LEONID GURVITS
(LOS ALAMOS NAT. LAB,
gurvits@LANL.GOV)

CLASSICAL COMPLEXITY
AND
BIPARTITE ENTANGLEMENT.

Topics.

1. Geometry of a convex compact set of separable bipartite quantum states.

2. NP-hardness of weak membership problem for $N \times M$ separability ($N \le M \le 2 + \binom{N}{2}$)

3. Derandomization of checking polynomial identities (symbolic determinants) and quantum entanglement.

3.a Quantum permanent....

$\rho_{A,B} : H_A \otimes H_B \to H_A \otimes H_B, \quad \rho_{A,B} \geq 0.$

PRODUCT STATES $\rho_A \otimes \rho_B$,

SEPARABLE = CONE { PRODUCT STATES }

$\downarrow$

$\rho_{A,B} = \sum \alpha_i Q_i \otimes P_i, \quad \alpha_i \geq 0.$

$\downarrow$ (NORMALIZATION OF TRACE)

$$\left\{ \rho_{A,B} = \sum \alpha_i Q_i \otimes P_i, \ \alpha_i \geq 0, \ \sum \alpha_i = 1, \ \mathrm{tr}\, Q_i = 1, \ \mathrm{tr}\, P_i = 1 \right\}$$

$\downarrow$

COMPACT CONVEX SET WITH NONEMPTY INTERIOUR.

METRICS

$$\|\rho_1-\rho_2\|_p = \left(\operatorname{tr}|\rho_1-\rho_2|^p\right)^{\frac{1}{p}}, \quad p \geq 1.$$

Assume "WLOG" that $\dim H_A = \dim H_B = N$.

Question:

? $\max\{R : B_p(I, R) \subset \text{Separable}\} = R(N,p)$

answer

Theorem (2002; Gurvits, Barnum, PRA coming)

$$R(N,p) = \begin{cases} 1, & 1 \leq p \leq 2 \\ N^{\frac{2}{p}-1}, & 2 \leq p < \infty. \end{cases}$$

Cor. 1. $\rho_{A,B} : H_A \otimes H_B \to H_A \otimes H_B$; $\rho \geq 0$, $\operatorname{tr}\rho = 1$.

$D = \dim H_A \cdot \dim H_B$

if purity $\operatorname{tr}\rho^2 \leq \frac{1}{d-1}$ then ρ is separable.

Cor. 2. $(1-\varepsilon)\frac{I}{D} + \varepsilon\rho$ is separable

if $\varepsilon \leq \frac{1}{d-1}$ (ρ is pure).

(even a bit up)

OR 3. $I + a\rho$ is separable if

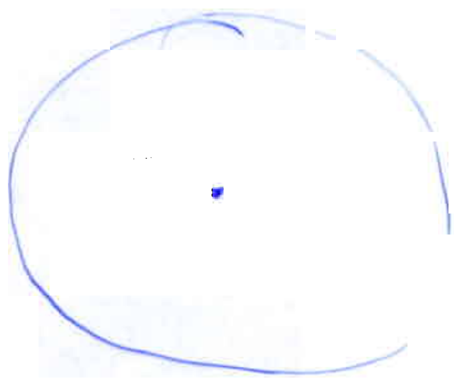
$$-1 \le a \le \frac{D}{D-2}.$$

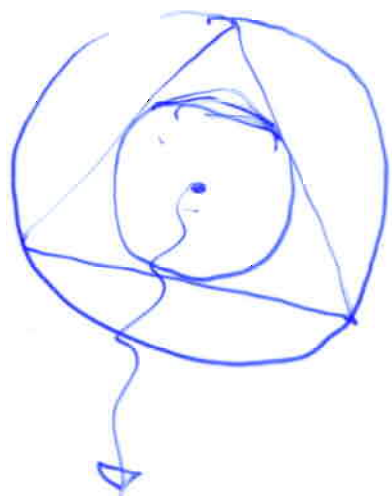
⋮

OR. 4. Largest 2-ball for normalized bipartite $D = N \times M$ states:

$$\boxed{\text{inner radius} = \frac{1}{\sqrt{D(D-1)}}}$$

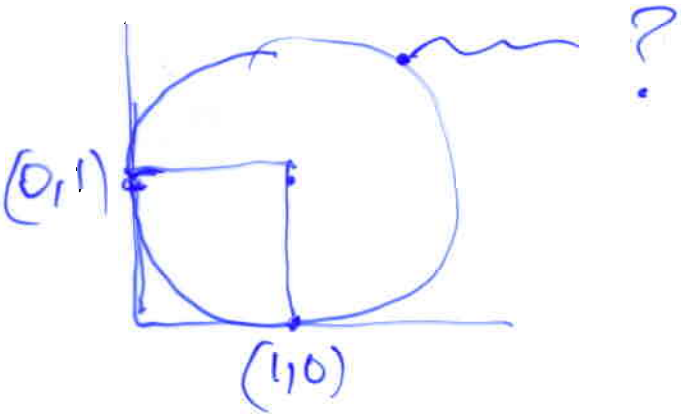
$$\text{outer radius} = \sqrt{\frac{D-1}{D}}$$





$\frac{1}{D} I$

One comment.



yes.

$\rho = I + \Delta$,

$\sigma(\Delta) \in \{\pm \frac{1}{N}\}$,

$\# +1 = \frac{N(N-1)}{2}$ $\rightarrow$ Don't know in which basis, existence result.

$\# -1 = \frac{N(N+1)}{2}$

(2.1.11) The Weak Violation Problem (WVIOL).

Given a vector $c \in \mathbb{Q}^n$, a rational number γ, and a rational number $\varepsilon > 0$, either

(i) *assert that $c^T x \le \gamma + \varepsilon$ for all $x \in S(K, -\varepsilon)$*
(i. e., $c^T x \le \gamma$ is almost valid), *or*

(ii) *find a vector $y \in S(K, \varepsilon)$ with $c^T y \ge \gamma - \varepsilon$*
(a vector almost violating $c^T x \le \gamma$).

(2.1.12) The Weak Validity Problem (WVAL).

Given a vector $c \in \mathbb{Q}^n$, a rational number γ, and a rational number $\varepsilon > 0$, either

(i) *assert that $c^T x \le \gamma + \varepsilon$ for all $x \in S(K, -\varepsilon)$, or*

(ii) *assert that $c^T x \ge \gamma - \varepsilon$ for some $x \in S(K, \varepsilon)$*
(i. e., $c^T x \le \gamma$ is almost nonvalid).

(2.1.13) The Weak Separation Problem (WSEP).

Given a vector $y \in \mathbb{Q}^n$ and a rational number $\delta > 0$, either

(i) *assert that $y \in S(K, \delta)$, or*

(ii) *find a vector $c \in \mathbb{Q}^n$ with $\|c\|_\infty = 1$ such that $c^T x \le c^T y + \delta$ for every $x \in S(K, -\delta)$*
(i. e., find an almost separating hyperplane).

(2.1.14) The Weak Membership Problem (WMEM).

Given a vector $y \in \mathbb{Q}^n$ and a rational number $\delta > 0$, either

(i) *assert that $y \in S(K, \delta)$, or*

(ii) *assert that $y \notin S(K, -\delta)$.*

Similarly as in the strong version SVIOL (2.1.2), the special case of (2.1.11) where $c = 0$ and $\gamma = -1$ is of particular importance. Note, however, that (for $\varepsilon < 1$) output (i) of WVIOL only means that $S(K, -\varepsilon)$ is empty (K might still be nonempty) and output (ii) means finding a point almost in K. We call this special case of WVIOL the **weak nonemptiness problem (WNEMPT)**.

n-DIMENSIONAL CENTERED CONVEX SET

$K \subset R^n$, $\mathring{K} \neq \emptyset$.

$\exists\, a_0$ SUCH THAT $B(a_0, r) \subset K$ AND $B(0, R) \supset K$.

COMPLEXITY OF CENTERED K

$$\langle K \rangle = \langle a_0 \rangle + n + \underbrace{\langle r \rangle}_{\text{inner radius}} + \underbrace{\langle R \rangle}_{\text{outer radius}}$$

The main point is that the complexity of a convex set of separable density matrices is Poly (MN). $\rightarrow$ $n = D-1 = M \cdot N - 1$.

$$\langle sep \rangle = \langle \tfrac{1}{D} I \rangle + D-1 + \langle \tfrac{1}{D-1} \rangle + \langle 1 \rangle .$$

$S(K, \varepsilon) \rightarrow \varepsilon$-neighborhood of K,
(ε-approximated by separable)
$S(K, -\varepsilon) = \{x : x \in K$ and $B(x, \varepsilon) \in K\}$
(in our context,
$\rho \notin S(K, -\varepsilon) \Longleftrightarrow$ ε-approximated by entangled).

Main fact:

Weak membership problem:
Given ρ (rational) and rational ε
To assert
(yes) that ρ is ε-separable ($\rho \in S(K, +\varepsilon)$)
or
(no) that ρ is ε-entangled. ($\rho \notin S(K, -\varepsilon)$)

WMEM(K, ρ, ε).

Weak optimization (roughly) $\rightarrow$ WOPT(C, K, ε).
$$\min_{x \in K} \langle c, X \rangle = \cancel{t} \pm \varepsilon$$

(YUDIN-NEMIROVSKII, 1976)

IF WMEM(K, ρ, ε) can be done in poly$(\langle K\rangle, \langle \rho\rangle, \langle \varepsilon\rangle)$

Then WOPT also can be done in poly$(\langle K\rangle, \langle c\rangle, \langle \varepsilon\rangle)$.

We know that $\langle K\rangle$ is poly$(n \cdot m,$

$$C = \begin{bmatrix} 0 & A_1 & \cdots & A_k \\ A_1 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 \\ & \vdots & & & \\ A_k & 0 & 0 & & 0 \end{bmatrix},$$

A_i are $m \times m$ real symmetric matrices,

$$\max_{\rho \in Sep} \cancel{tr}(C \cdot \rho) = \left(\max_{\substack{x \in R^m, \\ \|x\|=1}} \sum_{i=1}^{k} (A_i x, x)^2\right)^{\frac{1}{2}}$$

what we have:

$$\max_{\substack{x\in\mathbb{R}^m,\\ \|x\|=1}} \sum_{i=1}^{k} (A_i x, x)^2 \quad \text{with } \varepsilon\text{-accuracy},$$

in Poly$(\sum\langle A_i\rangle, \langle\varepsilon\rangle, m\cdot k)$.

Hardness prove in
[Ben Tal, Nemirovskii, 1998],

$$k = \frac{m(m-1)}{2} + 1 \Longleftarrow \text{knapsack (max-cut)}.$$

$$\Downarrow$$

$$\{x_i x_j,\ i<j\},\quad I - \frac{aa^T}{1+\langle a,a\rangle}$$

$$\Downarrow$$

$$\sum_{i<j} x_i^2 x_j^2 + \left(m - \frac{\langle a,x\rangle^2}{1+\langle a,a\rangle}\right)^2 = f(x)$$

if $\exists \pm 1$ x with $\langle a,x\rangle=0$ then $\max\limits_{\|x\|=1} f(x) = \binom{m}{2} + m^2$,

otherwise $\max\limits_{\|x\|=1} f(x) \le \binom{m}{2} + m^2 - \text{Poly}\left(\frac{1}{m\|a\|^2}\right)$.

Density matrices $\longleftrightarrow$ C-P operators | S 0

$\rho_{A,B} : C^N \otimes C^N \to C^N \otimes C^N$

$$\rho_{A,B} = \begin{bmatrix} \boxed{A_{1,1}} & & \boxed{A_{1,N}} \\ & \boxed{A_{i,j}} & \\ & & \end{bmatrix} \succeq 0$$

$A_{i,j}$ are $N \times N$ matrices

$T : M(N) \to M(N)$:

$T(X) = \sum X(i,j) A_{i,j}$ $\quad \vert \to A_{i,j} = T(e_i e_j^+)$

$T^* \to$ Dual respect to $\langle X, Y \rangle = \operatorname{tr} X Y^+$.

$T^*(X) = \{ \operatorname{tr}(A_{i,j} \cdot X) \}$.

T is entanglement breaking iff

$\left[\; T(e_i e_j^+) \; \right]$ is separable.

Relative invariant

$\varphi(C \otimes D \, \rho_{A,B} \, C^+ \otimes D^+) = |\operatorname{Det} C|^2 \cdot |\operatorname{Det} D|^2 \cdot \varphi(\rho_{A,B})$.

T is DOUBLY STOCHASTIC (UNITAL) | 500

IF $T(I) = I$ AND $T^*(I) = I$.

$$DS(T) = tr(T(I) - I)^2 + tr(T^*(I) - I)^2.$$

$$C \otimes D \; \rho_{A,B} \; C^+ \otimes D^+$$ (local operations)

$$\Updownarrow$$

$$T'(X) = C \, T(D^+ X D) \, C^+$$

PROBLEM

LOCAL ORBIT $(\rho_{A,B}) \ni$ DOUBLY STOCHASTIC?

(WHAT IS A CORRESPONDING RELATIVE INVARIANT, i.e. $\exists$ DOUBLY STOCHASTIC IN THE LOCAL ORBIT iff

$\varphi(\rho_{A,B}) > 0$ (ANALOG OF THE PERMANENT).

CLASSICAL ANALOG

$$A = (a_{ij} \geq 0)$$

ORBIT $\{ Diag_1 A \, Diag_2 \}$, $Diag_1, Diag_2 > 0$

QUESTION $\overline{\{Diag_1 A Diag_2\}} \ni$ DOUBLY-STOCHASTIC.

RESULT: iff $Per(A) > 0$.

One ALGORITHM (SINKHORN'S SCALING).

$$R(A) = Diag(r_1^{-1}, \ldots r_N^{-1}) A \rightarrow \quad Ae = e$$

$$C(A) = A \, Diag(c_1^{-1}, \ldots c_N^{-1}) \longrightarrow \quad A^T e = e.$$

Operator analog:

$$R(T) = T', \quad T'(X) = T(I)^{-\frac{1}{2}} T(X) T(I)^{-\frac{1}{2}} \rightarrow T(I) = I$$

$$C(T) = T'', \quad T''(X) = T(T^*(I)^{-\frac{1}{2}} X \, T^*(I)^{-\frac{1}{2}}) \rightarrow T^*(I) = I.$$

ALGORITTHMS:

$\ldots CRCR(A) \Rightarrow$ CONVERGES TO DOUBLY-STOCHASTIC

$\ldots CRCR(T) \longrightarrow$? AND HOW FAST.

(MORE COMPLICATED MARGINALS/TRACES)

$(12)(23)\cdots(N-1,N) \longrightarrow$ ALREADY DIFFERENT IN "QUANTUM"

SYMBOLIC DETERMINANTS AND BIPARTITE ENTANGLEMENT.

QUESTION

$$\mathrm{Det}\left(\sum_{i=1}^{k} x_i A_i\right) \equiv 0 \,?$$

$A_i \in M(N)$ ($N \times N$ MATRICES).

OR: GIVEN A LINEAR SUBSPACE $X \subset M(N)$.
DOES THERE EXIST A NONSINGULAR MATRIX $A \in X$.

OR: GIVEN $\rho_{A,B} : C^N \otimes C^N \to C^N \otimes C^N$.
$C^N \otimes C^N \cong M(N)$.
DOES IMAGE $\rho_{A,B}$ CONTAIN A NONSINGULAR MATRIX?

$$\left(\rho_{A,B} = \sum |A_i\rangle\langle A_i|\right)$$

The problem is in BPP.

Example

$$\mathrm{Det}\begin{bmatrix} 0 & 0 & x_{ij} & 0 \\ & 6 & & \\ x_{kl} & & & 0 \end{bmatrix} \equiv ?$$

$\downarrow$

perfect matchings (in P).

More complicated:

$A_{i} = x_i y_j^{+} \rightarrow$ intersection of

two geometric matroids:

$\exists\ 1 \le i_1 < i_2 \cdots < i_k \le K$ s.t.

$\mathrm{Det}[X_{i_1} \cdots X_{i_k}] \neq 0$ in P.

and

$\mathrm{Det}[Y_{i_1} \cdots Y_{i_k}] \neq 0.$

$(\rho_{A,B} = \sum x_i x_i^{+} \otimes y_i y_i^{+} \rightarrow$ separable).

EDMONDS–RADO PROPERTY:

IF X DOES NOT CONTAIN A NONSINGULAR MATRIX THEN
$\exists$ TWO LINEAR SUBSPACES $Z_1, Z_2 \subset \mathbb{C}^n$
SUCH THAT $\dim Z_2 < \dim Z_1$
AND $A(Z_1) \subset Z_2$ FOR ALL $A \in X$.

THEOREM.

EDMONDS–RADO PROPERTY ALLOWS DETERMINISTIC POLY-TIME ALGORITHM.

IF LINEAR SUBSPACE $X \subset M(n)$ HAS "RANK-ONE" BASIS (SEPARABILITY) THEN HAS EDMONDS–RADO PROPERTY.

SUPPOSE THAT $M(n) \supset X = \mathrm{Span}(A_1, \ldots A_k)$
$$N(L) \supset Y = \mathrm{Span}(B_1, \ldots B_k)$$

DEFINE $Z \in M(n+L)$,
$$Z = \mathrm{Span}\left(\begin{pmatrix} A_1 & * \\ 0 & B_1 \end{pmatrix}, \ldots, \begin{pmatrix} A_k & * \\ 0 & B_k \end{pmatrix}\right).$$

THEN IF X, Y HAVING EDMONDS–RADO PROP., THEN Z ALSO HAS.

The "WORST" ENTANGLED:
Does not have Edmonds-Rado property.

Example

$X \subset M(3) = \{$ all skew-symmetric matrices $\}$.

How it works.

$X = \mathrm{Span}\{A_1, \ldots, A_k\}$.

CP operator

$$T(X) = \sum_{i=1}^{k} A_i X A_i^{*}.$$

T is rank non-decreasing

if $\mathrm{Rank}\, T(X) \geq \mathrm{Rank}(X)$, $X \succeq 0$