Polynomial Time Algebraic Algorithms

What can you solve with rank and determinant?

Saket Saurabh

Institute of Mathematical Sciences

(slides partially made by Marek/Lap Chi Lau/Ho Yee/Kai Man/Tsz Chiu)

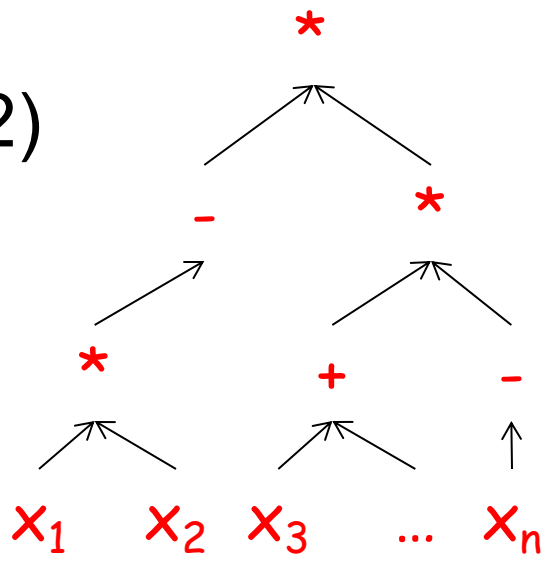
https://web.iitd.ac.in/~raiashutosh/Courses/agacourse.html

Technical Engine

- Polynomial Identity Testing (PIT)

Polynomial identity testing

- Given: polynomial $p(x_1, x_2, \ldots, x_n)$ as arithmetic formula (fan-out 1):
  - multiplication (fan-in 2)
  - addition (fan-in 2)
  - negation (fan-in 1)



Polynomial identity testing

- Question: Is p identically zero?
  - i.e., is $p(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbf{F}^n$
  - (assume $|\mathbf{F}|$ larger than degree of $p(\mathbf{x})$)

- "polynomial identity testing" because given two polynomials p, q, we can check the identity $p \equiv q$ by checking if $(p - q) \equiv 0$

Polynomial identity testing

- Try all $|\mathbf{F}|^n$ inputs?
  - may be exponentially many
- multiply out symbolically, check that all coefficients are zero?
  - may be exponentially many coefficients

- Can randomness help?
  - i.e., flip coins, allow small probability of wrong answer

Polynomial identity testing

Lemma (Schwartz-Zippel): Let

$$p(x_1, x_2, \ldots, x_n)$$

be a total degree d polynomial over a field **F** and let S be any subset of **F**. Then if p is not identically 0, for uniform random choice of $r_1, r_2, \ldots, r_n$ in S,

$$\Pr_{r_1,r_2,\ldots,r_n \in S}[\, p(r_1, r_2, \ldots, r_n) = 0] \leq d/|S|.$$

(Note: this probability bound does not depend on n.)

Polynomial identity testing

- Proof:
  - induction on number of variables n
  - base case: n = 1, p is univariate polynomial of degree at most d
  - at most d roots, so

$$\Pr[\, p(r_1) = 0] \leq d/|S|$$

Polynomial identity testing

– write $p(x_1, x_2, \ldots, x_n)$ as

$$p(x_1, x_2, \ldots, x_n) = \Sigma_i (x_1)^i p_i(x_2, \ldots, x_n)$$

– Let k = max i for which $p_i(x_2, \ldots, x_n)$ is not identically zero,

– So $p_k(x_2, \ldots, x_n)$ has degree d-k.

– By induction hypothesis:

$$\Pr[\, p_k(r_2, \ldots, r_n) = 0] \leq (d\text{-}k)/|S|$$

– Whenever $p_k(r_2, \ldots, r_n) \neq 0$, $p(x_1, r_2, \ldots, r_n)$ is a univariate polynomial of degree k, so by induction hypothesis:

$$\Pr[p(r_1,r_2,\ldots,r_n)=0 \mid p_k(r_2,\ldots,r_n) \neq 0] \leq k/|S|$$

Polynomial identity testing

So we have shown both:

(1) $\Pr[\ p_k(r_2, \ldots, r_n) = 0] \leq (d\text{-}k)/|S|$, and

(2) $\Pr[p(r_1,r_2,\ldots,r_n)=0 \mid p_k(r_2,\ldots,r_n) \neq 0] \leq k/|S|$

We Conclude:

$\Pr[\ p(r_1, \ldots, r_n) = 0] \leq (d\text{-}k)/|S| + k/|S| = d/|S|$

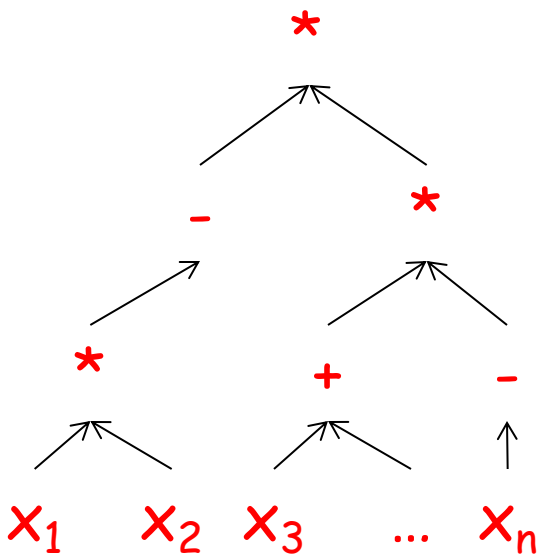
– Note: can add these probabilities (1) + (2) because:

$\Pr[E_2] = \Pr[E_2|E_1]\Pr[E_1] + \Pr[E_2|\neg E_1]\Pr[\neg\ E_1]$

$\leq \Pr[E_1] + \Pr[E_2|\neg E_1]$

Polynomial identity testing

- Given: polynomial $p(x_1, x_2, \ldots, x_n)$
- Is p identically zero?



- Note: degree d is at most the size of input

Polynomial identity testing

- Randomized algorithm:
- given field **F,** pick a subset $S \subset \mathbf{F}$ of size 2d
  - pick $r_1, r_2, \ldots, r_n$ from S uniformly at random
  - if $p(r_1, r_2, \ldots, r_n) = 0$, answer "yes"
  - if $p(r_1, r_2, \ldots, r_n) \neq 0$, answer "no"
- if p is identically zero, then never wrong
- if not, Schwartz-Zippel ensures probability of error at most ½

(Can extend the result to multivariate polynomials defined by algebriac circuits.)

Outline

I. Bipartite Matchings

II. General Matchings

III. Linear Matroid Intersection *(will mention)*

IV. Linear Matroid Parity *(will mention)*

Remark: Today we aim at polynomial time (randomized) algorithms, we are not going to optimize the running time.

Template

- Use PIT

- Define a polynomial P(x=x_1, x_2, …,x_n) such that

1. P(x) ≠ 0 if and only if G has a perfect matching, and
2. P(x) is easy to evaluate.

Determinant

Determinant of a matrix : Determinant of a square matrix $A = [a_i j]_{n \times n}$ is defined as :

$$det(A) = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

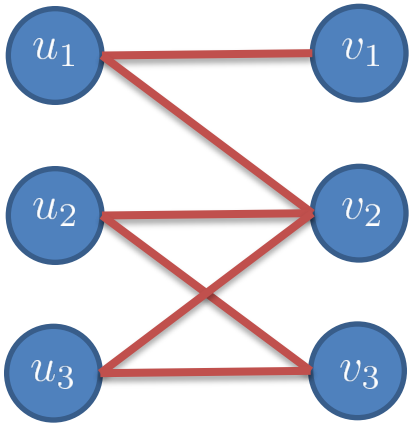
where,

- S_n is the set of all permutations over $\{1....n\}$
- $sgn(\sigma) = (-1)^j$
  where j is the number of inversions in σ (i.e, the number of $i < j$ such that $\sigma(i) > \sigma(j)$)
- $a_{i,j}$ is the entry in the matrix A corresponding to i^{th}s row and j^{th} coloumn.

Bipartite Perfect Matching

$$A_{i,j} = \begin{cases} x_e \text{ if } v_i v_j \in E \\ 0 \text{ otherwise} \end{cases}$$

G =



A =

	V	
x_1	x_2	
	x_3	x_4
	x_5	x_6

U

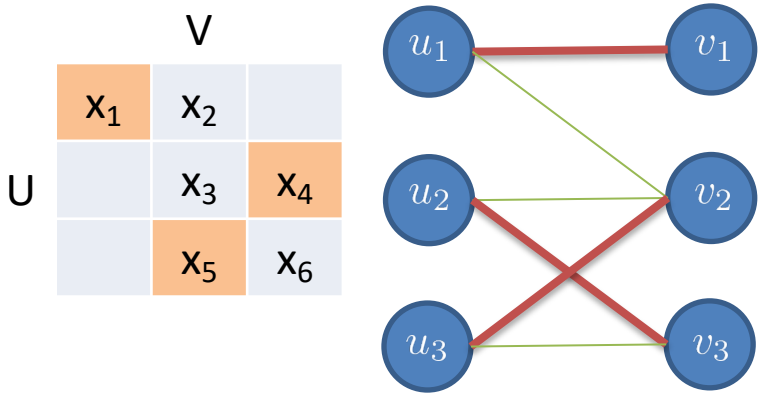
[Edmonds] G has a perfect matching if and only if det(A) is not the zero polynomial.

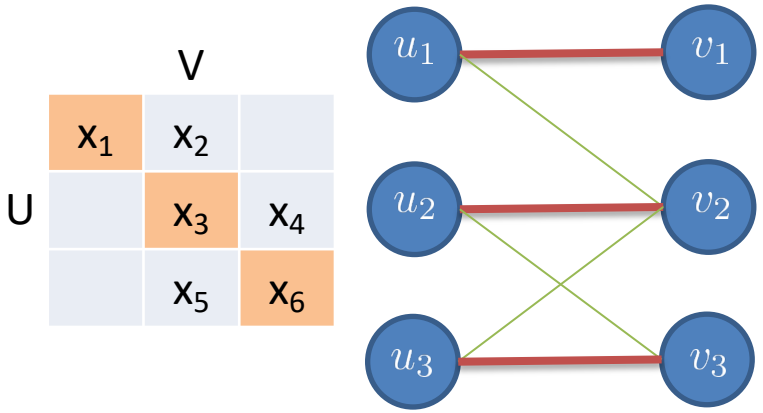
Bipartite Perfect Matching

[Edmonds] G has a perfect matching if and only if det(A) is not the zero polynomial.

$$\det \begin{pmatrix} x_1 & x_2 & \\ & x_3 & x_4 \\ & x_5 & x_6 \end{pmatrix} = x_1x_3x_6 - x_1x_4x_5$$

Each term in the determinant corresponds to a perfect matching





Bipartite Perfect Matching

[Edmonds] G has a perfect matching if and only if det(A) is not the zero polynomial.

$$\det(A) = \sum_{\sigma \in \mathcal{S}^n} sgn(\sigma) \prod_{i=1}^{n} A_{i,\sigma(i)}$$

Non-zero if all edges appear

Permutation of {1,2,..,n}

If there is no perfect matching, then all terms are zero, and det(A)=0.

If there is a perfect matching, then that term is unique, and det(A)≠0.

Randomized Algorithm

[Lovasz] Substitute each variable of A by a random element from a large enough finite field to obtain B.

Then, whp, if $\det(A)\neq 0$, then $\det(B)\neq 0$.

[Schwartz,Zippel] If $P\in F[x_1,\ldots,x_n]$ is a non-zero polynomial of degree d, then $P(r_1,\ldots,r_n)=0$ with probability at most $d/|F|$, where $r_1,\ldots,r_n$ are random elements in F.

Since det(B) is a degree n polynomial, choosing $|F|=\Theta(n^2)$ would work, so each field operation takes O(log n) time.

Linear Algebraic Algorithms

[Lovasz] Substitute each variable of A by a random element from a large enough finite field to obtain B.

Then, whp, if det(A)≠0, then det(B)≠0.

Checking whether det(B)≠0 is equivalent to checking whether B is of full rank.

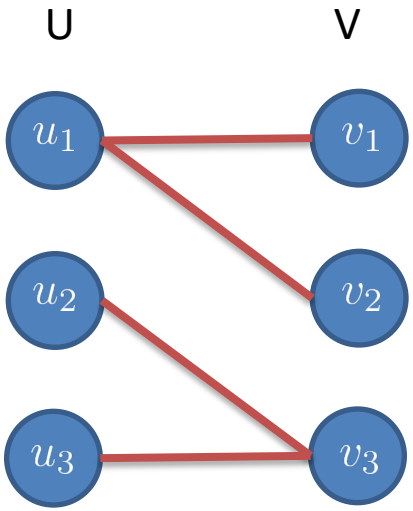
[Bunch,Hopcroft] The determinant of A, the rank of A, the inverse of A can all be computed in $\tilde{O}(n^{\omega})$ time, where ω<2.376 is the matrix multiplication exponent.

Therefore, we have an $\tilde{O}(n^{\omega})$ randomized algorithm to determine whether a bipartite graph has a perfect matching.

Maximum Bipartite Matching

$$A_{i,j} = \begin{cases} x_e \text{ if } v_i v_j \in E \\ 0 \text{ otherwise} \end{cases}$$

G =



A =

	V	
x_1	x_2	
		x_3
		x_4

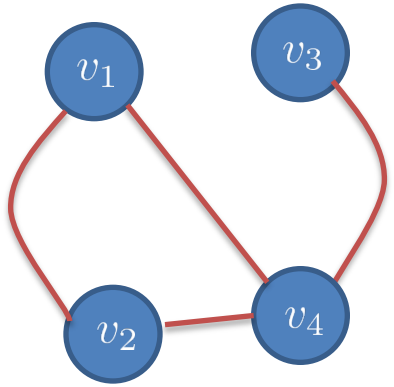
U

[Lovasz] The size of a maximum matching is equal to the rank of A.

General Matching

$$A_{i,j} = \begin{cases} x_{i,j} & \text{if } v_iv_j \in E \text{ and } i < j \\ -x_{j,i} & \text{if } v_iv_j \in E \text{ and } i > j \\ 0 & \text{otherwise} \end{cases}$$

G =



T =

	$x_{1,2}$		$x_{1,4}$
$-x_{1,2}$			$x_{2,4}$
			$x_{3,4}$
$-x_{1,4}$	$-x_{2,4}$	$-x_{3,4}$	

[Tutte] det(T)≠0 iff G has a perfect matching.

Linear Matroid Intersection

Given two matrices A and B, each of size rxn, find a maximum subset S of {1,…,n} so that the corresponding columns are linearly independent in both A and B.

A =

0	1	0	0
1	0	0	0
0	0	1	1

B =

0	1	1	0
0	1	1	1
1	0	1	0

Linear Matroid Intersection

$A =$

0	1	0	0
1	0	0	0
0	0	1	1

$B =$

0	1	1	0
0	1	1	1
1	0	1	0

$M =$

				0	1	0	0
				1	0	0	0
				0	0	1	1
				A			
0	0	1	a				
1	1	0		b			
1	1	1			c		
0	1	0				d	
B^T							

[Geelen] A and B have a common independent set of size k if and only if M is of rank at least n+k.

Linear Matroid Parity

- Given **n** column pairs (b_1,c_1) …. (b_n,c_n), each of size **r**

n=6

A =

Pair 1		Pair 2		Pair 3		Pair 4		Pair 5		Pair 6	
0	0	0	0	0	1	1	0	0	0	0	1
0	0	1	0	1	0	0	0	0	1	0	0
0	1	0	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	0	1	1	0	1	0
b_1	c_1	b_2	c_2	b_3	c_3	b_4	c_4	b_5	c_5	b_6	c_6

r=4

- Find the maximum number of pairs, so that the chosen columns are linearly independent

Linear Matroid Parity

- Given **n** column pairs (b_1,c_1) …. (b_n,c_n), each of size **r**

n=6

A =

Pair 1		Pair 2		Pair 3		Pair 4		Pair 5		Pair 6	
0	0	0	0	0	1	1	0	0	0	0	1
0	0	1	0	1	0	0	0	0	1	0	0
0	1	0	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	0	1	1	0	1	0
b_1	c_1	b_2	c_2	b_3	c_3	b_4	c_4	b_5	c_5	b_6	c_6

r=4

- Find the maximum number of pairs, so that the chosen columns are linearly independent

Linear Matroid Parity

$$M = \begin{bmatrix} A & T_0 \\ -A^T & \end{bmatrix}$$

[Geelen and Iwata] There are k pairs of independent columns if and only if rank(M) is at least 2k+2n.

Linear Matroid Parity

$$A = \begin{bmatrix} 0 & A \\ -A^T & 0 \end{bmatrix} \qquad T = \begin{bmatrix} 0 & 0 \\ 0 & T_0 \end{bmatrix}$$

[Geelen and Iwata] There are k pairs of independent columns if and only if rank(A+T) is at least 2k+2n.

Linear Matroid Parity

Lemma: Note that M=A+T. For any set S, $M_{S,S}$ is non-singular, iff there is a partition S=X\cup Y, such that $A_{X,X}$ is non-singular and $T_{Y,Y}$ is non-singular.

Lemma 2: If M is a skew symmetric matrix, and X is a maximum set of independent rows, then $M_{X,X}$ is a maximum non-singular submatrix of M.

[Geelen and Iwata] There are k pairs of independent columns if and only if rank(M) is at least 2k+2n.

Thank you for your attention!