Derandomizing the Isolation Lemma and Parallel Algorithms

Rohit Gurjar
California Institute of Technology

Based on Joint works with Stephen Fenner, Thomas Thierauf and, Nisheeth Vishnoi

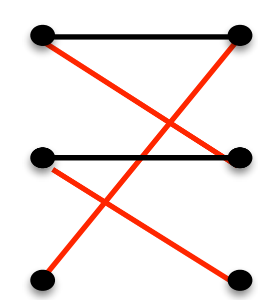
January 16, 2018

Introduction

- Randomness is a powerful tool for designing efficient algorithms.
- Power/Limits of randomization?
- Can we derandomize all efficient algorithms?
- P=BPP?
- Connections to circuit lower bounds.

Derandomization Questions

- Some examples of successful derandomization -
  - Primality testing [AKS02]
  - s-t connectivity [Rei05]
- Interesting open questions:
  - Generating primes, Approximating the Permanent
  - Parallel algorithms for matching
  - Polynomial Identity Testing (PIT) (circuit lower bounds)

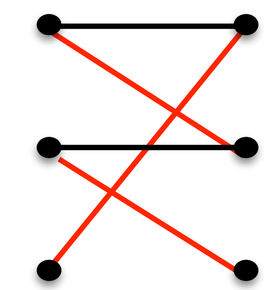


$$(a^2+nb^2)(c^2+nd^2)-(ac+nbd)^2-n(ad-bc)^2=0$$

Isolation Lemma [MVV87]

- For $w\colon E \to \mathbb{Z}$ and $S \subseteq E$, define
$$w(S) = \sum_{e \in S} w(e)$$
- Let $\mathcal{B} \subseteq 2^E$ be a family of subsets of E.
- For each $e \in E$, assign a weight randomly and independently from $\{1, 2, \ldots, 2|E|\}$.
- Then there is a unique minimum weight set in $\mathcal{B}$ with probability at least 1/2.

Isolation Lemma: Applications



- Perfect Matching in RNC [MVV87]

poly(n) processors
polylog(n) time

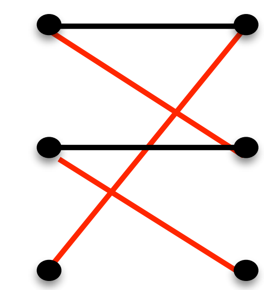
- Polynomial Identity
- Clique to Unique-clique [MVV87]
- Reachability in UL/poly [RA00]
- Disjoint paths $(s_1 \sim t_1, s_2 \sim t_2)$ in RP [BH14]

Derandomization

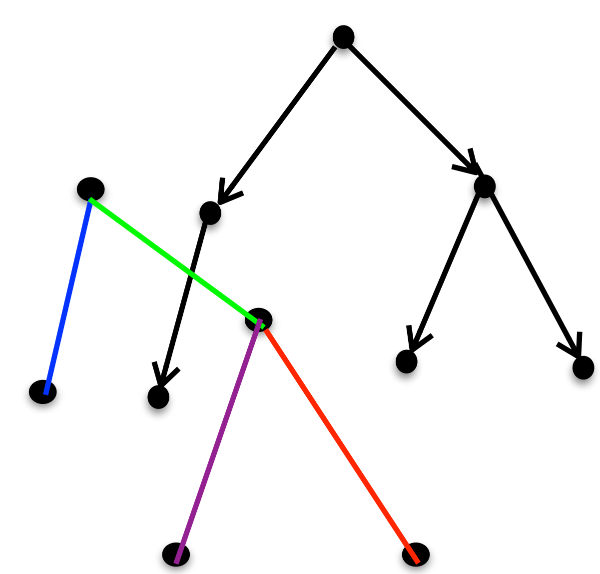
- construct an isolating weight assignment deterministically (poly-bounded weights).
- The family is not given explicitly.
- Known for only very specific families -
  - Families with polynomially many sets
  - perfect matchings in a bipartite planar graph
- We give a geometric approach: derandomize the Isolation Lemma for a large class of families.
  (quasi-polynomially bounded weights $n^{O(\log n)}$)

Our Results

- Perfect Matchings in a Bipartite Graph
  - Bipartite perfect matching in quasi-NC
  - Max-flow, depth-first search tree, subtree isomorphism



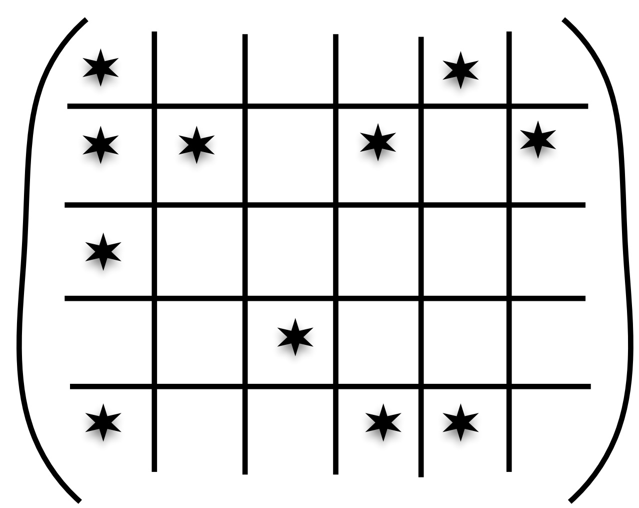
- Linear Matroid Intersection in quasi-NC
  - two edge-disjoint spanning trees
  - r-arborescence
  - rainbow spanning tree



More Applications

- Polynomial Identity Testing
  - Hitting-set: every nonzero polynomial has a nonzero evaluation for at least one of the points.
  - quasi-polynomial size hitting sets for
    $$\det(A_1 x_1 + \cdots + A_m x_m)$$
    where $A_1, \ldots, A_m$ are rank 1 matrices.
  - Edmonds' Problem: max rank matrix in $span(A_1, \ldots, A_m)$
- Maximum rank matrix completion

$$\begin{pmatrix} x_1 & 0 & 7x_3 \\ 2x_1 & x_2 & 0 \\ 0 & 0 & \cdots\; x_3 \\ x_1 & -x_2 & 0 \end{pmatrix}$$



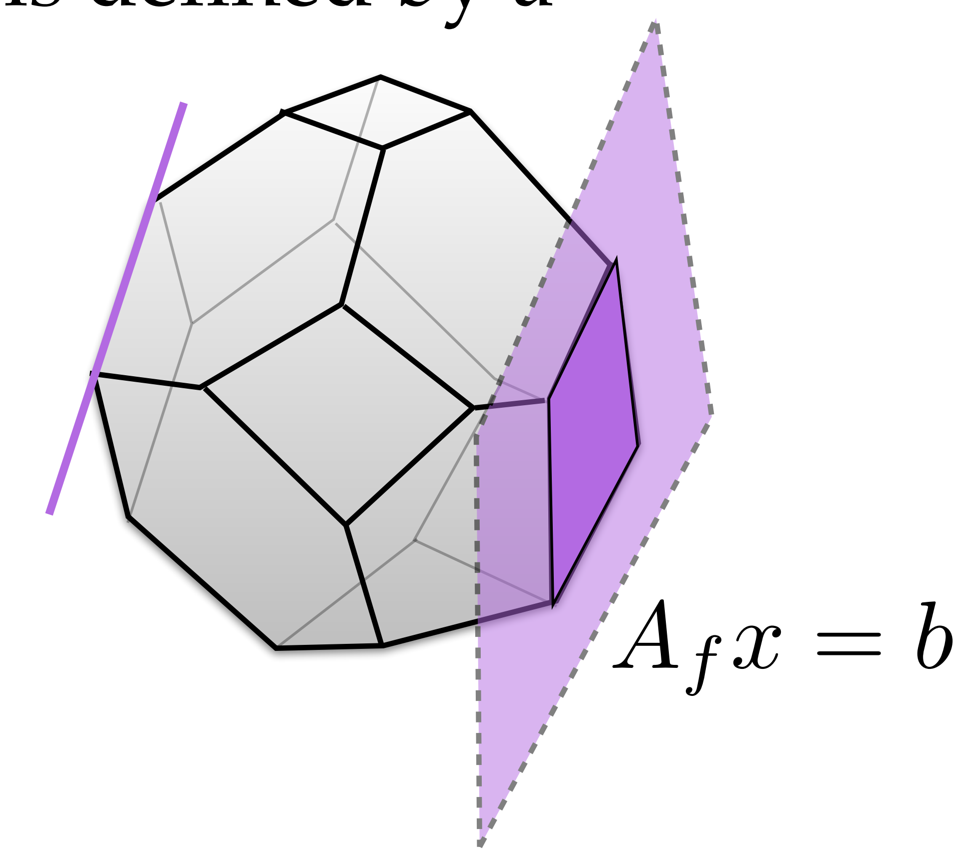
Further Generalization

- For $S \subseteq E$, let $x^S \in \{0,1\}^E$ be its indicator vector.
- For a family $\mathcal{B} \subseteq 2^E$, define a polytope

$$P(\mathcal{B}) = \text{conv-hull}\{x^S \mid S \in \mathcal{B}\} \quad \subseteq \mathbb{R}^E$$

- Sufficient: when every face f of $P(\mathcal{B})$ is defined by a totally unimodular matrix.

- every sub-determinant in A_f is $0, \pm 1$



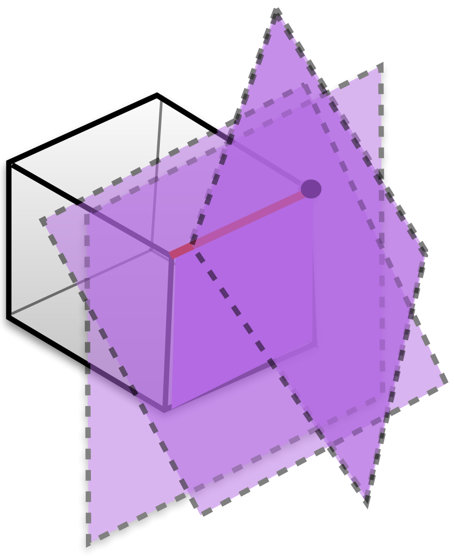
Polytopes with TU faces

- Simplest examples: Polytopes with TU constraints
    - Perfect Matching, Independent sets, Vertex covers, Edge covers in bipartite graphs
- Matroid Intersection, Polymatroid Intersection Polytope,
- Directed Cut Cover Polytope,
- Submodular base polytope
- Submodular flow polyhedron,
- Many other polytopes defined via submodular/supermodular set functions [Schrijver '03]

Approach

- For $w \in \mathbb{R}^E$, consider the function $w \cdot x$ over $P(\mathcal{B})$
- For a set $S \subseteq E$, $\quad w \cdot x^S = w(S)$
- Goal: Design $w \in \mathbb{Z}^E$ ($\log n$ bits), s.t. $w \cdot x$ has a unique minimum over $P(\mathcal{B})$
- Construction of w in many rounds.

w



Construction

- Take two points a and b in the polytope and ensure

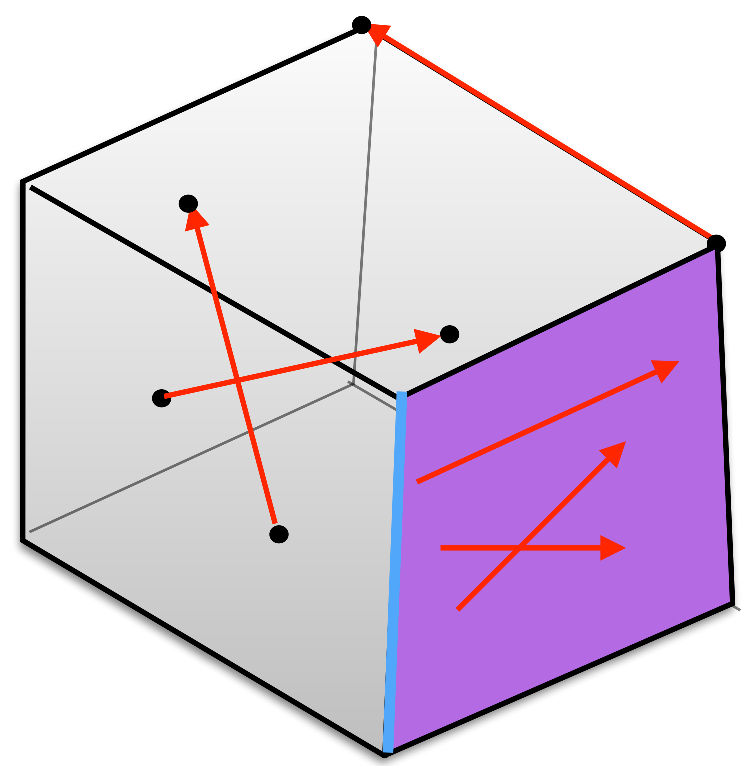
$$w \cdot a \neq w \cdot b$$

$$w \cdot (a - b) \neq 0$$

- Take many such vectors

$$w \cdot v_1 \neq 0, \quad w \cdot v_2 \neq 0, \cdots, w \cdot v_k \neq 0$$

- Minimizing face is not parallel to $v_1, v_2, \ldots, v_k$
- Polynomially many vectors at once (with poly-bounded integer coordinates)

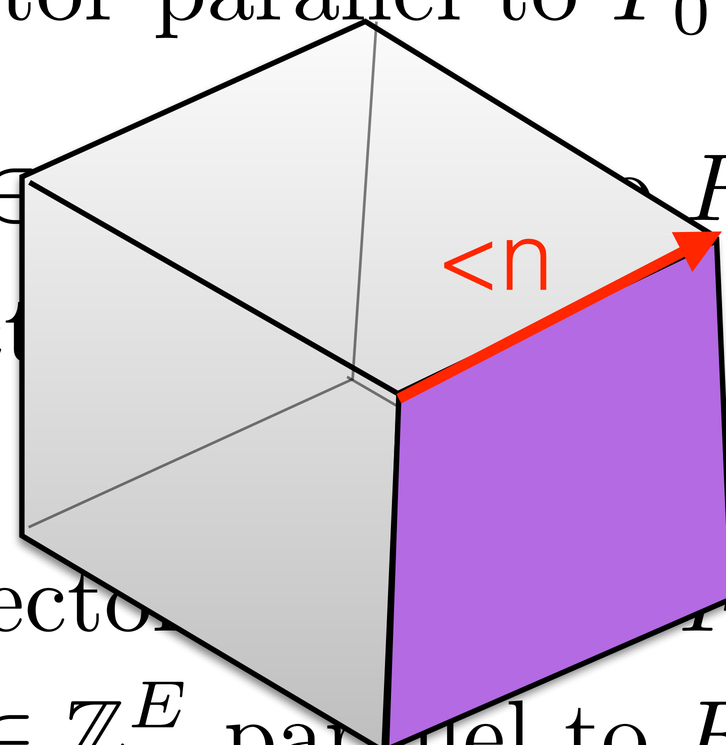


Construction

w_0 : $w_0 \cdot v \neq 0$ for all $v \in \mathbb{Z}^E$ of length ≤ 2 (poly(n) many)

F_0 : face minimizing $w_0 \cdot x$

Each integral vector parallel to F_0 has length > 2



w_1 : $w_1 \cdot v \neq 0$ $\forall v \in$ … F_0 and of length ≤ 4

F_1 : Each integral vect… has length > 4

F_{i-1} : Each integral vecto… F_{i-1} has length $> 2^i$

w_i : $w_i \cdot v \neq 0$ $\forall v \in \mathbb{Z}^E$ parallel to F_{i-1} and of length $\leq 2^{i+1}$

Only poly(n) many ?

$F_{\log n}$: Each integral v… length $> n$

The face $F_{\log n}$ is a unique point

Sufficient Condition

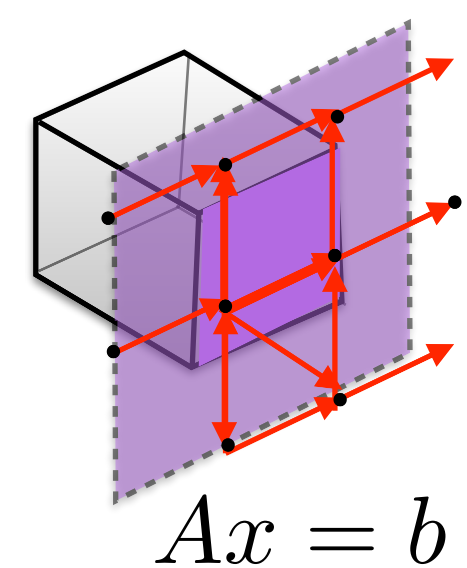
- For a face F, let

$$L_F = \text{ set of integral vectors parallel to } F$$

- For each face F,
  if every vector in L_F has length $> r$
  then #vectors in L_F of length $\leq 2r$ is poly-bounded.

$$L_F = \{v \in \mathbb{Z}^E \mid Av = 0\}$$

- #near-shortest vectors in L_F is poly(n)



#Near-shortest Vectors

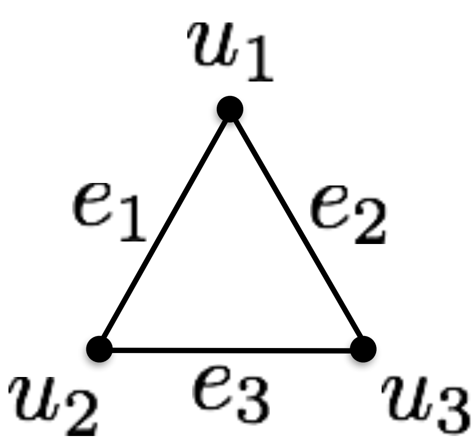
$$L = \{v \in \mathbb{Z}^n \mid Av = 0\}$$

- Theorem: When A is totally unimodular then number of near-shortest vectors in the lattice L is poly(n).

- We get Isolation for every polytope with TU faces.

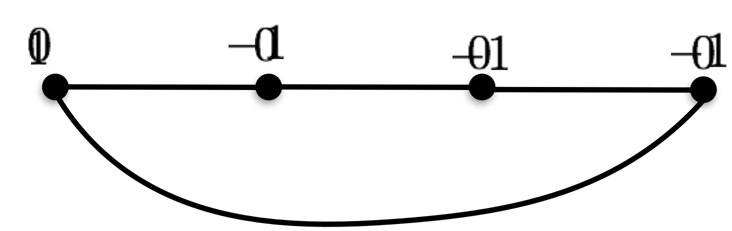
A Simple TU Matrix

- For a graph G, consider its signed incidence matrix



$$\begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \end{array} \begin{array}{c} \begin{array}{ccc} e_1 & e_2 & e_3 \end{array} \\ \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & -1 & -1 \end{bmatrix} \end{array} = A$$

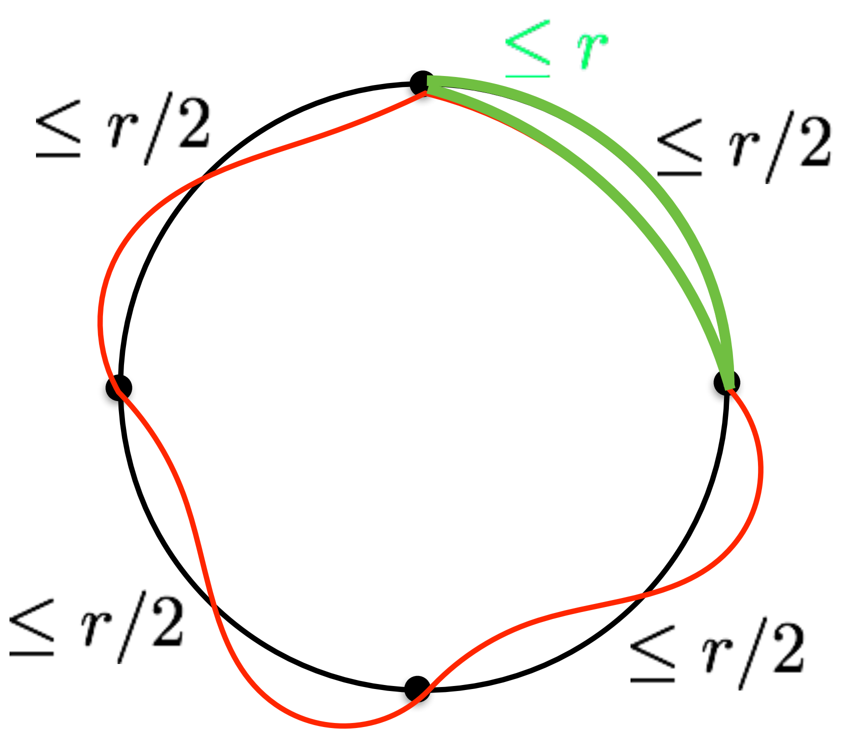
- Solutions for $Av = 0$?



- Vectors in $\{v \in \mathbb{Z}^E \mid Av = 0\}$ come exactly from cycles (and their integral combinations)

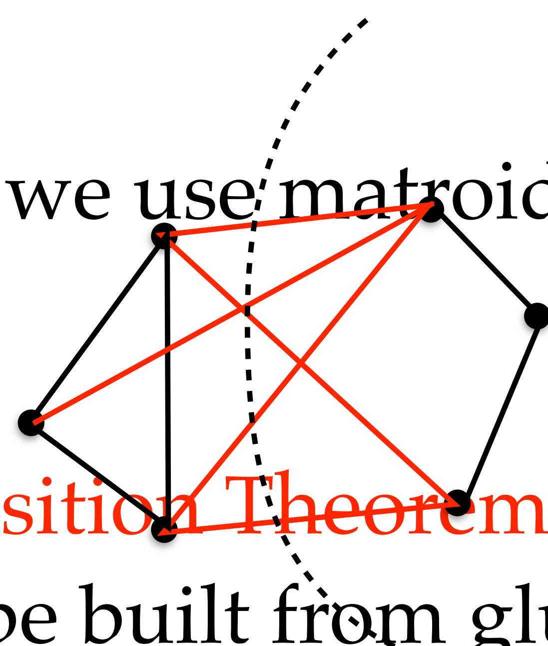
Near-shortest Cycles

- #near-shortest vectors = #near-shortest cycles in G
- [Sub95] #near-shortest cycles in G is poly(n).
- Let the shortest cycle length = r+1.
- To bound #cycles of length $\leq$ 2r.
- Claim: A tuple defines a unique cycle.
-



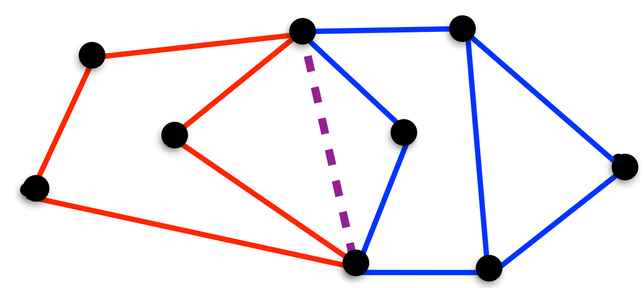
Near-shortest Vectors in TU Lattices

- **Graphic Lattice**: #near-shortest cycles in G is poly(n) [Sub95]
- **Cographic Lattice**: #near-minimum cuts in G is poly(n) [Karger 93]
- **General TU lattices**: we use matroid theory to bound #near-shortest vectors

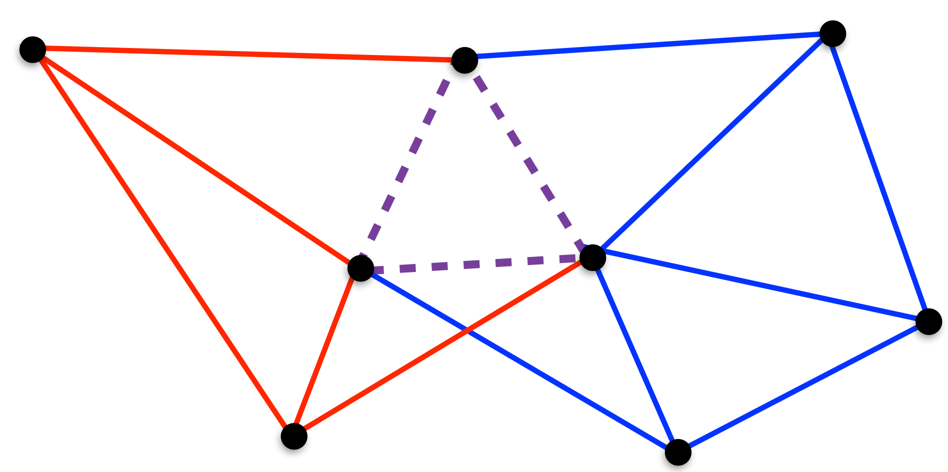


- Seymour's Decomposition Theorem for regular matroids: Each TU matrix can be built from gluing together three kinds of matrices — graphic, cographic and, R_{10} (via k-sums)

Seymour’s Decomposition



2-sum



3-sum

Future Directions

- Generalizing the Isolation approach
  - Which lattices $\{v \in \mathbb{Z}^n \mid Av = 0\}$ have small no. of near-shortest vectors?
  - #shortest vectors vs. #near-shortest vectors
- Quasi-polynomial to polynomial ?
  - NC algorithms for matching and linear matroid intersection
  - Reachability in Unambiguous Log-space (UL)
  - Poly-time solutions for some PIT and matrix completion problems.

Future Directions

- Parallel algorithms for more optimization problems
  - Linear Programming with Totally Unimodular constraints
  - Linear Matroid Matching
  - Matroid Intersection (under rank oracle)
- Polynomial Identity Testing
  - $\det(A_1 x_1 + \cdots + A_m x_m)$ for rank-2 matrices $A_1, \ldots, A_m$
  - Non-commutative rank of $A_1 x_1 + \cdots + A_m x_m$ (black-box)
  - Approximate rank of $A_1 x_1 + \cdots + A_m x_m$ (black-box)

Thank You

Backup