Symmetrizing sum of squares polynomials on the hypercube.

Anupam Prakash,
Center for Quantum Technologies and
Nanyang Technological University, Singapore.

February 1, 2016

Based on joint work with Troy Lee, Ronald De Wolf and Henry Yuen.
Arxiv:1601.02311.

Overview

1. Grigoriev's knapsack lower bound

2. Symmetrizing SoS polynomials on hypercube

3. Blekherman's theorem

Positivestellensatz refutations

- Consider the polynomial system $f(x) = r, f_i(x) = 0 \; \forall i \in [n]$, a refutation of the system is a proof that the system has no solutions.

Positivestellensatz refutations

- Consider the polynomial system $f(x) = r, f_i(x) = 0 \; \forall i \in [n]$, a refutation of the system is a proof that the system has no solutions.
- A Positivestellensatz refutation of degree d is an identity of the form:

$$g(x)(f(x) - r) + \sum_{i=1}^{n} g_i(x) f_i(x) = 1 + h(x) \ .$$

where $deg(fg) \leq d, deg(f_i g_i) \leq d$ and $h(x) = \sum_i h_i(x)^2$ with $deg(h_i) \leq d/2$.

Positivestellensatz refutations

- Consider the polynomial system $f(x) = r, f_i(x) = 0 \; \forall i \in [n]$, a refutation of the system is a proof that the system has no solutions.
- A Positivestellensatz refutation of degree d is an identity of the form:

$$g(x)(f(x) - r) + \sum_{i=1}^{n} g_i(x) f_i(x) = 1 + h(x) \ .$$

  where $deg(fg) \le d, deg(f_i g_i) \le d$ and $h(x) = \sum_i h_i(x)^2$ with $deg(h_i) \le d/2$.
- If there is a solution x to the polynomial system, the left side evaluates to 0 while the right side is at least 1.

Positivestellensatz refutations

- Consider the polynomial system $f(x) = r, f_i(x) = 0 \ \forall i \in [n]$, a refutation of the system is a proof that the system has no solutions.
- A Positivestellensatz refutation of degree d is an identity of the form:

$$g(x)(f(x) - r) + \sum_{i=1}^{n} g_i(x) f_i(x) = 1 + h(x) \ .$$

where $deg(fg) \leq d, deg(f_i g_i) \leq d$ and $h(x) = \sum_i h_i(x)^2$ with $deg(h_i) \leq d/2$.

- If there is a solution x to the polynomial system, the left side evaluates to 0 while the right side is at least 1.
- How to lower bound the degree of Positivestellensatz refutations?

Pseudo Expectations

- A degree-d pseudo-expectation $\widetilde{E}$ is a linear function on the space of degree-d polynomials such that $\widetilde{E}[h^2] \geq 0$ for all h s.t. $deg(h) \leq d/2$.

Pseudo Expectations

- A degree-d pseudo-expectation $\widetilde{E}$ is a linear function on the space of degree-d polynomials such that $\widetilde{E}[h^2] \geq 0$ for all h s.t. $deg(h) \leq d/2$.
- Construct a pseudo-expectation $\widetilde{E}[f_i(x)g_i(x)] = 0$ and $\widetilde{E}[(f(x) - r).g(x)] = 0$ for all polynomials $g(x), g_i(x)$ such that $deg(f_i g), deg(fg) \leq d$.

Pseudo Expectations

- A degree-d pseudo-expectation $\widetilde{E}$ is a linear function on the space of degree-d polynomials such that $\widetilde{E}[h^2] \geq 0$ for all h s.t. $deg(h) \leq d/2$.
- Construct a pseudo-expectation $\widetilde{E}[f_i(x)g_i(x)] = 0$ and $\widetilde{E}[(f(x) - r).g(x)] = 0$ for all polynomials $g(x), g_i(x)$ such that $deg(f_i g), deg(fg) \leq d$.
- Suppose there is a Positivestellensatz refutation of degree d,

$$g(x)(f(x) - r) + \sum_{i=1}^{n} g_i(x) f_i(x) = 1 + h(x) \ .$$

Pseudo Expectations

- A degree-d pseudo-expectation $\widetilde{E}$ is a linear function on the space of degree-d polynomials such that $\widetilde{E}[h^2] \geq 0$ for all h s.t. $deg(h) \leq d/2$.
- Construct a pseudo-expectation $\widetilde{E}[f_i(x)g_i(x)] = 0$ and $\widetilde{E}[(f(x) - r).g(x)] = 0$ for all polynomials $g(x), g_i(x)$ such that $deg(f_i g), deg(fg) \leq d$.
- Suppose there is a Positivestellensatz refutation of degree d,

$$g(x)(f(x) - r) + \sum_{i=1}^{n} g_i(x) f_i(x) = 1 + h(x) \ .$$

- Then the pseudo-expectation function $\widetilde{E}$ for the left side evaluates to 0, while that for the right side is at least 1.

The knapsack system

- The knapsack system consists of the equations $\sum_i x_i = r$ where $r \notin \mathbb{Z}$ and $x_i^2 = x_i, \forall i \in [n]$. Clearly there is no solution.

The knapsack system

- The knapsack system consists of the equations $\sum_i x_i = r$ where $r \notin \mathbb{Z}$ and $x_i^2 = x_i, \forall i \in [n]$. Clearly there is no solution.
- What is the degree of the PS refutation for the knapsack?

$$g(x) \cdot \left(\sum_{i=1}^{n} x_i - r \right) + \sum_{i=1}^{n} g_i(x) \cdot (x_i^2 - x_i) = 1 + h(x) \ .$$

The knapsack system

- The knapsack system consists of the equations $\sum_i x_i = r$ where $r \notin \mathbb{Z}$ and $x_i^2 = x_i, \forall i \in [n]$. Clearly there is no solution.
- What is the degree of the PS refutation for the knapsack?

$$g(x) \cdot \left(\sum_{i=1}^{n} x_i - r \right) + \sum_{i=1}^{n} g_i(x) \cdot (x_i^2 - x_i) = 1 + h(x) \ .$$

The knapsack system

- The knapsack system consists of the equations $\sum_i x_i = r$ where $r \notin \mathbb{Z}$ and $x_i^2 = x_i, \forall i \in [n]$. Clearly there is no solution.
- What is the degree of the PS refutation for the knapsack?

$$g(x) \cdot \left(\sum_{i=1}^{n} x_i - r \right) + \sum_{i=1}^{n} g_i(x) \cdot (x_i^2 - x_i) = 1 + h(x) \ .$$

- **Theorem (Grigoriev 01)**

  If $0 < r < (n-1)/2$, then there is no Positivstellensatz refutation of the knapsack system with parameter r with degree $2\lfloor r \rfloor + 2$.

Grigoriev's proof

- The proof defines a pseudo-expectation $\widetilde{E}$ on monomials:

$$\widetilde{E}[x^S] = \frac{r.(r-1).\cdots.(r-|S|+1)}{n.(n-1).\cdots.(n-|S|+1)}$$

and by extension on all multilinear polynomials.

Grigoriev's proof

- The proof defines a pseudo-expectation $\widetilde{E}$ on monomials:

$$\widetilde{E}[x^S] = \frac{r.(r-1).\cdots.(r-|S|+1)}{n.(n-1).\cdots.(n-|S|+1)}$$

  and by extension on all multilinear polynomials.
- It is easy to show that $\widetilde{E}[g.(\sum_i x_i - r)] = 0$.

Grigoriev's proof

- The proof defines a pseudo-expectation $\widetilde{E}$ on monomials:

$$\widetilde{E}[x^S] = \frac{r.(r-1).\cdots.(r-|S|+1)}{n.(n-1).\cdots.(n-|S|+1)}$$

  and by extension on all multilinear polynomials.
- It is easy to show that $\widetilde{E}[g.(\sum_i x_i - r)] = 0$.
- The proof of positivity $\widetilde{E}[h^2] \geq 0$ if $deg(h) \leq \lfloor r \rfloor + 2$ is involved.

Grigoriev's proof

- The proof defines a pseudo-expectation $\widetilde{E}$ on monomials:

$$\widetilde{E}[x^S] = \frac{r.(r-1).\cdots.(r-|S|+1)}{n.(n-1).\cdots.(n-|S|+1)}$$

  and by extension on all multilinear polynomials.
- It is easy to show that $\widetilde{E}[g.(\sum_i x_i - r)] = 0$.
- The proof of positivity $\widetilde{E}[h^2] \geq 0$ if $deg(h) \leq \lfloor r \rfloor + 2$ is involved.
- We present here a simple proof of Grigoriev's lower bound.

Grigoriev's proof

- The proof defines a pseudo-expectation $\widetilde{E}$ on monomials:

$$\widetilde{E}[x^S] = \frac{r.(r-1).\cdots.(r-|S|+1)}{n.(n-1).\cdots.(n-|S|+1)}$$

  and by extension on all multilinear polynomials.
- It is easy to show that $\widetilde{E}[g.(\sum_i x_i - r)] = 0$.
- The proof of positivity $\widetilde{E}[h^2] \geq 0$ if $deg(h) \leq \lfloor r \rfloor + 2$ is involved.
- We present here a simple proof of Grigoriev's lower bound.
- All known Sum of Squares hierarchy lower bounds reduce to either the $3XOR$ or knapsack lower bounds of Grigoriev.

Symmetric polynomials on the hypercube

- Let M_n be the space of n-variate multilinear polynomials.

Symmetric polynomials on the hypercube

- Let M_n be the space of n-variate multilinear polynomials.
- M_n is the coordinate ring of the hypercube $H = \{0, 1\}^n$, that is $M_n := \mathbb{R}[x_1, x_2, \cdots, x_n]/\langle x_i^2 - x_i : i \in [n]\rangle$.

Symmetric polynomials on the hypercube

- Let M_n be the space of n-variate multilinear polynomials.
- M_n is the coordinate ring of the hypercube $H = \{0,1\}^n$, that is $M_n := \mathbb{R}[x_1, x_2, \cdots, x_n]/\langle x_i^2 - x_i : i \in [n]\rangle$.
- The symmetric group S_n acts on M_n by permuting the indices of the monomials.

Symmetric polynomials on the hypercube

- Let M_n be the space of n-variate multilinear polynomials.
- M_n is the coordinate ring of the hypercube $H = \{0,1\}^n$, that is $M_n := \mathbb{R}[x_1, x_2, \cdots, x_n]/\langle x_i^2 - x_i : i \in [n]\rangle$.
- The symmetric group S_n acts on M_n by permuting the indices of the monomials.
- Example: If $\sigma(1234) = 3142$ then $\sigma(x_1x_2 + x_3x_4) = x_3x_1 + x_4x_2$.

Symmetric polynomials on the hypercube

- Let M_n be the space of n-variate multilinear polynomials.
- M_n is the coordinate ring of the hypercube $H = \{0,1\}^n$, that is $M_n := \mathbb{R}[x_1, x_2, \cdots, x_n]/\langle x_i^2 - x_i : i \in [n]\rangle$.
- The symmetric group S_n acts on M_n by permuting the indices of the monomials.
- Example: If $\sigma(1234) = 3142$ then $\sigma(x_1x_2 + x_3x_4) = x_3x_1 + x_4x_2$.
- A multilinear polynomial can be symmetrized:

$$\mathsf{Sym}(p)(x) := \frac{1}{n!} \sum_{\sigma \in S_n} p(\sigma x)$$

Symmetric polynomials on the hypercube

- Let M_n be the space of n-variate multilinear polynomials.
- M_n is the coordinate ring of the hypercube $H = \{0,1\}^n$, that is $M_n := \mathbb{R}[x_1, x_2, \cdots, x_n]/\langle x_i^2 - x_i : i \in [n]\rangle$.
- The symmetric group S_n acts on M_n by permuting the indices of the monomials.
- Example: If $\sigma(1234) = 3142$ then $\sigma(x_1x_2 + x_3x_4) = x_3x_1 + x_4x_2$.
- A multilinear polynomial can be symmetrized:

$$\mathsf{Sym}(p)(x) := \frac{1}{n!} \sum_{\sigma \in S_n} p(\sigma x)$$

- What is the symmetrization the degree 2 monomial x_1x_2?

Symmetrization

- Sym$(x_1x_2) = \frac{1}{n!}\sum_\sigma \sigma(x_1x_2) = \frac{(n-2)!2!}{n!}\sum_{i\neq j} x_ix_j$.

Symmetrization

- Sym$(x_1x_2) = \frac{1}{n!}\sum_\sigma \sigma(x_1x_2) = \frac{(n-2)!2!}{n!}\sum_{i\neq j} x_ix_j$.
- Let $x \in \{0,1\}^n$ and $|x| = \sum_i x_i$,

$$\mathrm{Sym}(x_1x_2\cdots x_k) = \frac{\binom{|x|}{k}}{\binom{n}{k}} = \frac{|x|.(|x|-1).\cdots.(|x|-k+1)}{n.(n-1).\cdots.(n-k+1)}$$

Symmetrization

- Sym$(x_1x_2) = \frac{1}{n!}\sum_\sigma \sigma(x_1x_2) = \frac{(n-2)!2!}{n!}\sum_{i\neq j} x_ix_j$.
- Let $x \in \{0,1\}^n$ and $|x| = \sum_i x_i$,

$$\text{Sym}(x_1x_2\cdots x_k) = \frac{\binom{|x|}{k}}{\binom{n}{k}} = \frac{|x|.(|x|-1).\cdots.(|x|-k+1)}{n.(n-1).\cdots.(n-k+1)}$$

- In fact, this is an identity over M_n valid for all x.

Symmetrization

- Sym$(x_1x_2) = \frac{1}{n!}\sum_\sigma \sigma(x_1x_2) = \frac{(n-2)!2!}{n!}\sum_{i\neq j} x_ix_j$.
- Let $x \in \{0,1\}^n$ and $|x| = \sum_i x_i$,

$$\text{Sym}(x_1x_2\cdots x_k) = \frac{\binom{|x|}{k}}{\binom{n}{k}} = \frac{|x|.(|x|-1).\cdots.(|x|-k+1)}{n.(n-1).\cdots.(n-k+1)}$$

- In fact, this is an identity over M_n valid for all x.
- The symmetrization Sym$(p)(x)$ is a univariate polynomial in $z = |x|$ and is denoted as Sym$^{uni}(p)(z)$.

Symmetrization

- Sym$(x_1x_2) = \frac{1}{n!}\sum_\sigma \sigma(x_1x_2) = \frac{(n-2)!2!}{n!}\sum_{i\neq j} x_ix_j$.
- Let $x \in \{0,1\}^n$ and $|x| = \sum_i x_i$,

$$\text{Sym}(x_1x_2\cdots x_k) = \frac{\binom{|x|}{k}}{\binom{n}{k}} = \frac{|x|.(|x|-1).\cdots.(|x|-k+1)}{n.(n-1).\cdots.(n-k+1)}$$

- In fact, this is an identity over M_n valid for all x.
- The symmetrization Sym$(p)(x)$ is a univariate polynomial in $z = |x|$ and is denoted as Sym$^{uni}(p)(z)$.
- Is the symmetrization of a square polynomial Sym$^{uni}(p^2)(z)$ positive on $[0,n]$? What are its positivity properties?

Symmetrizing squares

- If $p = x_1 x_2$, then $\text{Sym}^{uni}(p^2)(z) = \frac{z.(z-1)}{n.(n-1)}$ is negative for $z \in (0, 1)$.

Symmetrizing squares

- If $p = x_1 x_2$, then $\mathrm{Sym}^{uni}(p^2)(z) = \frac{z.(z-1)}{n.(n-1)}$ is negative for $z \in (0, 1)$.
- However, $\mathrm{Sym}^{uni}(p^2)(z)$ is positive on the integer points $z \in [0, n]$.

Symmetrizing squares

- If $p = x_1 x_2$, then $\mathrm{Sym}^{uni}(p^2)(z) = \frac{z.(z-1)}{n.(n-1)}$ is negative for $z \in (0, 1)$.
- However, $\mathrm{Sym}^{uni}(p^2)(z)$ is positive on the integer points $z \in [0, n]$.

Symmetrizing squares

- If $p = x_1x_2$, then Sym$^{uni}(p^2)(z) = \frac{z.(z-1)}{n.(n-1)}$ is negative for $z \in (0,1)$.
- However, Sym$^{uni}(p^2)(z)$ is positive on the integer points $z \in [0,n]$.

- **Theorem (Blekherman)**

The polynomial Sym$^{uni}(p^2)(z)$ where $deg(p) = d, d \leq n/2$ can be expressed as

$$\begin{aligned} \mathit{Sym}^{uni}(p^2)(z) = q_d(z) + z(n-z)q_{d-1}(z) + \cdots \\ \cdots z(z-1)(n-z)(n-1-z)q_{d-2}(z) + \cdots \\ \cdots + \prod_{0 \leq i < t} (z-i)(n-z-i)q_0(z) \end{aligned} \tag{1}$$

where $q_t(z)$ is a sum of squares of degree at most t polynomials.

Positivity properties

- Symmetrization of the sum of squares of degree-d polynomials on the hypercube is a positive combination of $(d + 1)$ terms.

Positivity properties

- Symmetrization of the sum of squares of degree-d polynomials on the hypercube is a positive combination of $(d+1)$ terms.
- Eg: If polynomials p_i have degree at most 2, then Sym$^{uni}(\sum_i p_i^2)$ has the expansion:

$$q_2(z) + z(n-z)q_1(z) + z(z-1)(n-z)(n-z-1)q_0(x).$$

Positivity properties

- Symmetrization of the sum of squares of degree-d polynomials on the hypercube is a positive combination of $(d+1)$ terms.
- Eg: If polynomials p_i have degree at most 2, then $\text{Sym}^{uni}(\sum_i p_i^2)$ has the expansion:

$$q_2(z) + z(n-z)q_1(z) + z(z-1)(n-z)(n-z-1)q_0(x).$$

- The SoS polynomial $q_{d-i}(x)$ is multiplied by a polynomial that is non negative on $[i-1, n-i+1]$.

Positivity properties

- Symmetrization of the sum of squares of degree-d polynomials on the hypercube is a positive combination of $(d+1)$ terms.
- Eg: If polynomials p_i have degree at most 2, then $\text{Sym}^{uni}(\sum_i p_i^2)$ has the expansion:

$$q_2(z) + z(n-z)q_1(z) + z(z-1)(n-z)(n-z-1)q_0(x).$$

- The SoS polynomial $q_{d-i}(x)$ is multiplied by a polynomial that is non negative on $[i-1, n-i+1]$.
- The $i+1$st term in the expansion is therefore non negative in the interval $[i-1, n-i+1]$.

Positivity properties

- Symmetrization of the sum of squares of degree-d polynomials on the hypercube is a positive combination of $(d+1)$ terms.
- Eg: If polynomials p_i have degree at most 2, then Sym$^{uni}(\sum_i p_i^2)$ has the expansion:

$$q_2(z) + z(n-z)q_1(z) + z(z-1)(n-z)(n-z-1)q_0(x).$$

- The SoS polynomial $q_{d-i}(x)$ is multiplied by a polynomial that is non negative on $[i-1, n-i+1]$.
- The $i+1$st term in the expansion is therefore non negative in the interval $[i-1, n-i+1]$.
- Sym$^{uni}(\sum_i p_i^2)$ is non negative on $[d-1, n-d+1]$ if $deg(p_i) \leq d$.

Proof of Grigoriev's bound

- How does Grigoriev's certificate $\widetilde{E}[p]$ relate to symmetric polynomials?

Proof of Grigoriev's bound

- How does Grigoriev's certificate $\widetilde{E}[p]$ relate to symmetric polynomials?
- $$\widetilde{E}[p] = \mathsf{Sym}^{uni}(p)(r)$$

Proof of Grigoriev's bound

- How does Grigoriev's certificate $\widetilde{E}[p]$ relate to symmetric polynomials?
- $$\widetilde{E}[p] = \mathsf{Sym}^{uni}(p)(r)$$
- By the previous slide, $\mathsf{Sym}^{uni}(p^2)(r) \geq 0$ if $deg(p) \leq d$ and $r \in [d-1, n-d+1]$.

Proof of Grigoriev's bound

- How does Grigoriev's certificate $\widetilde{E}[p]$ relate to symmetric polynomials?
- $$\widetilde{E}[p] = \mathsf{Sym}^{uni}(p)(r)$$
- By the previous slide, $\mathsf{Sym}^{uni}(p^2)(r) \geq 0$ if $deg(p) \leq d$ and $r \in [d-1, n-d+1]$.
- Grigoriev's certificate is positive if the degree $d \leq \lfloor r \rfloor + 1$.

Proof of Grigoriev's bound

- How does Grigoriev's certificate $\widetilde{E}[p]$ relate to symmetric polynomials?
- $$\widetilde{E}[p] = \mathsf{Sym}^{uni}(p)(r)$$
- By the previous slide, $\mathsf{Sym}^{uni}(p^2)(r) \geq 0$ if $deg(p) \leq d$ and $r \in [d-1, n-d+1]$.
- Grigoriev's certificate is positive if the degree $d \leq \lfloor r \rfloor + 1$.

Proof of Grigoriev's bound

- How does Grigoriev's certificate $\widetilde{E}[p]$ relate to symmetric polynomials?
- $$\widetilde{E}[p] = \mathsf{Sym}^{uni}(p)(r)$$
- By the previous slide, $\mathsf{Sym}^{uni}(p^2)(r) \geq 0$ if $deg(p) \leq d$ and $r \in [d-1, n-d+1]$.
- Grigoriev's certificate is positive if the degree $d \leq \lfloor r \rfloor + 1$.
- **Theorem (Grigoriev 01)**

  If $0 < r < (n-1)/2$, then there is no Positivstellensatz refutation of the knapsack system with parameter r with degree $2\lfloor r \rfloor + 2$.

Partial derivatives

- Let W_t be the operator that sums over partial derivatives of a degree-t polynomial,

$$W_t p(x) = \left(\sum_{i \in [n]} \frac{\partial}{\partial x_i} \right) p(x) \ .$$

Partial derivatives

- Let W_t be the operator that sums over partial derivatives of a degree-t polynomial,

$$W_t p(x) = \left(\sum_{i \in [n]} \frac{\partial}{\partial x_i} \right) p(x) \ .$$

- Example: $W_3(x_1 x_2 x_3) = x_1 x_2 + x_2 x_3 + x_3 x_1$.

Partial derivatives

- Let W_t be the operator that sums over partial derivatives of a degree-t polynomial,

$$W_t p(x) = \left(\sum_{i \in [n]} \frac{\partial}{\partial x_i} \right) p(x) \ .$$

- Example: $W_3(x_1 x_2 x_3) = x_1 x_2 + x_2 x_3 + x_3 x_1$.
- For $t > 0$, the matrix W_t has rows, columns indexed by $S, T \subset [n]$ with $|S| = t - 1$ and $|T| = t$ and $(W_t)_{S,T} = 1$ if $S \subset T$ and 0 otherwise.

Partial derivatives

- Let W_t be the operator that sums over partial derivatives of a degree-t polynomial,

$$W_t p(x) = \left(\sum_{i \in [n]} \frac{\partial}{\partial x_i} \right) p(x) \ .$$

- Example: $W_3(x_1 x_2 x_3) = x_1 x_2 + x_2 x_3 + x_3 x_1$.
- For $t > 0$, the matrix W_t has rows, columns indexed by $S, T \subset [n]$ with $|S| = t - 1$ and $|T| = t$ and $(W_t)_{S,T} = 1$ if $S \subset T$ and 0 otherwise.
- The transpose acts as a multiplication operator:

$$W_t^T x^S = \sum_{i \notin S} x^{S \cup \{i\}} = x^S (|x| - t + 1) \ .$$

Johnson graphs and $Ker(W_t)$

- W_t has a non trivial kernel as its domain has dimension $\binom{n}{t}$ while the image has dimension at most $\binom{n}{t-1}$.

Johnson graphs and $Ker(W_t)$

- W_t has a non trivial kernel as its domain has dimension $\binom{n}{t}$ while the image has dimension at most $\binom{n}{t-1}$.
- Johnson graph: $J(n,t)$ has vertices corresponding to the t subsets of $[n]$ with S,T adjacent if $|S \cap T| = t-1$.

Johnson graphs and $Ker(W_t)$

- W_t has a non trivial kernel as its domain has dimension $\binom{n}{t}$ while the image has dimension at most $\binom{n}{t-1}$.
- Johnson graph: $J(n,t)$ has vertices corresponding to the t subsets of $[n]$ with S,T adjacent if $|S \cap T| = t-1$.
- We have the relations:

$$\begin{aligned} W_t^T W_t &= tI + A_J(n,t) \\ W_t W_t^T &= (n-t+1)I + A_J(n,t-1) \ . \end{aligned} \tag{2}$$

Johnson graphs and $Ker(W_t)$

- W_t has a non trivial kernel as its domain has dimension $\binom{n}{t}$ while the image has dimension at most $\binom{n}{t-1}$.
- Johnson graph: $J(n,t)$ has vertices corresponding to the t subsets of $[n]$ with S, T adjacent if $|S \cap T| = t - 1$.
- We have the relations:

$$\begin{aligned} W_t^T W_t &= tI + A_J(n,t) \\ W_t W_t^T &= (n-t+1)I + A_J(n,t-1) \ . \end{aligned} \tag{2}$$

- $Ker(W_t)$ is the eigenspaces of Johnson graph $J(n,t)$ with eigenvalue $-t$.

Johnson graphs and $Ker(W_t)$

- W_t has a non trivial kernel as its domain has dimension $\binom{n}{t}$ while the image has dimension at most $\binom{n}{t-1}$.
- Johnson graph: $J(n,t)$ has vertices corresponding to the t subsets of $[n]$ with S, T adjacent if $|S \cap T| = t-1$.
- We have the relations:

$$\begin{aligned} W_t^T W_t &= tI + A_J(n,t) \\ W_t W_t^T &= (n-t+1)I + A_J(n,t-1) \ . \end{aligned} \tag{2}$$

- $Ker(W_t)$ is the eigenspaces of Johnson graph $J(n,t)$ with eigenvalue $-t$.
- The dimension of $Ker(W_t)$ is $\binom{n}{t} - \binom{n}{t-1}$, this follows from the spectrum of the Johnson graph.

The representations of S_n

- The symmetric group S_n acts on the polynomial ring M_n by permuting indices of monomials.

The representations of S_n

- The symmetric group S_n acts on the polynomial ring M_n by permuting indices of monomials.
- An irreducible representation is a subspace of M_n invariant under the action of S_n that do not contain non trivial invariant subspaces.

The representations of S_n

- The symmetric group S_n acts on the polynomial ring M_n by permuting indices of monomials.
- An irreducible representation is a subspace of M_n invariant under the action of S_n that do not contain non trivial invariant subspaces.
- The subspace of degree t polynomials is invariant under S_n. Is it an irreducible representation?

The representations of S_n

- The symmetric group S_n acts on the polynomial ring M_n by permuting indices of monomials.
- An irreducible representation is a subspace of M_n invariant under the action of S_n that do not contain non trivial invariant subspaces.
- The subspace of degree t polynomials is invariant under S_n. Is it an irreducible representation?
- It contains a non trivial invariant subspace $Ker(W_t)$ as it the kernel of a 'symmetric' differential operator.

The representations of S_n

- The symmetric group S_n acts on the polynomial ring M_n by permuting indices of monomials.
- An irreducible representation is a subspace of M_n invariant under the action of S_n that do not contain non trivial invariant subspaces.
- The subspace of degree t polynomials is invariant under S_n. Is it an irreducible representation?
- It contains a non trivial invariant subspace $Ker(W_t)$ as it the kernel of a 'symmetric' differential operator.
- It turns out that the $Ker(W_t)$ are the irreducible representations of S_n, this follows in a more general setting from the intersecting kernels theorem of G.D.James.

An explicit basis for $Ker(W_t)$.

- Example: The polynomial $p(x) = (x_1 - x_2).(x_3 - x_4).(x_5 - x_6)$ belongs to $Ker(W_3)$.

An explicit basis for $Ker(W_t)$.

- Example: The polynomial $p(x) = (x_1 - x_2).(x_3 - x_4).(x_5 - x_6)$ belongs to $Ker(W_3)$.
- Partial derivatives of $p(x)$ cancel in pairs: $\frac{\partial p}{\partial x_1} = -\frac{\partial p}{\partial x_2} = (x_3 - x_4).(x_5 - x_6)$.

An explicit basis for $Ker(W_t)$.

- Example: The polynomial $p(x) = (x_1 - x_2).(x_3 - x_4).(x_5 - x_6)$ belongs to $Ker(W_3)$.
- Partial derivatives of $p(x)$ cancel in pairs: $\frac{\partial p}{\partial x_1} = -\frac{\partial p}{\partial x_2} = (x_3 - x_4).(x_5 - x_6)$.
- For an array $\mathcal{A} = (a(1), a(2), \ldots, a(2t))$ let $p_{\mathcal{A}}(x) := \prod_{i \in [t]} (x_{a(2i-1)} - x_{a(2i)})$.

An explicit basis for $Ker(W_t)$.

- Example: The polynomial $p(x) = (x_1 - x_2).(x_3 - x_4).(x_5 - x_6)$ belongs to $Ker(W_3)$.
- Partial derivatives of $p(x)$ cancel in pairs: $\frac{\partial p}{\partial x_1} = -\frac{\partial p}{\partial x_2} = (x_3 - x_4).(x_5 - x_6)$.
- For an array $\mathcal{A} = (a(1), a(2), \ldots, a(2t))$ let $p_{\mathcal{A}}(x) := \prod_{i \in [t]} (x_{a(2i-1)} - x_{a(2i)})$.
- If elements in $\mathcal{A}$ are distinct, then $p_{\mathcal{A}}(x) \in Ker(W_t)$. Is there a basis for $Ker(W_t)$ that consists of such polynomials?

An explicit basis for $Ker(W_t)$.

- Example: The polynomial $p(x) = (x_1 - x_2).(x_3 - x_4).(x_5 - x_6)$ belongs to $Ker(W_3)$.
- Partial derivatives of $p(x)$ cancel in pairs: $\frac{\partial p}{\partial x_1} = -\frac{\partial p}{\partial x_2} = (x_3 - x_4).(x_5 - x_6)$.
- For an array $\mathcal{A} = (a(1), a(2), \ldots, a(2t))$ let $p_{\mathcal{A}}(x) := \prod_{i\in[t]}(x_{a(2i-1)} - x_{a(2i)})$.
- If elements in $\mathcal{A}$ are distinct, then $p_{\mathcal{A}}(x) \in Ker(W_t)$. Is there a basis for $Ker(W_t)$ that consists of such polynomials?
- The polynomials $p_{\mathcal{A}}(x)$ are linearly dependent, there are $\binom{n}{2t}$ arrays of distinct elements but $Ker(W_t)$ has dimension $\binom{n}{t} - \binom{n}{t-1}$.

An explicit basis for $Ker(W_t)$.

- A standard $(n-t,t)$ Young tableau $\mathcal{U}$ is an arrangement of $[n]$ in two rows of size $n-t$ and t, such that each row and column is sorted in ascending order.

An explicit basis for $Ker(W_t)$.

- A standard $(n-t, t)$ Young tableau $\mathcal{U}$ is an arrangement of $[n]$ in two rows of size $n-t$ and t, such that each row and column is sorted in ascending order.
- The straightening algorithm [CSST08]: The polynomials $p_{\mathcal{A}}(x)$ for where $(a(2i-i), a(2i))$ are entries of the i-th column of a standard Young tableau are linearly independent.

An explicit basis for $Ker(W_t)$.

- A standard $(n-t,t)$ Young tableau $\mathcal{U}$ is an arrangement of $[n]$ in two rows of size $n-t$ and t, such that each row and column is sorted in ascending order.
- The straightening algorithm [CSST08]: The polynomials $p_{\mathcal{A}}(x)$ for where $(a(2i-i), a(2i))$ are entries of the i-th column of a standard Young tableau are linearly independent.
- Hook length formula: The number of standard Young tableau is $\binom{n}{t} - \binom{n}{t-1}$.

An explicit basis for $Ker(W_t)$.

- A standard $(n-t,t)$ Young tableau $\mathcal{U}$ is an arrangement of $[n]$ in two rows of size $n-t$ and t, such that each row and column is sorted in ascending order.
- The straightening algorithm [CSST08]: The polynomials $p_{\mathcal{A}}(x)$ for where $(a(2i-i),a(2i))$ are entries of the i-th column of a standard Young tableau are linearly independent.
- Hook length formula: The number of standard Young tableau is $\binom{n}{t}-\binom{n}{t-1}$.
- We therefore have an explicit basis for $Ker(W_t)$ consisting of polynomials $p_{\mathcal{A}}(x)$, that come from standard Young tableau.

Polynomial decompositions

- Let L_t be the space of degree t polynomials, then $L_t = Im(W_t^t) \oplus Ker(W_t)$.

Polynomial decompositions

- Let L_t be the space of degree t polynomials, then $L_t = Im(W_t^t) \oplus Ker(W_t)$.
- Recall that $W_t^t q(x) = (|x| - t + 1)q(x)$, thus every polynomial $p(x) \in L_t$ can be written as $p_t(x) + (|x| - t + 1)q(x)$ where $q(x) \in L_{t-1}$.

Polynomial decompositions

- Let L_t be the space of degree t polynomials, then $L_t = Im(W_t^t) \oplus Ker(W_t)$.
- Recall that $W_t^t q(x) = (|x| - t + 1)q(x)$, thus every polynomial $p(x) \in L_t$ can be written as $p_t(x) + (|x| - t + 1)q(x)$ where $q(x) \in L_{t-1}$.
- By induction we have the decomposition:

$$p(x) = p_t(x) + \sum_{i=1}^{t} p_{t-i}(x) \prod_{j=1}^{i} (|x| - t + j)$$

where $p_i \in Ker(W_i)$.

Polynomial decompositions

- Let L_t be the space of degree t polynomials, then $L_t = Im(W_t^t) \oplus Ker(W_t)$.
- Recall that $W_t^t q(x) = (|x| - t + 1)q(x)$, thus every polynomial $p(x) \in L_t$ can be written as $p_t(x) + (|x| - t + 1)q(x)$ where $q(x) \in L_{t-1}$.
- By induction we have the decomposition:

$$p(x) = p_t(x) + \sum_{i=1}^{t} p_{t-i}(x) \prod_{j=1}^{i} (|x| - t + j)$$

  where $p_i \in Ker(W_i)$.
- Let M_t be the space of degree at most t polynomials, decompose the degree j component of M_t as above and and collect all terms that belong to $Ker(W_j)$.

Proof overview

Proof overview

- **Lemma**

  Polynomials $p(x) \in M_t$ *can be decomposed as* $p(x) = \sum_{j=0}^{t} q_j(x)$*, where* $q_j(x) = \sum_{0 \leq i \leq t-j} |x|^i p_{ij}(x)$ *and each* $p_{ij}(x) \in$ *Ker*(W_j).

Proof overview

- **Lemma**

  Polynomials $p(x) \in M_t$ *can be decomposed as* $p(x) = \sum_{j=0}^{t} q_j(x)$*, where* $q_j(x) = \sum_{0 \leq i \leq t-j} |x|^i p_{ij}(x)$ *and each* $p_{ij}(x) \in$ *Ker*(W_j)*.*

  - The proof of Blekherman's theorem uses above decomposition for $p(x)$ and two more lemmas.

Proof overview

- **Lemma**

  Polynomials $p(x) \in M_t$ can be decomposed as $p(x) = \sum_{j=0}^{t} q_j(x)$, where $q_j(x) = \sum_{0 \le i \le t-j} |x|^i p_{ij}(x)$ and each $p_{ij}(x) \in$ Ker(W_j).

  - The proof of Blekherman's theorem uses above decomposition for $p(x)$ and two more lemmas.
  - First, Sym$(gh) = 0$ if $g \in$ Ker$(W_j), h \in$ Ker(W'_j) such that $n/2 > j > j'$.

Proof overview

- **Lemma**

  Polynomials $p(x) \in M_t$ can be decomposed as $p(x) = \sum_{j=0}^{t} q_j(x)$, where $q_j(x) = \sum_{0 \leq i \leq t-j} |x|^i p_{ij}(x)$ and each $p_{ij}(x) \in$ Ker(W_j).

  - The proof of Blekherman's theorem uses above decomposition for $p(x)$ and two more lemmas.
  - First, Sym$(gh) = 0$ if $g \in$ Ker$(W_j), h \in$ Ker(W'_j) such that $n/2 > j > j'$.
  - Second, we need to evaluate Sym(gh) when $g, h \in$ Ker(W_j) belong to the same kernel.

Proof overview

- **Lemma**

  Polynomials $p(x) \in M_t$ can be decomposed as $p(x) = \sum_{j=0}^{t} q_j(x)$, where $q_j(x) = \sum_{0 \le i \le t-j} |x|^i p_{ij}(x)$ and each $p_{ij}(x) \in$ Ker(W_j).

  - The proof of Blekherman's theorem uses above decomposition for $p(x)$ and two more lemmas.
  - First, Sym$(gh) = 0$ if $g \in$ Ker$(W_j), h \in$ Ker(W_j') such that $n/2 > j > j'$.
  - Second, we need to evaluate Sym(gh) when $g, h \in$ Ker(W_j) belong to the same kernel.
  - We use explicit bases for Ker(W_t) constructed earlier to prove these lemmas.

Different kernels

- Lemma: $\mathsf{Sym}(gh) = 0$ if $g \in \mathsf{Ker}(W_j), h \in \mathsf{Ker}(W'_j)$ for $n/2 > j > j'$.

Different kernels

- Lemma: $\mathsf{Sym}(gh) = 0$ if $g \in \mathsf{Ker}(W_j), h \in \mathsf{Ker}(W_j')$ for $n/2 > j > j'$.
- It suffices to prove for $x \in \{0,1\}^n$ and when g, h are basis vectors $p_{\mathcal{U}}(x), p_{\mathcal{V}}(x)$.

Different kernels

- Lemma: $\mathsf{Sym}(gh) = 0$ if $g \in \mathsf{Ker}(W_j), h \in \mathsf{Ker}(W'_j)$ for $n/2 > j > j'$.
- It suffices to prove for $x \in \{0,1\}^n$ and when g, h are basis vectors $p_{\mathcal{U}}(x), p_{\mathcal{V}}(x)$.
- Example: $g(x) = (x_1 - x_2)(x_3 - x_4)(x_5 - x_6)$ and $h(x) = (x_1 - x_2)(x_3 - x_5)$.

Different kernels

- Lemma: Sym$(gh) = 0$ if $g \in$ Ker$(W_j), h \in$ Ker(W'_j) for $n/2 > j > j'$.
- It suffices to prove for $x \in \{0,1\}^n$ and when g, h are basis vectors $p_{\mathcal{U}}(x), p_{\mathcal{V}}(x)$.
- Example: $g(x) = (x_1 - x_2)(x_3 - x_4)(x_5 - x_6)$ and $h(x) = (x_1 - x_2)(x_3 - x_5)$.
- g, h correspond to matchings of size $j, j' = 3, 2$ respectively. The union of these matchings has an odd length path.

Different kernels

- Lemma: $\mathrm{Sym}(gh) = 0$ if $g \in \mathrm{Ker}(W_j), h \in \mathrm{Ker}(W'_j)$ for $n/2 > j > j'$.
- It suffices to prove for $x \in \{0,1\}^n$ and when g, h are basis vectors $p_{\mathcal{U}}(x), p_{\mathcal{V}}(x)$.
- Example: $g(x) = (x_1 - x_2)(x_3 - x_4)(x_5 - x_6)$ and $h(x) = (x_1 - x_2)(x_3 - x_5)$.
- g, h correspond to matchings of size $j, j' = 3, 2$ respectively. The union of these matchings has an odd length path.
- The path for this example is 4356, thus $g(x)h(x) = (x_4 - x_3)(x_3 - x_5)(x_5 - x_6)t(x)$ where $t(x)$ does not depend on variables in the path.

Different kernels

- Let $\sigma(4356) = abcd$ define $\overline{\sigma}(4356) = badc$ and $\overline{\sigma}(l) = \sigma(l)$ for all other l. This defines an involution on S_n.

Different kernels

- Let $\sigma(4356) = abcd$ define $\overline{\sigma}(4356) = badc$ and $\overline{\sigma}(l) = \sigma(l)$ for all other l. This defines an involution on S_n.
- As $x \in \{0,1\}^n$, the path polynomial $(x_a - x_b)(x_b - x_c)(x_c - x_d)$ is non zero if and only if $x_{abcd} = (0,1,0,1)$ or $x_{abcd} = (1,0,1,0)$.

Different kernels

- Let $\sigma(4356) = abcd$ define $\overline{\sigma}(4356) = badc$ and $\overline{\sigma}(l) = \sigma(l)$ for all other l. This defines an involution on S_n.
- As $x \in \{0,1\}^n$, the path polynomial $(x_a - x_b)(x_b - x_c)(x_c - x_d)$ is non zero if and only if $x_{abcd} = (0,1,0,1)$ or $x_{abcd} = (1,0,1,0)$.
- The involution flips between the two cases above, thus $\sigma(g(x)h(x)) + \overline{\sigma}(g(x)h(x)) = 0$.

Different kernels

- Let $\sigma(4356) = abcd$ define $\overline{\sigma}(4356) = badc$ and $\overline{\sigma}(l) = \sigma(l)$ for all other l. This defines an involution on S_n.
- As $x \in \{0,1\}^n$, the path polynomial $(x_a - x_b)(x_b - x_c)(x_c - x_d)$ is non zero if and only if $x_{abcd} = (0,1,0,1)$ or $x_{abcd} = (1,0,1,0)$.
- The involution flips between the two cases above, thus $\sigma(g(x)h(x)) + \overline{\sigma}(g(x)h(x)) = 0$.
- Sym$(gh)(x) = 0$ is an average over all permutations and is therefore 0 for $x \in \{0,1\}^n$.

Same Kernels

- Define the following inner product for degree t polynomials:

$$\langle g|h\rangle := \sum_{S\subseteq[n],|S|=t} g_S h_S \ .$$

Same Kernels

- Define the following inner product for degree t polynomials:

$$\langle g|h\rangle := \sum_{S\subseteq[n],|S|=t} g_S h_S \ .$$

- $\text{Sym}^{uni}(gh)$ for $g,h \in \text{Ker}(W_t)$ is a polynomial of degree at most $2t$.

Same Kernels

- Define the following inner product for degree t polynomials:

$$\langle g|h\rangle := \sum_{S\subseteq[n],|S|=t} g_S h_S \ .$$

- $\text{Sym}^{uni}(gh)$ for $g, h \in \text{Ker}(W_t)$ is a polynomial of degree at most $2t$.
- The basis polynomial $p_{\mathcal{U}}(x) = (x_{u(1)} - x_{u(2)}). \cdots .(x_{u(2t-1)} - x_{u(2t)}) = 0$ if $x \in \{0,1\}^n$ has less than t zeros or less than t ones.

Same Kernels

- Define the following inner product for degree t polynomials:

$$\langle g|h\rangle := \sum_{S\subseteq[n],|S|=t} g_S h_S \ .$$

- $\text{Sym}^{uni}(gh)$ for $g, h \in \text{Ker}(W_t)$ is a polynomial of degree at most $2t$.
- The basis polynomial $p_{\mathcal{U}}(x) = (x_{u(1)} - x_{u(2)}).\cdots.(x_{u(2t-1)} - x_{u(2t)}) = 0$ if $x \in \{0,1\}^n$ has less than t zeros or less than t ones.
- The polynomial $\text{Sym}^{uni}(gh)$ has roots at $|x| = \{0, 1, \cdots, t-1\} \cup \{n, n-1, \cdots, n-t+1\}$.

Same Kernels

- Define the following inner product for degree t polynomials:

$$\langle g|h\rangle := \sum_{S\subseteq[n],|S|=t} g_S h_S \enspace .$$

- $\mathrm{Sym}^{uni}(gh)$ for $g, h \in \mathrm{Ker}(W_t)$ is a polynomial of degree at most $2t$.
- The basis polynomial $p_{\mathcal{U}}(x) = (x_{u(1)} - x_{u(2)}). \cdots .(x_{u(2t-1)} - x_{u(2t)}) = 0$ if $x \in \{0,1\}^n$ has less than t zeros or less than t ones.
- The polynomial $\mathrm{Sym}^{uni}(gh)$ has roots at $|x| = \{0, 1, \cdots, t-1\} \cup \{n, n-1, \cdots, n-t+1\}$.
- $\mathrm{Sym}(gh)(x) = \lambda \prod_{0\leq i<t}(|x|-i)(n-|x|-i)$, how to evaluate the constant λ?

Same Kernels

- As g, h are homogeneous degree t polynomials, for all $x \in \{0,1\}^n, |x| = t$ there is a unique coefficient S such that $g(x) = g_S, h(x) = h_S$.

Same Kernels

- As g, h are homogeneous degree t polynomials, for all $x \in \{0,1\}^n, |x| = t$ there is a unique coefficient S such that $g(x) = g_S, h(x) = h_S$.
- There are $t!(n-t)!$ different permutations $\sigma \in S_n$ such that $g(\sigma x) = g_S$, that is:

$$\mathsf{Sym}(gh)(x) = \frac{t!(n-t)!}{n!} \sum_{|S|=t} g_S h_S \ .$$

Same Kernels

- As g, h are homogeneous degree t polynomials, for all $x \in \{0,1\}^n, |x| = t$ there is a unique coefficient S such that $g(x) = g_S, h(x) = h_S$.
- There are $t!(n-t)!$ different permutations $\sigma \in S_n$ such that $g(\sigma x) = g_S$, that is:

$$\mathsf{Sym}(gh)(x) = \frac{t!(n-t)!}{n!} \sum_{|S|=t} g_S h_S \ .$$

- Solving for λ we obtain:

$$\mathsf{Sym}(gh)(x) = \langle g|h \rangle \frac{(n-2t)!}{n!} \prod_{0 \leq i < t} (|x| - i)(n - |x| - i) \ .$$

Completing the proof

- Recall that $p(x) = \sum_{j=0}^{t} q_j(x)$ where $q_j(x) = \sum_{0 \leq k \leq t-j} |x|^k p_{kj}(x)$ such that each $p_{kj} \in Ker(W_j)$.

Completing the proof

- Recall that $p(x) = \sum_{j=0}^{t} q_j(x)$ where $q_j(x) = \sum_{0 \le k \le t-j} |x|^k p_{kj}(x)$ such that each $p_{kj} \in Ker(W_j)$.
- As the symmetrization of the product of polynomials in different kernels vanishes, Sym$(p^2) = \sum_{j=0}^{t}$ Sym $\left(q_j^2\right)$.

Completing the proof

- Recall that $p(x) = \sum_{j=0}^{t} q_j(x)$ where $q_j(x) = \sum_{0 \leq k \leq t-j} |x|^k p_{kj}(x)$ such that each $p_{kj} \in Ker(W_j)$.
- As the symmetrization of the product of polynomials in different kernels vanishes, $\text{Sym}(p^2) = \sum_{j=0}^{t} \text{Sym}\left(q_j^2\right)$.
- Using previous lemma, $Sym(q_j^2) = \sum_{0 \leq k,l \leq t-j} \text{Sym}(|x|^{k+l} p_{kj} p_{lj})$ evaluates to,

$$c \prod_{0 \leq i < j} (|x| - i)(n - |x| - i) \sum_{0 \leq k,l \leq t-j} \langle p_{kj} | p_{lj} \rangle |x|^{k+l}$$

$$= c \left(\prod_{0 \leq i < j} (|x| - i)(n - |x| - i) \right) \mathbf{x}^T P \mathbf{x}$$

Concluding remarks

- Lower bounds on the sum of squares degree of functions $f(x) = (x-k)(x-k+1)$ can be proved using Blekherman's theorem.

Concluding remarks

- Lower bounds on the sum of squares degree of functions $f(x) = (x-k)(x-k+1)$ can be proved using Blekherman's theorem.
- Can Blekherman's theorem be used to simplify sum of squares lower bounds for planted clique?

Concluding remarks

- Lower bounds on the sum of squares degree of functions $f(x) = (x - k)(x - k + 1)$ can be proved using Blekherman's theorem.
- Can Blekherman's theorem be used to simplify sum of squares lower bounds for planted clique?
- Can a representation theoretic approach help prove further sum of squares lower bounds?