Algebraic techniques in parameterized algorithms, Part III: Group Algebras

Łukasz Kowalik

University of Warsaw

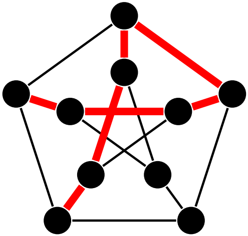
FPT School, Bedlewo, August 2014

(directed) Longest Path problem revisited.

Problem

INPUT: directed graph G, integer k.

QUESTION: Does G contain a k-vertex path?



(directed) LONGEST PATH problem revisited.

Why LONGEST PATH again?

- We have seen an $O(2^k(kn)^{O(1)})$-time algorithm using polynomials of characteristic two, labelled walks, inclusion-exclusion, etc.

(directed) LONGEST PATH problem revisited.

Why LONGEST PATH again?

- We have seen an $O(2^k(kn)^{O(1)})$-time algorithm using polynomials of characteristic two, labelled walks, inclusion-exclusion, etc.
- Today: yet another (though earlier) $O(2^k(kn)^{O(1)})$-time algorithm using **different (even more algebraic) approach** of so-called group algebras.

(directed) LONGEST PATH problem revisited.

Why LONGEST PATH again?

- We have seen an $O(2^k(kn)^{O(1)})$-time algorithm using polynomials of characteristic two, labelled walks, inclusion-exclusion, etc.
- Today: yet another (though earlier) $O(2^k(kn)^{O(1)})$-time algorithm using **different (even more algebraic) approach** of so-called group algebras.
- The lecture is based on works of Koutis (2008) and Williams (2009).

(directed) LONGEST PATH problem revisited.

Why LONGEST PATH again?

- We have seen an $O(2^k(kn)^{O(1)})$-time algorithm using polynomials of characteristic two, labelled walks, inclusion-exclusion, etc.
- Today: yet another (though earlier) $O(2^k(kn)^{O(1)})$-time algorithm using **different (even more algebraic) approach** of so-called group algebras.
- The lecture is based on works of Koutis (2008) and Williams (2009).
- Note that $O(2^k(kn)^{O(1)})$ is still unbeaten for directed graphs.

A new approach

- Introduce a variable x_v for each vertex $v \in V$.

A new approach

- Introduce a variable x_v for each vertex $v \in V$.
- Define a polynomial on variables x_v

$$P(\cdots) = \sum_{\substack{k\text{-walk} \\ v_1 v_2 \cdots v_k}} \prod_{i=1}^{k} x_{v_i}.$$

A new approach

- Introduce a variable x_v for each vertex $v \in V$.
- Define a polynomial on variables x_v

$$P(\cdots) = \sum_{\substack{k\text{-walk} \\ v_1 v_2 \cdots v_k}} \prod_{i=1}^{k} x_{v_i}.$$

- We can evaluate P using $O(k|E|)$ arithmetic operations (e.g. by DP, see previous lecture)

A new approach

- Introduce a variable x_v for each vertex $v \in V$.
- Define a polynomial on variables x_v
$$P(\cdots) = \sum_{\substack{k\text{-walk}\\ v_1 v_2 \cdots v_k}} \prod_{i=1}^{k} x_{v_i}.$$
- We can evaluate P using $O(k|E|)$ arithmetic operations (e.g. by DP, see previous lecture)
- paths (good walks) correspond to multilinear monomials in P.

A new approach

- Introduce a variable x_v for each vertex $v \in V$.
- Define a polynomial on variables x_v
$$P(\cdots) = \sum_{\substack{k\text{-walk} \\ v_1 v_2 \cdots v_k}} \prod_{i=1}^{k} x_{v_i}.$$
- We can evaluate P using $O(k|E|)$ arithmetic operations (e.g. by DP, see previous lecture)
- paths (good walks) correspond to multilinear monomials in P.
- non-path walks (bad walks) correspond to monomials containing x_v^2 for some vertex v.

Imagine...

$$P(\cdots) = \sum_{\substack{k\text{-walk} \\ v_1 v_2 \cdots v_k}} \prod_{i=1}^{k} x_{v_i}$$

Imagine a new wonderful world in which

- each term corresponding to a bad walk vanishes
- (some) terms corresponding to the good walks stay.

while we evaluate P.

Imagine...

$$P(\cdots) = \sum_{\substack{k\text{-walk} \\ v_1 v_2 \cdots v_k}} \prod_{i=1}^{k} x_{v_i}$$

Imagine a new wonderful ~~world~~ **algebraic structure** S such that if we evaluate P over S,

- a non-multilinear monomial evaluates to 0 over some subset S' of S,
- a multilinear monomial evaluates to non-zero over S' (with high probability),

Some algebra: finite fields

Some algebra: fields

Field is a triple $(F, +, \cdot)$, where

- F is a set, $+$ and $\cdot$ are binary operations
- associativity: $(a+b)+c = a+(b+c)$, $\quad (a\cdot b)\cdot c = a\cdot(b\cdot c)$
- commutativity: $a+b = b+a$, $\quad a\cdot b = b\cdot a$
- distributivity: $a\cdot(b+c) = a\cdot b + a\cdot c$.
- additive identity: $\exists\ 0 \in F$ s.t. $0 + a = a$.
- multiplicative identity: $\exists\ 1 \in F$ s.t. $\forall a \in F\setminus\{0\}:\ 1\cdot a = a$.
- additive inverses: $\forall\ a \in F\ \exists b \in F$ s.t. $a+b=0$;
- multiplicative inverses: $\forall\ a \in F\setminus\{0\}\ \exists\ b \in F$ s.t. $a\cdot b = 1$;

Some familiar (infinite) fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Some algebra: finite fields

- For every prime p and integer k there is exactly one (up to isomorphism) field of size p^k.
- We denote this field by $GF(p^k)$ (GF = Galois Field).

- For prime p, the field $GF(p)$ is the familiar set $\{0, \ldots, p-1\}$ with addition and multiplication modulo p.

$GF(2)$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Some algebra: finite fields of size p^k

- Elements of $GF(p^k)$ are univariate polynomials of degree at most $k-1$ with coefficients from $GF(p)$.
- Choose an irreducible univariate polynomial f of degree k with coefficients from $GF(p)$ (it always exists!)
- Addition and multiplication is the usual addition and multiplication of polynomials plus taking modulo f.
- Corollary: $GF(p^k)$ is of characteristic p, i.e. $\forall a \in GF(p^k)$, $\underbrace{a + a + \ldots + a}_{p \text{ times}} = 0$.

Example: $GF(2^2) = \{0, 1, x, x+1\}$. Let $f(x) = x^2 + x + 1$.

$x + (x+1) = (1+1)x + 1 = 1$

$x \cdot (x+1) = x^2 + x \bmod (x^2+x+1) = x^2+x+1+1 \bmod (x^2+x+1) = 1.$

Some algebra: finite fields of size p^k

- Elements of $GF(p^k)$ are univariate polynomials of degree at most $k-1$ with coefficients from $GF(p)$.
- Choose an irreducible univariate polynomial f of degree k with coefficients from $GF(p)$ (it always exists!)
- Addition and multiplication is the usual addition and multiplication of polynomials plus taking modulo f.
- Corollary: $GF(p^k)$ is of characteristic p, i.e. $\forall a \in GF(p^k)$, $\underbrace{a + a + \ldots + a}_{p \text{ times}} = 0$.

Example: $GF(2^2) = \{0, 1, x, x+1\}$. Let $f(x) = x^2 + x + 1$.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Finite fields of size p^k: computational complexity

- Assume $p = O(1)$.
- Addition: k additions in $GF(p)$, time $O(k)$.
- Multiplication: multiply polynomials, perform modulo f.
  - Naively: time $O(k^2)$,
  - Using FFT: time $O(k \log k \log \log k)$.

Some algebra: group algebras

Some algebra: group

Group is a pair $(G, \cdot)$, where

- G is a set, $\cdot$ is a binary operation
- associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- identity: $\exists\ 1 \in G$ s.t. $\forall a \in G:\ 1 \cdot a = a$.
- inverses: $\forall\ a \in G\ \exists b \in G$ s.t. $a \cdot b = 1$;

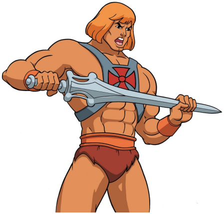
Some familiar groups: $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z}_n, +)$.
$\mathbb{Z}_n = \{0, \ldots, n-1\}$, with addition modulo n.

The group for today

The first hero of today is.....

The group for today

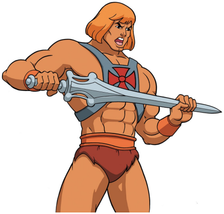
The first hero of today is.....



The group $(\mathbb{Z}_2^k, \oplus)$

The group for today

The first hero of today is.....



The group $(\mathbb{Z}_2^k, \oplus)$

$$\mathbb{Z}_2^k = \{(a_1, \ldots, a_k) \;:\; a_i \in \mathbb{Z}_2\}$$

$\oplus$ is the pointwise addition in $\mathbb{Z}_2$.

$$(0,1,1,0) \oplus (0,1,0,1) = (0,0,1,1).$$

$$(0,1,1,0)^{-1} = (1,0,0,1)$$

We denote $W_0 = (0,0,\ldots,0)$.

Some algebra: group algebra

Group algebra $F[G]$ is a triple $(S, +, \cdot)$, where

- F is a field with operations $+_F$ and $\cdot_F$ (or simply $+$, $\cdot$),
- G is a group with operation $\cdot_G$ (or simply $\cdot$),
- $S = \{\sum_{g \in G} a_g g \ : \ \forall g \in G \ a_g \in F\}$, i.e. S is the set of all **formal sums** over all elements of G with coefficients from F (note: $|S| = |F|^{|G|}$)
- $(\sum_{g \in G} a_g g) + (\sum_{g \in G} b_g g) = \sum_{g \in G} (a_g +_F b_g) g$
- $$(\sum_{g \in G} a_g g) \cdot (\sum_{g \in G} b_g g) = \sum_{\substack{g \in G \\ h \in G}} (a_g \cdot_F b_h)\, g \cdot_G h$$

Some algebra: group algebra

Group algebra $F[G]$ is a triple $(S, +, \cdot)$, where

- F is a field with operations $+_F$ and $\cdot_F$ (or simply $+$, $\cdot$),
- G is a group with operation $\cdot_G$ (or simply $\cdot$),
- $S = \{\sum_{g \in G} a_g g \;:\; \forall g \in G\; a_g \in F\}$,
  i.e. S is the set of all **formal sums** over all elements of G with coefficients from F (note: $|S| = |F|^{|G|}$)
- $(\sum_{g \in G} a_g g) + (\sum_{g \in G} b_g g) = \sum_{g \in G} (a_g +_F b_g) g$
-

$$(\sum_{g \in G} a_g g) \cdot (\sum_{g \in G} b_g g) = \cancel{\sum_{\substack{g \in G \\ h \in G}} (a_g \cdot_F b_h)\, g \cdot_G h} =$$

$$\sum_{g \in G} \left(\sum_{g_1 \cdot_G g_2 = g} (a_{g_1} \cdot_F b_{g_2}) \right) g = \sum_{g \in G} \left(\sum_{g_1 \in G} (a_{g_1} \cdot_F b_{g_1^{-1} g}) \right) g$$

Some algebra: group algebra

Group algebra $F[G]$ is a triple $(S, +, \cdot)$, where

- F is a field with operations $+_F$ and $\cdot_F$ (or simply $+$, $\cdot$),
- G is a group with operation $\cdot_G$ (or simply $\cdot$),
- $S = \{\sum_{g\in G} a_g g \ : \ \forall g \in G \ a_g \in F\}$,
  i.e. S is the set of all **formal sums** over all elements of G with coefficients from F (note: $|S| = |F|^{|G|}$)
- $$(\sum_{g\in G} a_g g) + (\sum_{g\in G} b_g g) = \sum_{g\in G}(a_g +_F b_g)g$$
- $$(\sum_{g\in G} a_g g) \cdot (\sum_{g\in G} b_g g) = \sum_{g\in G}\left(\sum_{g_1\in G}(a_{g_1} \cdot_F b_{g_1^{-1}g})\right) g$$

The group algebra for today

The main heroes of today are.....

The main heroes of today are.....

$F = GF(2^\ell)$  $G = \mathbb{Z}_2^k$

The group algebra $GF(2^\ell)[\mathbb{Z}_2^k]$

Example: $GF(2^2)[\mathbb{Z}_2^3]$

Recall that $GF(2^2) = \{0, 1, x, x+1\}$; irreducible polynomial: $x^2 + x + 1$.

Elements of $GF(2^2)[\mathbb{Z}_2^3]$ are of the form $\sum_{g \in \mathbb{Z}_2^3} a_g g$, where $a_g \in GF(2^2)$.

$\sum_{g \in \mathbb{Z}_2^3} 0g = 0$ is the additive identity.

$1 \cdot W_0 = W_0$ is the multiplicative identity (note that $W_0 \neq 0$).

$$\left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} + (1+x) \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right) + \left(\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + x \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right) =$$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} + x \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + x \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Example: $GF(2^2)[\mathbb{Z}_2^3]$

Recall that $GF(2^2) = \{0, 1, x, x+1\}$; irreducible polynomial: $x^2 + x + 1$.

Elements of $GF(2^2)[\mathbb{Z}_2^3]$ are of the form $\sum_{g \in \mathbb{Z}_2^3} a_g g$, where $a_g \in GF(2^2)$.

$$\left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} + x \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right) \cdot x \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} =$$

$$(1 \cdot x) \left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right) + (x \cdot x) \left(\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right) =$$

$$x \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + (x+1) \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} .$$

Why $GF(2^\ell)[\mathbb{Z}_2^k]$ is cool?

Vanishing Lemma (Koutis)

For every $v \in \mathbb{Z}_2^k$, $(W_0 + v)^2 = 0$ in $GF(2^\ell)[\mathbb{Z}_2^k]$.

Proof

$$\begin{aligned}
(W_0 + v)^2 &= (W_0 \oplus W_0) + (W_0 \oplus v) + (v \oplus W_0) + (v \oplus v) \\
&= \quad W_0 \quad + \quad v \quad + \quad v \quad + \quad W_0 \\
&= (1+1)W_0 + (1+1)v \\
&= 0W_0 + 0v \\
&= 0.
\end{aligned}$$

Why $GF(2^\ell)[\mathbb{Z}_2^k]$ is cool?

Vanishing Lemma (Koutis)

For every $v \in \mathbb{Z}_2^k$, $(W_0 + v)^2 = 0$ in $GF(2^\ell)[\mathbb{Z}_2^k]$.

Algorithm for Longest path

1. Let $P(x_1, \ldots, x_n) = \sum_{\substack{k\text{-walk} \\ v_1 v_2 \cdots v_k}} \prod_{i=1}^{k} x_{v_i}$
2. Pick vectors $v_1, \ldots, v_n \in \mathbb{Z}_2^k$ uniformly at random.
3. Answer YES iff $P(W_0 + v_1, \ldots, W_0 + v_n) \neq 0$.

- By Vanishing Lemma, if there is no k-path, we **always** get NO.
- We need to show that otherwise we get YES with good probability, i.e., that multilinear monomials do not vanish w.h.p.

Behaviour of multilinear monomials

Independency Lemma

If $v_1, \dots, v_k \in \mathbb{Z}_2^k$ are linearly independent over $GF(2)$, then

$$\prod_{i=1}^{k}(W_0 + v_i) = \begin{cases} \sum_{v \in \mathbb{Z}_2^k} v & \text{if } v_1, \dots, v_k \text{ are linearly independent over } GF(2) \\ 0 & \text{otherwise} \end{cases}.$$

Behaviour of multilinear monomials

Independency Lemma

If $v_1, \ldots, v_k \in \mathbb{Z}_2^k$ are linearly independent over $GF(2)$, then

$$\prod_{i=1}^{k}(W_0+v_i) = \begin{cases} \sum_{v\in\mathbb{Z}_2^k} v & \text{if } v_1,\ldots,v_k \text{ are linearly independent over } GF(2) \\ 0 & \text{otherwise} \end{cases}.$$

Proof

Assume independence. (We skip the proof for the dependent case here.)

- $\prod_{i=1}^{k}(W_0 + v_i) = \sum_{S\subseteq[k]} \bigoplus_{j\in S} v_j.$
- $\{v_1, \ldots, v_k\}$ is a basis of $\mathbb{Z}_2^k$, so $\{\bigoplus_{j\in S} v_j \ : \ S \subseteq [k]\} = \mathbb{Z}_2^k$.
- Hence, in the sum there are **all** the vectors from $\mathbb{Z}_2^k$.

Behaviour of multilinear monomials

Independency Lemma

If $v_1, \ldots, v_k \in \mathbb{Z}_2^k$ are linearly independent over $GF(2)$, then

$$\prod_{i=1}^{k}(W_0+v_i) = \begin{cases} \sum_{v\in\mathbb{Z}_2^k} v & \text{if } v_1, \ldots, v_k \text{ are linearly independent over } GF(2) \\ 0 & \text{otherwise} \end{cases}.$$

Corollary

For a path $y_1, \ldots, y_k$, if the random vectors $v_{y_1}, \ldots, v_{y_k}$ are linearly independent, then the term $\prod_{i=1}^{k}(W_0 + v_{y_i})$ evaluates to $\sum_{v\in\mathbb{Z}_2^k} v \neq 0$.

Question: What is the probability that k random vectors $v_1, \ldots, v_k \in \mathbb{Z}_2^k$ are linearly independent over $GF(2)$?

Chances of linear independence

Independency Probability Bound

Random vectors $v_1, \ldots, v_k \in \mathbb{Z}_2^k$ are linearly independent over $GF(2)$ with probability at least e^{-2}.

Proof.

How many linearly independent sequences of k vectors are there?

- Choose v_1 in $2^k - 1$ ways (avoid W_0),
- Choose v_2 in $2^k - 2$ ways (avoid W_0, v_1),
- Choose v_3 in $2^k - 2^2$ ways (avoid $\mathrm{span}(\{v_1, v_2\})$),

$$\vdots$$

- Choose v_k in $2^k - 2^{k-1}$ ways (avoid $\mathrm{span}(\{v_1, \ldots, v_{k-1}\})$),

There are $\prod_{i=0}^{k-1}(2^k - 2^i)$ linearly independent sequences of k vectors.

Chances of linear independence

Independency Probability Bound

Random vectors $v_1, \ldots, v_k \in \mathbb{Z}_2^k$ are linearly independent over $GF(2)$ with probability at least e^{-2}.

Proof.

There are $\prod_{i=0}^{k-1}(2^k - 2^i)$ linearly independent sequences of k vectors.

$$\Pr = \frac{\prod_{i=0}^{k-1}(2^k - 2^i)}{2^{k^2}} = \frac{\prod_{i=0}^{k-1} 2^k(1 - 2^i/2^k)}{2^{k^2}} = \prod_{i=0}^{k-1}(1 - 2^i/2^k)$$

Apply the inequality $1 - x \geq e^{-2x}$ for $x \in [0, \frac{1}{2}]$:

$$\Pr \geq e^{-2\sum_{i=0}^{k-1} 2^i/2^k} = e^{-2(2^k-1)/2^k} \geq e^{-2}.$$

Multilinear monomials, cont'd.

Assume there is a k-path $y_1, \ldots, y_k$ (if more, take any.)

Corollary

$$\prod_{i=1}^{k}(W_0 + v_{y_i}) = \sum_{v \in \mathbb{Z}_2^k} v \text{ with probability at least } e^{-2}.$$

Multilinear monomials, cont'd.

Assume there is a k-path $y_1, \ldots, y_k$ (if more, take any.)

Corollary

$\prod_{i=1}^{k}(W_0 + v_{y_i}) = \sum_{v \in \mathbb{Z}_2^k} v$ with probability at least e^{-2}.

Question

Does it mean that with probability at least e^{-2} P evaluates to non-zero?

Multilinear monomials, cont'd.

Assume there is a k-path $y_1, \ldots, y_k$ (if more, take any.)

Corollary

$$\prod_{i=1}^{k}(W_0 + v_{y_i}) = \sum_{v \in \mathbb{Z}_2^k} v \text{ with probability at least } e^{-2}.$$

Question

Does it mean that with probability at least e^{-2} P evaluates to non-zero?

Answer

NO! The term $\sum_{v \in \mathbb{Z}_2^k} v$ may cancel with identical terms originating from other multilinear monomials.

How can we prevent the cancelling?

Multilinear monomials, cont'd.

The final trick

1. Pick $|E|$ elements $\{w_e \ : \ e \in E\} \subseteq GF(2^\ell)$ uniformly at random.
2. Pick vectors $v_1, \ldots, v_n \in \mathbb{Z}_2^k$ uniformly at random.
3. Let $P'(\mathbf{x}, \mathbf{y}) = \sum_{\substack{k\text{-walk} \\ v_1 v_2 \cdots v_k}} \prod_{i=1}^{k} x_{v_i} \prod_{i=1}^{k-1} y_{v_i v_{i+1}}$
4. Answer YES iff $P'(W_0 + v_1, \ldots, W_0 + v_n, w_{e_1} W_0, \ldots, w_{e_{|E|}} W_0) \neq 0$.

Hence, for some k-paths $P_1, \ldots, P_r$, $r \geq 0$, $P_j = y_{j,1}, \cdots, y_{j,k}$ we have $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0) = \left(\sum_{j=1}^{r} \prod_{i=1}^{k-1} w_{y_{j,i} y_{j,i+1}} \right) \sum_{v \in \mathbb{Z}_2^k} v$, and our favourite path $y_1, \ldots, y_k$ is among $P_1, \ldots, P_r$ with prob. $\geq e^{-2}$.

Multilinear monomials, cont'd.

For some k-paths $P_1, \ldots, P_r$, $r \geq 0$, $P_j = y_{j,1}, \cdots, y_{j,k}$ we have $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0) = \left(\sum_{j=1}^{r} \prod_{i=1}^{k-1} w_{y_{j,i} y_{j,i+1}}\right) \sum_{v \in \mathbb{Z}_2^k} v$, and our favourite path $y_1, \ldots, y_k$ is among $P_1, \ldots, P_r$ with prob. $\geq e^{-2}$.

Multilinear monomials, cont'd.

For some k-paths $P_1, \ldots, P_r$, $r \geq 0$, $P_j = y_{j,1}, \cdots, y_{j,k}$ we have

$$P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0) = \left(\sum_{j=1}^{r} \prod_{i=1}^{k-1} w_{y_{j,i} y_{j,i+1}} \right) \sum_{v \in \mathbb{Z}_2^k} v,$$

and our favourite path $y_1, \ldots, y_k$ is among $P_1, \ldots, P_r$ with prob. $\geq e^{-2}$.

Consider the polynomial $Q(w_{e_1}, \ldots, w_{e_{|E|}}) = \sum_{j=1}^{r} \prod_{i=1}^{k-1} w_{y_{j,i} y_{j,i+1}}$.

Schwartz-Zippel Lemma

Let $p(x_1, x_2, \ldots, x_n)$ be a non-zero polynomial of degree at most d over a field F and let S be a finite subset of F. Sample values $a_1, a_2, \ldots, a_n$ from S uniformly at random. Then, $Pr[p(a_1, a_2, \ldots, a_n)] = 0] \leq d/|S|$.

If $\ell > \lceil \log k \rceil + 1$, then $Pr[Q(w_{e_1}, \ldots, w_{e_{|E|}}) \neq 0] \geq \frac{1}{2}$.

Conclusion

Theorem

- If there is no k-path, $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0)$ evaluates to 0.
- If there is a k-path, $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0)$ evaluates to non-zero with probability at least $1/(2e^2)$.

Conclusion

Theorem

- If there is no k-path, $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0)$ evaluates to 0.
- If there is a k-path, $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0)$ evaluates to non-zero with probability at least $1/(2e^2)$.

P' can be evaluated using $O(mk)$ arithmetic operations in $GF(2^\ell)[\mathbb{Z}_2^k]$.

Conclusion

Theorem

- If there is no k-path, $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0)$ evaluates to 0.
- If there is a k-path, $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0)$ evaluates to non-zero with probability at least $1/(2e^2)$.

P' can be evaluated using $O(mk)$ arithmetic operations in $GF(2^\ell)[\mathbb{Z}_2^k]$.

Have we just proved $RP = NP$?

Conclusion

Theorem

- If there is no k-path, $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0)$ evaluates to 0.
- If there is a k-path, $P'(W_0 + v_1, \ldots, w_{e_{|E|}} W_0)$ evaluates to non-zero with probability at least $1/(2e^2)$.

P' can be evaluated using $O(mk)$ arithmetic operations in $GF(2^\ell)[\mathbb{Z}_2^k]$.

Have we just proved $RP = NP$?

Not yet, what is the time complexity of $GF(2^\ell)[\mathbb{Z}_2^k]$ arithmetic?

$GF(2^\ell)[\mathbb{Z}_2^k]$ arithmetic

- Elements of $GF(2^\ell)[\mathbb{Z}_2^k]$ are of form $\sum_{g\in\mathbb{Z}_2^k} a_g g$
- We can represent them by vectors of 2^k elements from $GF(2^\ell)$.
- Addition takes $O(2^k)$ additions in $GF(2^\ell)$ (in time $O(\ell) = O(\log k)$)
- Multiplication done naively takes $O(4^k)$ multiplications in $GF(2^\ell)$ (in time $O(\ell \log \ell \log\log \ell) = O(\log k(\log\log k)^2)$
- We can implement multiplication in an FFT style in $O(2^k k)$ time and $O(2^k k)$ space.

Theorem (Williams 2009)

The algorithm we have just seen works in $O(2^k|E|k \log k(\log\log k)^2)$ time and $O(2^k k)$ space.

Note: Multiplication can be done in polynomial space as well (Koutis).

Take-home message

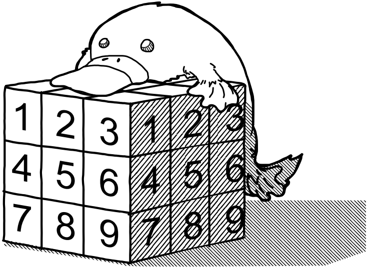
We have seen applications of three algebraic tools:

- Inclusion-Exclusion,
- Polynomials over finite fields of characteristic two,
- Group algebras.

A **common theme**:

- Relax your constraints (walks instead of paths, cycle covers instead of Hamiltonian cycles, etc...)
- Some unwanted ("bad") objects appear
- Using an algebraic tool, make the bad objects disappear, so that the good objects stay.

The end



Thank you!