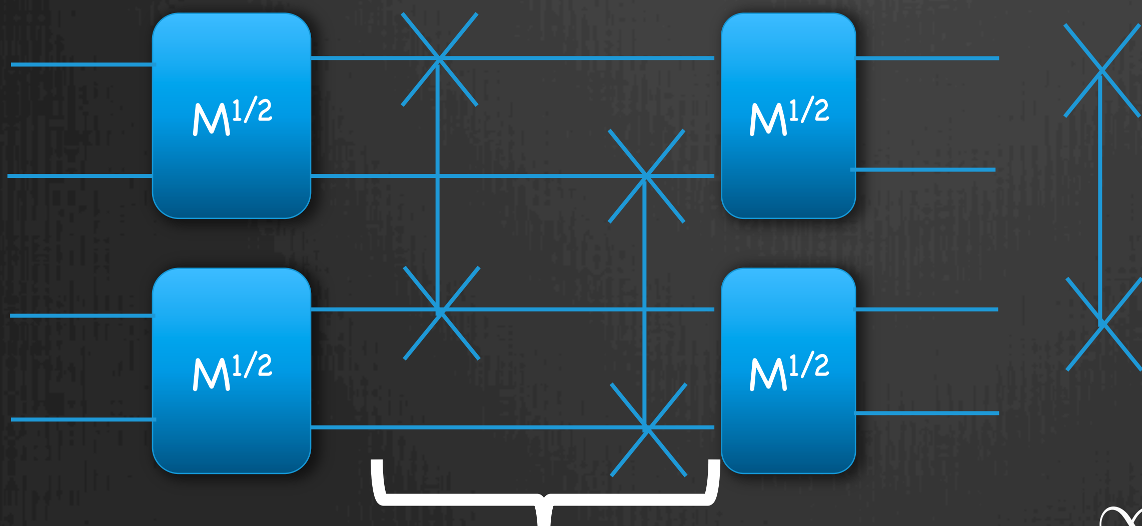
reduction from h_{Sep} to 2->4 norm

Goal:

Convert any $M \geq 0$ into the form $\sum_i |a_i\rangle\langle a_i| \otimes |a_i\rangle\langle a_i|$ while approximately preserving $h_{Sep}(M)$.

Construction: [H.-Montanaro, 1001.0017]

- Amplify so that $h_{Sep}(M)$ is ≈ 1 or $\ll 1$.
- Let $|a_i\rangle = M^{1/2}(|\phi\rangle \otimes |\phi\rangle)$ for Haar-random $|\phi\rangle$.



swap tests

$$= \frac{I + F}{2}$$

= "swap test"

$$\propto \mathbb{E}_\phi |\phi\rangle\langle\phi| \otimes |\phi\rangle\langle\phi|$$

SSE hardness??

1. Estimating $h_{Sep}(M) \pm 0.1$ for n-dimensional M is at least as hard as solving 3-SAT instance of length $\approx\log^2(n)$.
[H.-Montanaro 1001.0017] [Aaronson-Beigi-Drucker-Fefferman-Shor 0804.0802]

2. The Exponential-Time Hypothesis (ETH) implies a lower bound of $\Omega(n^{\log(n)})$ for $h_{Sep}(M)$.

3. ∴ lower bound of $\Omega(n^{\log(n)})$ for estimating $||A||_{2\to 4}$ for some family of projectors A.

4. These A might not be $P_{\geq\lambda}$ for any graph G.

5. (Still, first proof of hardness for constant-factor approximation of $||\cdot||_{2\to 4}$).

algorithms:
semi-definite programming (SDP) hierarchies

[Parrilo '00; Lasserre '01]

Problem:

Maximize a polynomial f(x) over $x \in \mathbb{R}^n$ subject to polynomial constraints $g_1(x) \geq 0, \ldots, g_m(x) \geq 0$.

SDP:

Optimize over "pseudo-expectations" of k'th-order moments of x.
Run-time is $n^{O(k)}$.

$$\tilde{\mathbb{E}}[p(x) + q(x)] = \tilde{\mathbb{E}}[p(x)] + \tilde{\mathbb{E}}[q(x)]$$

$$\tilde{\mathbb{E}}[p(x)^2] \geq 0$$

Dual:

min λ s.t. $\lambda - f(x) = r_0(x) + r_1(x)g_1(x) + \ldots + r_m(x)g_m(x)$
and $r_0, \ldots, r_m$ are SOS (sums of squares).

SDP hierarchy for Sep

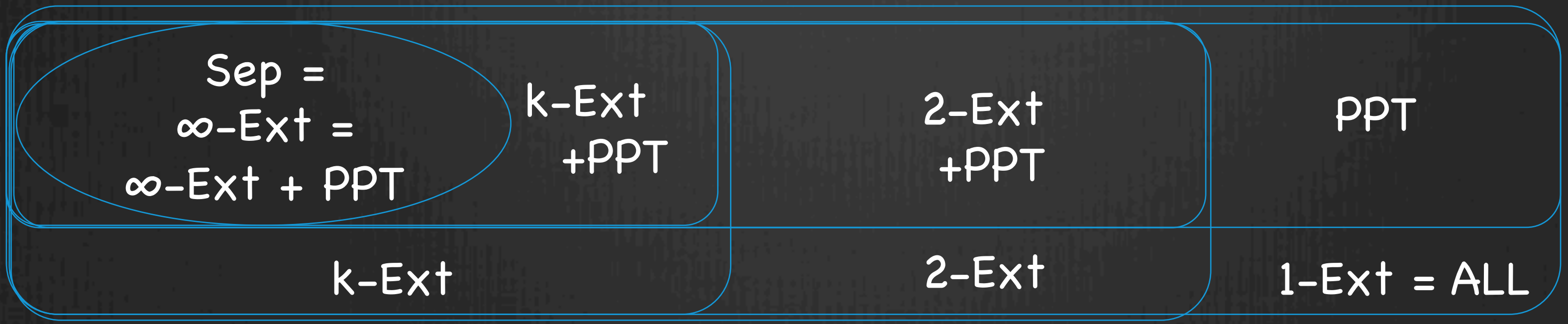
Relax $\rho^{AB} \in$ Sep to

1. $\tilde{\rho}^{A_1 \ldots A_k B_1 \ldots B_k}$ symmetric under permuting $A_1, \ldots, A_k, B_1, \ldots, B_k$ and partial transposes.

2. require $\rho^{AB} = \tilde{\rho}^{A_i B_j}$ for each i,j.

Lazier versions

1. Only use systems $AB_1 \ldots B_k$. → "k-extendable + PPT" relaxation.
2. Drop PPT requirement. → "k-extendable" relaxation.



the dream: quantum proofs for classical algorithms

1. Information-theory proofs of de Finetti/monogamy, e.g. [Brandão-Christandl-Yard, 1010.1750] [Brandão-H., 1210.6367]
   $h_{Sep}(M) \leq h_{k\text{-}Ext}(M) \leq h_{Sep}(M) + (\log(n) / k)^{1/2} \|M\|$
   if $M \in$ 1-LOCC

2. $M = \sum_i |a_i\rangle\langle a_i| \otimes |a_i\rangle\langle a_i|$ is $\propto$ 1-LOCC.

3. Constant-factor approximation in time $n^{O(\log(n))}$?

4. Problem: $\|M\|$ can be $\gg h_{Sep}(M)$. Need multiplicative approximaton.
   Also: implementing M via 1-LOCC loses dim factors

5. Still yields subexponential-time algorithm.

the way forward

conjectures → hardness

Currently approximating $h_{Sep}(M)$ is at least as hard as 3-SAT[$\log^2(n)$] for M of the form $M = \Sigma_i |a_i\rangle\langle a_i| \otimes |a_i\rangle\langle a_i|$.

Can we extend this so that $|a_i\rangle = P_{\geq\lambda}|i\rangle$ for $P_{\geq\lambda}$ a projector onto the $\geq\lambda$ eigenspace of some symmetric stochastic matrix?

Or can we reduce the 2->4 norm of a general matrix A to SSE of some graph G?

Would yield $n^{\Omega(\log(n))}$ lower bound for SSE and UG.

conjectures → algorithms

Goal: $M = (P_{\geq\lambda} \otimes P_{\geq\lambda})^\dagger \sum_i |i\rangle\langle i| \otimes |i\rangle\langle i| (P_{\geq\lambda} \otimes P_{\geq\lambda})$
Decide whether $h_{Sep}(M)$ is $\geq 1000/n$ or $\leq 10/n$.

Known: [BCY]
can achieve error $\varepsilon \lambda$ in time $\exp(\log^2(n)/\varepsilon^2)$ where
$\lambda = \min \{\lambda : M \leq \lambda N$ for some 1-LOCC $N\}$

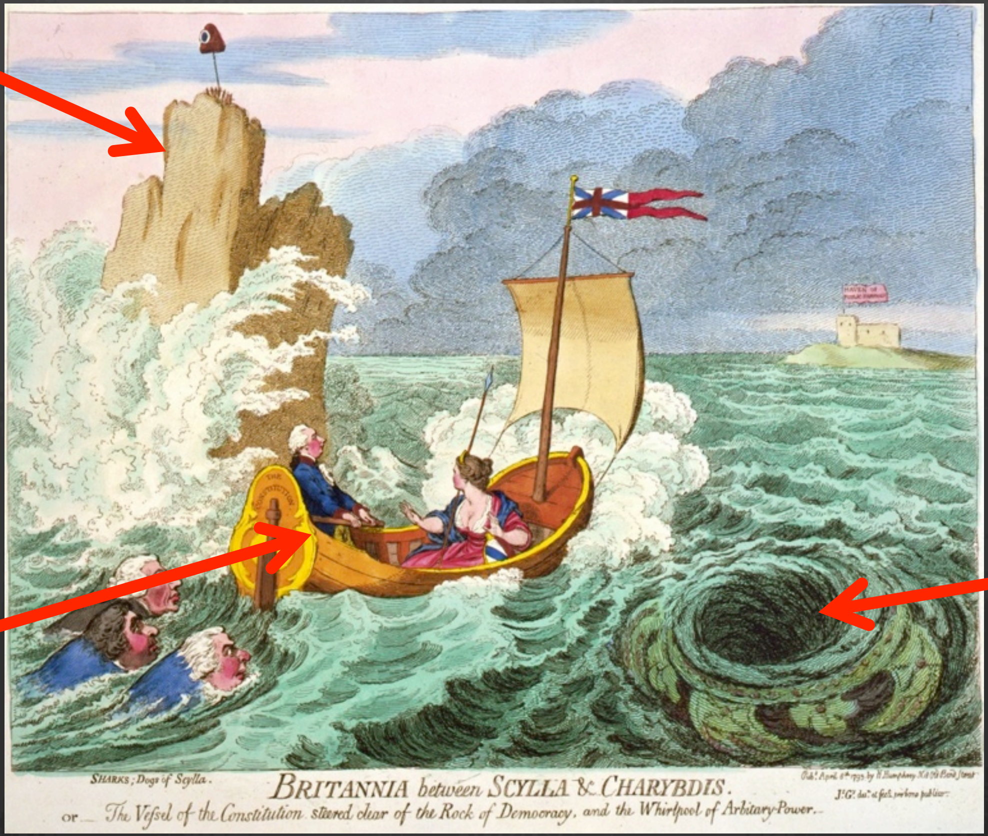
Improvements?
1. Remove 1-LOCC restriction: replace λ with $||M||$
2. Multiplicative approximation: replace λ with $h_{Sep}(M)$.

Multiplicative approximation would yield $n^{O(\log(n))}$–time algorithm for SSE and (sort of) UG.

difficulties

Antisymmetric state on $C^n \otimes C^n$ (a.k.a. "the universal counter-example")

- (n-1)-extendable
- far from Sep
- although only with non-PPT measurements
- also, not PPT



Analyzing the k-extendable relaxation using monogamy

"Near-optimal and explicit Bell inequality violations" [Buhrman, Regev, Scarpa, de Wolf 1012.5043]

- $M \in LO$
- based on UG

$$\frac{h_{k-\mathrm{Ext}}(M)}{h_{\mathrm{Sep}}(M)} \gtrsim \frac{n}{k \log^2(n)}$$

room for hope?

Improvements?

1. Remove 1-LOCC restriction: replace λ with $\min\{\lambda : M \leq \lambda N, N \in SEP\}$
2. Multiplicative approximation: replace λ with $h_{Sep}(M)$.

1. Note: $\lambda = ||M||$ won't work because of antisymmetric counterexample

Need:

a) To change 1-LOCC to SEP in the BCY bound.
b) To hope that $||M||$ is not too much bigger than $h_{sep}(M)$ in relevant cases.

2. Impossible in general without PPT (because of Buhrman et al. example)

Only one positive result for k-Ext + PPT.

[Navascues, Owari, Plenio. 0906.2731]

trace dist(k-Ext, Sep) ~ n/k

trace dist(k-Ext+PPT, Sep) ~ $(n/k)^2$

more open questions

- What is the status of QMA vs QMA(k) for k = 2 or poly(n)?
  Improving BCY from 1-LOCC to SEP would show QMA = QMA(poly).
  Note that QMA = BellQMA(poly) [Brandão-H. 1210.6367]

- How do monogamy relations differ between entangled states and general no-signaling boxes?
  (cf. 1210.6367 for connection to NEXP vs MIP*)

- More counter-example states.

- What does it mean when $I(A:B|E) = \varepsilon$?
  Does it imply $O(1/\varepsilon)$-extendability?