Lower bounds for combinatorial polytopes, inspired by quantum communication complexity

Ronald de Wolf

CWI Centrum Wiskunde & Informatica

Universiteit van Amsterdam

Joint with Samuel Fiorini (ULB), Serge Massar (ULB),

Sebastian Pokutta (Erlangen), Hans Raj Tiwary (ULB)

Background: solving NP by LP?

Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)

Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)
- Famous **NP**-hard problem: traveling salesman problem

Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)
- Famous **NP**-hard problem: traveling salesman problem
- A polynomial-size LP for TSP would show **P** $=$ **NP**

Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)
- Famous **NP**-hard problem: traveling salesman problem
- A polynomial-size LP for TSP would show **P** $=$ **NP**
- Swart'86–87 claimed to have found such LPs

Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)
- Famous **NP**-hard problem: traveling salesman problem
- A polynomial-size LP for TSP would show **P** $=$ **NP**
- Swart'86–87 claimed to have found such LPs
- Yannakakis'88: symmetric LPs for TSP are exponential

Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)
- Famous **NP**-hard problem: traveling salesman problem
- A polynomial-size LP for TSP would show **P** $=$ **NP**
- Swart'86–87 claimed to have found such LPs
- Yannakakis'88: symmetric LPs for TSP are exponential
- Swart's LPs were symmetric, so they couldn't work

Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)
- Famous **NP**-hard problem: traveling salesman problem
- A polynomial-size LP for TSP would show **P** $=$ **NP**
- Swart'86–87 claimed to have found such LPs
- Yannakakis'88: symmetric LPs for TSP are exponential
- Swart's LPs were symmetric, so they couldn't work
- 20-year open problem: what about non-symmetric LP?

Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)
- Famous **NP**-hard problem: traveling salesman problem
- A polynomial-size LP for TSP would show **P** $=$ **NP**
- Swart'86–87 claimed to have found such LPs
- Yannakakis'88: symmetric LPs for TSP are exponential
- Swart's LPs were symmetric, so they couldn't work
- 20-year open problem: what about non-symmetric LP?
- Sometimes non-symmetry helps a lot! (Kaibel et al'10)

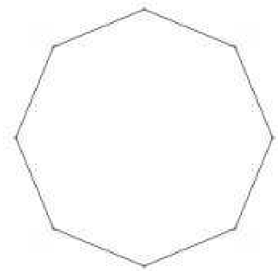
Background: solving NP by LP?

- Famous **P**-problem: linear programming (Khachian'79)
- Famous **NP**-hard problem: traveling salesman problem
- A polynomial-size LP for TSP would show **P** $=$ **NP**
- Swart'86–87 claimed to have found such LPs
- Yannakakis'88: symmetric LPs for TSP are exponential
- Swart's LPs were symmetric, so they couldn't work
- 20-year open problem: what about non-symmetric LP?
- Sometimes non-symmetry helps a lot! (Kaibel et al'10)
- Yannakakis, May 2011: "I believe in fact that it should be possible to prove that there is no polynomial-size formulation for the TSP polytope or any other NP-hard problem, although of course showing this remains a challenging task"

Basics of polytopes

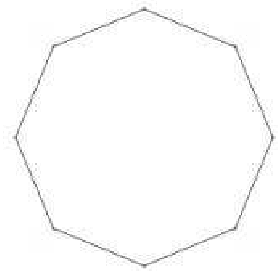
Basics of polytopes

- Polytope P: convex hull of finite set of points in $\mathbb{R}^d$



Basics of polytopes

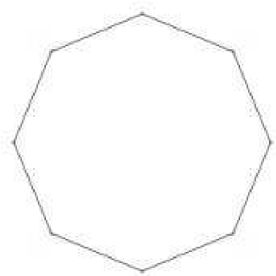
- Polytope P: convex hull of finite set of points in $\mathbb{R}^d$



$\Leftrightarrow$ bounded intersection of finitely many halfspaces

Basics of polytopes

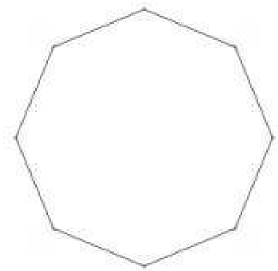
- Polytope P: convex hull of finite set of points in $\mathbb{R}^d$



  $\Leftrightarrow$ bounded intersection of finitely many halfspaces
- Can be written as system of linear inequalities:
  $P = \{x \in \mathbb{R}^d \mid Ax \leq b\}$

Basics of polytopes

- Polytope P: convex hull of finite set of points in $\mathbb{R}^d$

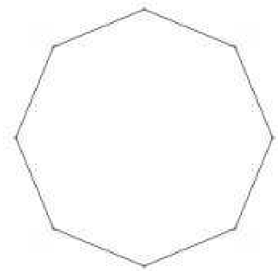


  $\Leftrightarrow$ bounded intersection of finitely many halfspaces

- Can be written as system of linear inequalities:
  $P = \{x \in \mathbb{R}^d \mid Ax \leq b\}$
  Different systems "$Ax \leq b$" can define the same P

Basics of polytopes

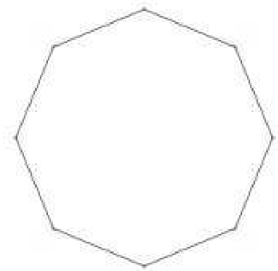
- Polytope P: convex hull of finite set of points in $\mathbb{R}^d$



  $\Leftrightarrow$ bounded intersection of finitely many halfspaces
- Can be written as system of linear inequalities:
  $P = \{x \in \mathbb{R}^d \mid Ax \leq b\}$
  Different systems "$Ax \leq b$" can define the same P
  The size of P is the minimal number of inequalities

Basics of polytopes

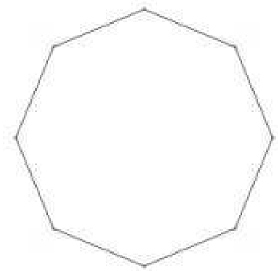
- Polytope P: convex hull of finite set of points in $\mathbb{R}^d$



  $\Leftrightarrow$ bounded intersection of finitely many halfspaces
- Can be written as system of linear inequalities:
  $P = \{x \in \mathbb{R}^d \mid Ax \leq b\}$
  Different systems "$Ax \leq b$" can define the same P
  The size of P is the minimal number of inequalities
- TSP polytope: convex hull of Hamiltonian cycles in K_n
  $P_{\text{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n \text{ is a tour of } K_n\}$

Basics of polytopes

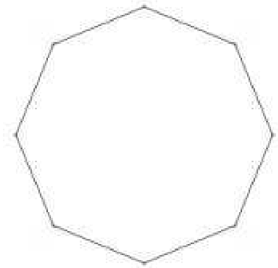
- Polytope P: convex hull of finite set of points in $\mathbb{R}^d$



  $\Leftrightarrow$ bounded intersection of finitely many halfspaces
- Can be written as system of linear inequalities:
  $P = \{x \in \mathbb{R}^d \mid Ax \leq b\}$
  Different systems "$Ax \leq b$" can define the same P
  The size of P is the minimal number of inequalities
- TSP polytope: convex hull of Hamiltonian cycles in K_n
  $P_{\mathrm{TSP}} = \mathrm{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n$ is a tour of $K_n\}$
- Solving TSP w.r.t. weight function w_{ij}:
  minimize the linear function $\sum_{i,j} w_{ij}x_{ij}$ over $x \in P_{\mathrm{TSP}}$

Basics of polytopes

- Polytope P: convex hull of finite set of points in $\mathbb{R}^d$



  $\Leftrightarrow$ bounded intersection of finitely many halfspaces
- Can be written as system of linear inequalities:
  $P = \{x \in \mathbb{R}^d \mid Ax \leq b\}$
  Different systems "$Ax \leq b$" can define the same P
  The size of P is the minimal number of inequalities
- TSP polytope: convex hull of Hamiltonian cycles in K_n
  $P_{\text{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n \text{ is a tour of } K_n\}$
- Solving TSP w.r.t. weight function w_{ij}:
  minimize the linear function $\sum_{i,j} w_{ij}x_{ij}$ over $x \in P_{\text{TSP}}$
- P_{TSP} has exponential size, so corresponding LP is huge

Extended formulations of polytopes

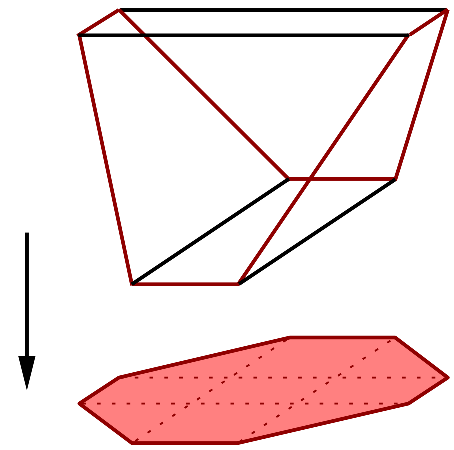
Extended formulations of polytopes

- Sometimes extra variables/dimensions can reduce size very much.

Extended formulations of polytopes

- Sometimes extra variables/dimensions can reduce size very much.

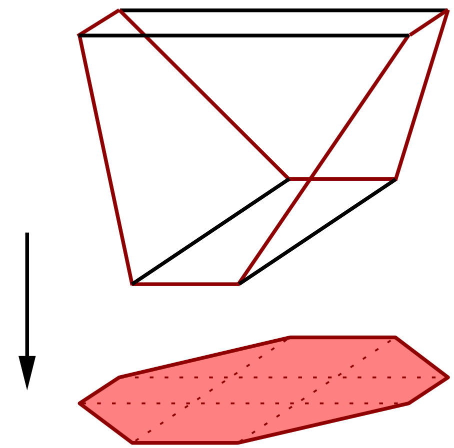
  Regular n-gon in $\mathbb{R}^2$ has size n, but is the projection of polytope in higher dimension, of size $O(\log n)$



Extended formulations of polytopes

- Sometimes extra variables/dimensions can reduce size very much.

  Regular n-gon in $\mathbb{R}^2$ has size n, but is the projection of polytope in higher dimension, of size $O(\log n)$

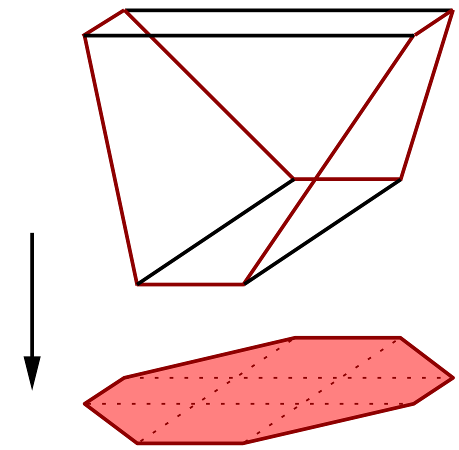


- Extended formulation of P:
  polytope $Q \subseteq \mathbb{R}^{d+k}$ s.t. $P = \{x \mid \exists\, y \text{ s.t. } (x, y) \in Q\}$

Extended formulations of polytopes

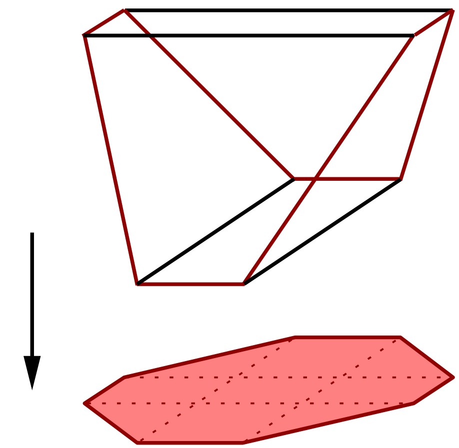
- Sometimes extra variables/dimensions can reduce size very much.

  Regular n-gon in $\mathbb{R}^2$ has size n, but is the projection of polytope in higher dimension, of size $O(\log n)$



- Extended formulation of P: polytope $Q \subseteq \mathbb{R}^{d+k}$ s.t. $P = \{x \mid \exists\, y \text{ s.t. } (x, y) \in Q\}$
- Optimizing over P reduces to optimizing over Q. If Q has small size, this can be done efficiently!

Extended formulations of polytopes



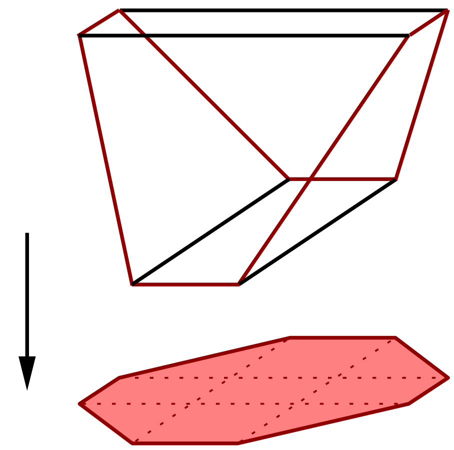
- Sometimes extra variables/dimensions can reduce size very much.

  Regular n-gon in $\mathbb{R}^2$ has size n, but is the projection of polytope in higher dimension, of size $O(\log n)$
- Extended formulation of P: polytope $Q \subseteq \mathbb{R}^{d+k}$ s.t. $P = \{x \mid \exists\, y$ s.t. $(x, y) \in Q\}$
- Optimizing over P reduces to optimizing over Q. If Q has small size, this can be done efficiently!
- How small can size(Q) be? Extension complexity: $xc(P) = \min\{$size$(Q) \mid Q$ is an EF of $P\}$

Extended formulations of polytopes

- Sometimes extra variables/dimensions can reduce size very much.

  Regular n-gon in $\mathbb{R}^2$ has size n, but is the projection of polytope in higher dimension, of size $O(\log n)$



- Extended formulation of P: polytope $Q \subseteq \mathbb{R}^{d+k}$ s.t. $P = \{x \mid \exists\, y \text{ s.t. } (x,y) \in Q\}$
- Optimizing over P reduces to optimizing over Q. If Q has small size, this can be done efficiently!
- How small can size(Q) be? Extension complexity: $xc(P) = \min\{\text{size}(Q) \mid Q \text{ is an EF of } P\}$
- Our goal: strong lower bounds on $xc(P)$ for interesting P

The TSP polytope: main result

The TSP polytope: main result

- $P_{\text{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n \text{ is a tour of } K_n\}$

The TSP polytope: main result

- $P_{\text{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n \text{ is a tour of } K_n\}$
- Our main result: $xc(P_{\text{TSP}}) \geq 2^{\Omega(\sqrt{n})}$

The TSP polytope: main result

- $P_{\mathrm{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n \text{ is a tour of } K_n\}$
- Our main result: $xc(P_{\mathrm{TSP}}) \geq 2^{\Omega(\sqrt{n})}$
- Hence every LP for TSP based on extended formulation of TSP-polytope needs exponential time

The TSP polytope: main result

- $P_{\text{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n \text{ is a tour of } K_n\}$
- Our main result: $xc(P_{\text{TSP}}) \geq 2^{\Omega(\sqrt{n})}$
- Hence every LP for TSP based on extended formulation of TSP-polytope needs exponential time
- This rules out a lot of potential algorithms

The TSP polytope: main result

- $P_{\text{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n$ is a tour of $K_n\}$
- Our main result: $xc(P_{\text{TSP}}) \geq 2^{\Omega(\sqrt{n})}$
- Hence every LP for TSP based on extended formulation of TSP-polytope needs exponential time
- This rules out a lot of potential algorithms
- Roadmap for the proof:

  2^n lower bound on xc of correlation polytope

The TSP polytope: main result

- $P_{\text{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n \text{ is a tour of } K_n\}$
- Our main result: $xc(P_{\text{TSP}}) \geq 2^{\Omega(\sqrt{n})}$
- Hence every LP for TSP based on extended formulation of TSP-polytope needs exponential time
- This rules out a lot of potential algorithms
- Roadmap for the proof:

  2^n lower bound on xc of correlation polytope
  [inspired by quantum communication complexity!]

The TSP polytope: main result

- $P_{\text{TSP}} = \text{conv}\{\chi^F \in \{0,1\}^{\binom{n}{2}} \mid F \subseteq E_n \text{ is a tour of } K_n\}$
- Our main result: $xc(P_{\text{TSP}}) \geq 2^{\Omega(\sqrt{n})}$
- Hence every LP for TSP based on extended formulation of TSP-polytope needs exponential time
- This rules out a lot of potential algorithms
- Roadmap for the proof:

2^n lower bound on xc of correlation polytope
[inspired by quantum communication complexity!]

$\Downarrow$ gadget-based reduction

$2^{\sqrt{n}}$ lower bound for TSP-polytope

How to lower bound extension compl?

How to lower bound extension compl?

- Slack matrix S of a polytope $P = \text{conv}(V)$ with inequalities $\{A_i x \leq b_i\}$ and points $V = \{v_j\}$:

$$S_{ij} = b_i - A_i v_j$$

How to lower bound extension compl?

- Slack matrix S of a polytope $P = \text{conv}(V)$ with inequalities $\{A_i x \leq b_i\}$ and points $V = \{v_j\}$:

$$S_{ij} = b_i - A_i v_j$$

NB: every entry is nonnegative; S is not unique

How to lower bound extension compl?

- Slack matrix S of a polytope $P = \text{conv}(V)$ with inequalities $\{A_i x \leq b_i\}$ and points $V = \{v_j\}$:

$$S_{ij} = b_i - A_i v_j$$

NB: every entry is nonnegative; S is not unique

- Positive factorization $S = \sum_{i=1}^{r} u_i v_i^T$, vectors $u_i, v_i \geq 0$

How to lower bound extension compl?

- Slack matrix S of a polytope $P = \text{conv}(V)$ with inequalities $\{A_i x \leq b_i\}$ and points $V = \{v_j\}$:

$$S_{ij} = b_i - A_i v_j$$

  NB: every entry is nonnegative; S is not unique

- Positive factorization $S = \sum_{i=1}^{r} u_i v_i^T$, vectors $u_i, v_i \geq 0$
- Nonnegative rank: $\text{rank}_+(S) = \min$ such r

How to lower bound extension compl?

- Slack matrix S of a polytope $P = \text{conv}(V)$ with inequalities $\{A_i x \leq b_i\}$ and points $V = \{v_j\}$:

$$S_{ij} = b_i - A_i v_j$$

  NB: every entry is nonnegative; S is not unique

- Positive factorization $S = \sum_{i=1}^{r} u_i v_i^T$, vectors $u_i, v_i \geq 0$
- Nonnegative rank: $\text{rank}_+(S) = \min$ such r
- Yannakakis'88: $xc(P) = \text{rank}_+(S)$

How to lower bound extension compl?

- Slack matrix S of a polytope $P = \text{conv}(V)$ with inequalities $\{A_i x \leq b_i\}$ and points $V = \{v_j\}$:

  $$S_{ij} = b_i - A_i v_j$$

  NB: every entry is nonnegative; S is not unique

- Positive factorization $S = \sum_{i=1}^{r} u_i v_i^T$, vectors $u_i, v_i \geq 0$
- Nonnegative rank: $\text{rank}_+(S) = \min$ such r
- Yannakakis'88: $xc(P) = \text{rank}_+(S)$
- $\text{rank}_+(S)$ has many connections with communication complexity

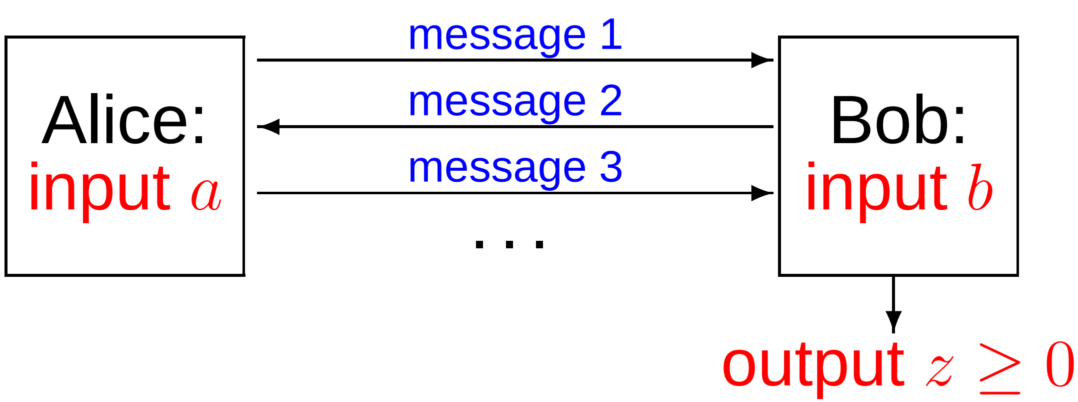
Communication compl. in expectation

Communication compl. in expectation

- "Computing a matrix M in expectation"

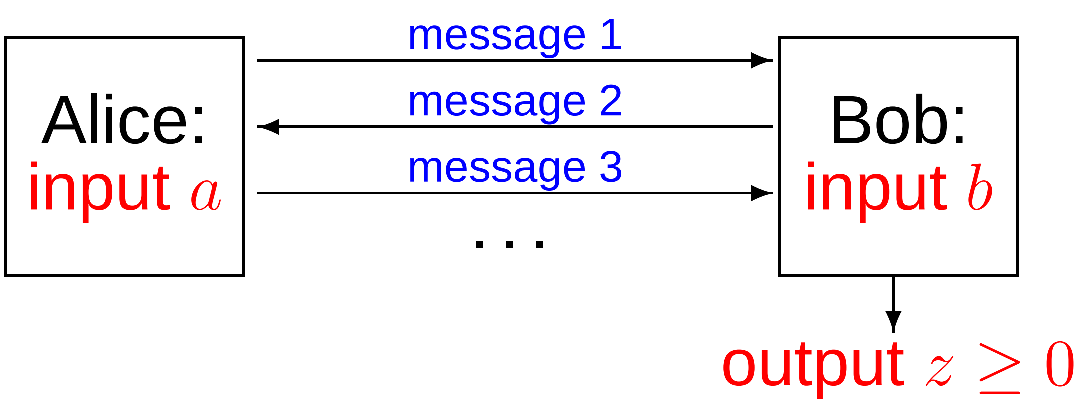
Communication compl. in expectation

- "Computing a matrix M in expectation":
  Alice gets input $a \in \{0,1\}^n$, Bob gets input $b \in \{0,1\}^n$,
  Bob should output a nonnegative z such that $\mathbb{E}[z] = M_{ab}$



Communication compl. in expectation

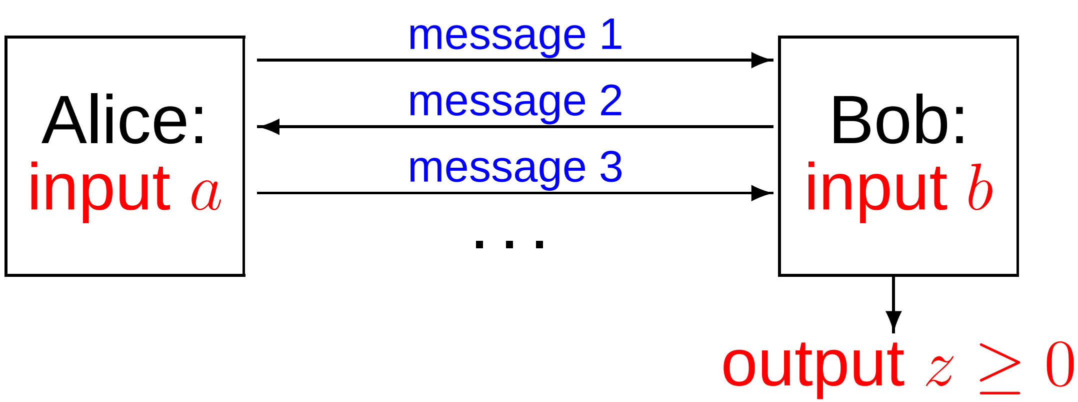
- "Computing a matrix M in expectation":
  Alice gets input $a \in \{0,1\}^n$, Bob gets input $b \in \{0,1\}^n$,
  Bob should output a nonnegative z such that $\mathbb{E}[z] = M_{ab}$



- Faenza et al.'11:
  classical communication required $= \log \text{rank}_+(M)$ bits

Communication compl. in expectation

- “Computing a matrix M in expectation”:
  Alice gets input $a \in \{0,1\}^n$, Bob gets input $b \in \{0,1\}^n$,
  Bob should output a nonnegative z such that $\mathbb{E}[z] = M_{ab}$



- Faenza et al.’11:
  classical communication required $= \log \text{rank}_+(M)$ bits
- Can we find a matrix M where
  quantum communication is exponentially smaller?

Quantum-classical separation

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

  $$M_{ab} = (1 - a^T b)^2$$

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

$$M_{ab} = (1 - a^T b)^2 \qquad \text{NB: } M_{ab} = 0 \text{ iff } a^T b = 1$$

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

$$M_{ab} = (1 - a^T b)^2 \qquad \text{NB: } M_{ab} = 0 \text{ iff } a^T b = 1$$

- **Claim**: $2^{\Omega(n)}$ rectangles needed to cover support of M

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

$$M_{ab} = (1 - a^T b)^2 \qquad \text{NB: } M_{ab} = 0 \text{ iff } a^T b = 1$$

- **Claim**: $2^{\Omega(n)}$ rectangles needed to cover support of M
  Proof (informally): Razborov showed that a rectangle that doesn't contain (a,b)-pairs with $a^T b = 1$, can cover only an exponentially small fraction of disjoint (a,b).

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

  $M_{ab} = (1 - a^T b)^2$ NB: $M_{ab} = 0$ iff $a^T b = 1$

- **Claim**: $2^{\Omega(n)}$ rectangles needed to cover support of M

  Proof (informally): Razborov showed that a rectangle that doesn't contain (a, b)-pairs with $a^T b = 1$, can cover only an exponentially small fraction of disjoint (a, b).

  $\Rightarrow 2^{\Omega(n)}$ rectangles needed to cover all disjoint (a, b)

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

$$M_{ab} = (1 - a^T b)^2 \qquad \text{NB: } M_{ab} = 0 \text{ iff } a^T b = 1$$

- **Claim**: $2^{\Omega(n)}$ rectangles needed to cover support of M
Proof (informally): Razborov showed that a rectangle that doesn't contain (a, b)-pairs with $a^T b = 1$, can cover only an exponentially small fraction of disjoint (a, b).
$\Rightarrow 2^{\Omega(n)}$ rectangles needed to cover all disjoint (a, b)

- If $M = \sum_{i=1}^{r} u_i v_i^T$, $u_i, v_i \geq 0$, each $u_i v_i^T$ gives a non-zero rectangle

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

  $$M_{ab} = (1 - a^T b)^2 \qquad \text{NB: } M_{ab} = 0 \text{ iff } a^T b = 1$$

- **Claim**: $2^{\Omega(n)}$ rectangles needed to cover support of M

  Proof (informally): Razborov showed that a rectangle that doesn't contain (a, b)-pairs with $a^T b = 1$, can cover only an exponentially small fraction of disjoint (a, b).

  $\Rightarrow 2^{\Omega(n)}$ rectangles needed to cover all disjoint (a, b)

- If $M = \sum_{i=1}^{r} u_i v_i^T$, $u_i, v_i \geq 0$, each $u_i v_i^T$ gives a non-zero rectangle $\Rightarrow r \geq 2^{\Omega(n)}$

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

  $M_{ab} = (1 - a^T b)^2$ NB: $M_{ab} = 0$ iff $a^T b = 1$

- **Claim**: $2^{\Omega(n)}$ rectangles needed to cover support of M

  Proof (informally): Razborov showed that a rectangle that doesn't contain (a,b)-pairs with $a^T b = 1$, can cover only an exponentially small fraction of disjoint (a,b).

  $\Rightarrow 2^{\Omega(n)}$ rectangles needed to cover all disjoint (a,b)

- If $M = \sum_{i=1}^{r} u_i v_i^T$, $u_i, v_i \geq 0$, each $u_i v_i^T$ gives a non-zero rectangle $\Rightarrow r \geq 2^{\Omega(n)} \Rightarrow \Omega(n)$ classical communication

Quantum-classical separation

- $2^n \times 2^n$ matrix M, indexed by $a, b \in \{0,1\}^n$ (de Wolf'00)

  $$M_{ab} = (1 - a^T b)^2 \qquad \text{NB: } M_{ab} = 0 \text{ iff } a^T b = 1$$

- **Claim**: $2^{\Omega(n)}$ rectangles needed to cover support of M
  Proof (informally): Razborov showed that a rectangle that doesn't contain (a, b)-pairs with $a^T b = 1$, can cover only an exponentially small fraction of disjoint (a, b).
  $\Rightarrow 2^{\Omega(n)}$ rectangles needed to cover all disjoint (a, b)

- If $M = \sum_{i=1}^{r} u_i v_i^T$, $u_i, v_i \geq 0$, each $u_i v_i^T$ gives a non-zero rectangle $\Rightarrow r \geq 2^{\Omega(n)} \Rightarrow \Omega(n)$ classical communication

- There is a $O(\log n)$-qubit protocol: Alice sends $(a, 1)$, Bob measures $(b, -1)$ (ignoring normalization)

Lower bound for correlation polytope

Lower bound for correlation polytope

- Correlation polytope: COR$(n) = $ conv$\{bb^T \mid b \in \{0,1\}^n\}$

Lower bound for correlation polytope

- Correlation polytope: COR$(n) = $ conv$\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \ \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

Lower bound for correlation polytope

- Correlation polytope: COR$(n) =$ conv$\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \ \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

Slack of this a-constraint w.r.t. vertex bb^T:

Lower bound for correlation polytope

- Correlation polytope: COR$(n) =$ conv$\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \; \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

Slack of this a-constraint w.r.t. vertex bb^T:
$S_{ab} = 1 - \text{Tr}\left[(2\text{diag}(a) - aa^T)bb^T\right]$

Lower bound for correlation polytope

- Correlation polytope: COR$(n) =$ conv$\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \ \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

Slack of this a-constraint w.r.t. vertex bb^T:
$S_{ab} = 1 - \text{Tr}\left[(2\text{diag}(a) - aa^T)bb^T\right] = (1 - a^T b)^2$

Lower bound for correlation polytope

- Correlation polytope: COR$(n) =$ conv$\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \ \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

Slack of this a-constraint w.r.t. vertex bb^T:
$S_{ab} = 1 - \text{Tr}\left[(2\text{diag}(a) - aa^T)bb^T\right] = (1 - a^T b)^2 = M_{ab}$

Lower bound for correlation polytope

- Correlation polytope: COR(n) = conv$\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \ \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

  Slack of this a-constraint w.r.t. vertex bb^T:
  $S_{ab} = 1 - \text{Tr}\left[(2\text{diag}(a) - aa^T)bb^T\right] = (1 - a^T b)^2 = M_{ab}$

- Take slack matrix S for COR, with 2^n vertices bb^T for columns, 2^n a-constraints for first 2^n rows, remaining facets for other rows

$$S = \begin{bmatrix} & \vdots & \\ \cdots & M_{ab} & \cdots \\ & \vdots & \\ \hline & \vdots & \end{bmatrix}$$

Lower bound for correlation polytope

- Correlation polytope: COR(n) = conv$\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \ \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

Slack of this a-constraint w.r.t. vertex bb^T:
$S_{ab} = 1 - \text{Tr}\left[(2\text{diag}(a) - aa^T)bb^T\right] = (1 - a^T b)^2 = M_{ab}$

- Take slack matrix S for COR, with 2^n vertices bb^T for columns, 2^n a-constraints for first 2^n rows, remaining facets for other rows

$$S = \left[\begin{array}{ccc} & \vdots & \\ \cdots & M_{ab} & \cdots \\ & \vdots & \\ \hline & \vdots & \end{array}\right]$$

- $xc(\text{COR}(n))$

Lower bound for correlation polytope

- Correlation polytope: $\text{COR}(n) = \text{conv}\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \ \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

Slack of this a-constraint w.r.t. vertex bb^T:
$S_{ab} = 1 - \text{Tr}\left[(2\text{diag}(a) - aa^T)bb^T\right] = (1 - a^T b)^2 = M_{ab}$

- Take slack matrix S for COR, with 2^n vertices bb^T for columns, 2^n a-constraints for first 2^n rows, remaining facets for other rows

$$S = \left[\begin{array}{ccc} & \vdots & \\ \cdots & M_{ab} & \cdots \\ & \vdots & \\ \hline & \vdots & \end{array}\right]$$

- $xc(\text{COR}(n)) = \text{rank}_+(S)$

Lower bound for correlation polytope

- Correlation polytope: $\text{COR}(n) = \text{conv}\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \text{COR}(n): \ \text{Tr}\left[(2\text{diag}(a) - aa^T)x\right] \leq 1$$

Slack of this a-constraint w.r.t. vertex bb^T:
$S_{ab} = 1 - \text{Tr}\left[(2\text{diag}(a) - aa^T)bb^T\right] = (1 - a^T b)^2 = M_{ab}$

- Take slack matrix S for COR, with 2^n vertices bb^T for columns, 2^n a-constraints for first 2^n rows, remaining facets for other rows

$$S = \begin{bmatrix} & \vdots & \\ \cdots & M_{ab} & \cdots \\ & \vdots & \\ \hline & \vdots & \end{bmatrix}$$

- $xc(\text{COR}(n)) = \text{rank}_+(S) \geq \text{rank}_+(M)$

Lower bound for correlation polytope

- Correlation polytope: $\mathsf{COR}(n) = \mathsf{conv}\{bb^T \mid b \in \{0,1\}^n\}$
- The following constraints hold (one for each $a \in \{0,1\}^n$):

$$\forall x \in \mathsf{COR}(n) : \ \mathsf{Tr}\left[(2\mathsf{diag}(a) - aa^T)x\right] \leq 1$$

  Slack of this a-constraint w.r.t. vertex bb^T:
  $S_{ab} = 1 - \mathsf{Tr}\left[(2\mathsf{diag}(a) - aa^T)bb^T\right] = (1 - a^T b)^2 = M_{ab}$

- Take slack matrix S for COR, with 2^n vertices bb^T for columns, 2^n a-constraints for first 2^n rows, remaining facets for other rows

$$S = \left[\begin{array}{ccc} & \vdots & \\ \cdots & M_{ab} & \cdots \\ & \vdots & \\ \hline & \vdots & \end{array}\right]$$

- $xc(\mathsf{COR}(n)) = \mathsf{rank}_+(S) \geq \mathsf{rank}_+(M) \geq 2^{\Omega(n)}$

Consequences for other polytopes

Consequences for other polytopes

- Via classical reductions we can prove lower bounds on the extension complexity of other polytopes:

Consequences for other polytopes

- Via classical reductions we can prove lower bounds on the extension complexity of other polytopes:
  - $\geq 2^n$ for the CUT polytope

Consequences for other polytopes

- Via classical reductions we can prove lower bounds on the extension complexity of other polytopes:
  - $\geq 2^n$ for the CUT polytope
  - $\geq 2^{\sqrt{n}}$ for TSP polytope

Consequences for other polytopes

- Via classical reductions we can prove lower bounds on the extension complexity of other polytopes:
  - $\geq 2^n$ for the CUT polytope
  - $\geq 2^{\sqrt{n}}$ for TSP polytope
  - $\geq 2^{\sqrt{n}}$ for Stable Set polytope for specific graph

Consequences for other polytopes

- Via classical reductions we can prove lower bounds on the extension complexity of other polytopes:
  - $\geq 2^n$ for the CUT polytope
  - $\geq 2^{\sqrt{n}}$ for TSP polytope
  - $\geq 2^{\sqrt{n}}$ for Stable Set polytope for specific graph
- This refutes all P$=$NP “proofs” à la Swart

Cartoon by Pavel Pudlak

Quantum techniques as a proof-tool

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?
- No – but we wouldn't have found this proof without our interest in quantum communication complexity

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?
- No – but we wouldn't have found this proof without our interest in quantum communication complexity
- Wittgenstein: climb the ladder, and then throw it away

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?
- No – but we wouldn't have found this proof without our interest in quantum communication complexity
- Wittgenstein: climb the ladder, and then throw it away
- This is yet another (albeit weak) example of "quantum proofs for classical theorems"

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?
- No – but we wouldn't have found this proof without our interest in quantum communication complexity
- Wittgenstein: climb the ladder, and then throw it away
- This is yet another (albeit weak) example of "quantum proofs for classical theorems". Also:
  - Lower bounds for locally decodable codes (K & dW)

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?
- No – but we wouldn't have found this proof without our interest in quantum communication complexity
- Wittgenstein: climb the ladder, and then throw it away
- This is yet another (albeit weak) example of "quantum proofs for classical theorems". Also:
  - Lower bounds for locally decodable codes (K & dW)
  - New proofs of classical complexity results:
    PP is closed under intersection,
    Permanent is #P-complete (Aaronson)

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?
- No – but we wouldn't have found this proof without our interest in quantum communication complexity
- Wittgenstein: climb the ladder, and then throw it away
- This is yet another (albeit weak) example of "quantum proofs for classical theorems". Also:
  - Lower bounds for locally decodable codes (K & dW)
  - New proofs of classical complexity results:
    PP is closed under intersection,
    Permanent is #P-complete (Aaronson)
  - Proof systems for lattice-problems (Aharonov,Regev)

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?
- No – but we wouldn't have found this proof without our interest in quantum communication complexity
- Wittgenstein: climb the ladder, and then throw it away
- This is yet another (albeit weak) example of "quantum proofs for classical theorems". Also:
  - Lower bounds for locally decodable codes (K & dW)
  - New proofs of classical complexity results:
    PP is closed under intersection,
    Permanent is #P-complete (Aaronson)
  - Proof systems for lattice-problems (Aharonov,Regev)
  - Proof of Varopoulos conjecture (BBLV)

Quantum techniques as a proof-tool

- Did we really need quantum for this proof?
- No – but we wouldn't have found this proof without our interest in quantum communication complexity
- Wittgenstein: climb the ladder, and then throw it away
- This is yet another (albeit weak) example of "quantum proofs for classical theorems". Also:
  - Lower bounds for locally decodable codes (K & dW)
  - New proofs of classical complexity results:
    PP is closed under intersection,
    Permanent is #P-complete (Aaronson)
  - Proof systems for lattice-problems (Aharonov,Regev)
  - Proof of Varopoulos conjecture (BBLV)
  - Efficient algorithms $\Rightarrow$ low-degree polynomials

Summary

Summary

- We studied the extension complexity of polytopes

Summary

- We studied the extension complexity of polytopes
- Showed exponential lower bounds on the extension complexities of the correlation, cut, stable set, and TSP polytopes, even for non-symmetric extensions. This solves a 20-year old problem of Yannakakis, inspired by quantum communication complexity

Summary

- We studied the extension complexity of polytopes
- Showed exponential lower bounds on the extension complexities of the correlation, cut, stable set, and TSP polytopes, even for non-symmetric extensions. This solves a 20-year old problem of Yannakakis, inspired by quantum communication complexity
- Further research:
  - Lower bound for the matching polytope? (Yannakakis: exponential LB for symmetric)

Summary

- We studied the extension complexity of polytopes
- Showed exponential lower bounds on the extension complexities of the correlation, cut, stable set, and TSP polytopes, even for non-symmetric extensions. This solves a 20-year old problem of Yannakakis, inspired by quantum communication complexity
- Further research:
  - Lower bound for the matching polytope? (Yannakakis: exponential LB for symmetric)
  - Lower bounds on positive semidefinite extensions? [Not shown here: this is closely connected to quantum communication complexity]

Summary

- We studied the extension complexity of polytopes
- Showed exponential lower bounds on the extension complexities of the correlation, cut, stable set, and TSP polytopes, even for non-symmetric extensions. This solves a 20-year old problem of Yannakakis, inspired by quantum communication complexity
- Further research:
  - Lower bound for the matching polytope? (Yannakakis: exponential LB for symmetric)
  - Lower bounds on positive semidefinite extensions? [Not shown here: this is closely connected to quantum communication complexity]
  - Lower bounds for approximation? [BFPS'12,BM'12]