# Symmetric Sums of Squares 

Annie Raymond<br>University of Massachusetts

Joint with James Saunderson (Monash University),<br>Mohit Singh (Georgia Tech), and Rekha Thomas (UW)

April 16, 2018

## Goal

Certify the nonnegativity of a symmetric polynomial over the hypercube.
Our key result: the runtime does not depend on the number of variables of the polynomial

1. Background
2. Our setting
3. Results
4. Flag algebras
5. Future work

## Nonnegative polynomials and sums of squares

A polynomial $p \in \mathbb{R}\left[x_{1}, \ldots, x_{n}\right]=: \mathbb{R}[\mathbf{x}]$ is nonnegative if $p\left(x_{1}, \ldots, x_{n}\right) \geq 0$ for all $\left(x_{1}, \ldots, x_{n}\right) \in \mathbb{R}^{n}$

$p$ sum of squares (sos), i.e., $p=\sum_{i=1}^{l} f_{i}^{2}$ where $f_{i} \in \mathbb{R}[\mathbf{x}] \Rightarrow p \geq 0$

Hilbert (1888): Not all nonnegative polynomials are sos.

Motzkin (1967, with Taussky-Todd): $M(x, y)=x^{4} y^{2}+x^{2} y^{4}+1-3 x^{2} y^{2}$ is a nonnegative polynomial but is not a sos.


## Finding sos certificates

- $p \in \mathbb{R}[\mathbf{x}]:=\mathbb{R}\left[x_{1}, \ldots, x_{n}\right]$ such that $\operatorname{deg}(p)=2 d$
- $[x]_{d}:=\left(1, x_{1}, \ldots, x_{n}, x_{1}^{2}, x_{1} x_{2}, \ldots, x_{n}^{d}\right)^{\top}$
$=$ vector of monomials in $\mathbb{R}[\mathbf{x}]$ of degree $\leq d$
- $p$ sos $\Leftrightarrow \exists Q \succeq 0$ such that $p=[x]_{d}^{\top} Q[x]_{d}$


## Finding sos certificates

- $p \in \mathbb{R}[\mathbf{x}]:=\mathbb{R}\left[x_{1}, \ldots, x_{n}\right]$ such that $\operatorname{deg}(p)=2 d$
- $[x]_{d}:=\left(1, x_{1}, \ldots, x_{n}, x_{1}^{2}, x_{1} x_{2}, \ldots, x_{n}^{d}\right)^{\top}$
$=$ vector of monomials in $\mathbb{R}[\mathbf{x}]$ of degree $\leq d$
- $p$ sos $\Leftrightarrow \exists Q \succeq 0$ such that $p=[x]_{d}^{\top} Q[x]_{d}$

$$
=[x]_{d}^{\top} B B^{\top}[x]_{d}=\left([x]_{d}^{\top} B\right)\left([x]_{d}^{\top} B\right)^{\top}
$$

## Finding sos certificates

- $p \in \mathbb{R}[\mathbf{x}]:=\mathbb{R}\left[x_{1}, \ldots, x_{n}\right]$ such that $\operatorname{deg}(p)=2 d$
- $[x]_{d}:=\left(1, x_{1}, \ldots, x_{n}, x_{1}^{2}, x_{1} x_{2}, \ldots, x_{n}^{d}\right)^{\top}$
$=$ vector of monomials in $\mathbb{R}[\mathbf{x}]$ of degree $\leq d$
- $p$ sos $\Leftrightarrow \exists Q \succeq 0$ such that $p=[x]_{d}^{\top} Q[x]_{d}$

$$
=[x]_{d}^{\top} B B^{\top}[x]_{d}=\left([x]_{d}^{\top} B\right)\left([x]_{d}^{\top} B\right)^{\top}
$$

## Example

$$
\begin{aligned}
p=x_{1}^{2}-x_{1} x_{2}+x_{2}^{2}+1 & =\left(\begin{array}{lll}
1 & x_{1} & x_{2}
\end{array}\right)\left(\begin{array}{ccc}
1 & 0 & 0 \\
0 & 1 & -\frac{1}{2} \\
0 & -\frac{1}{2} & 1
\end{array}\right)\left(\begin{array}{l}
1 \\
x_{1} \\
x_{2}
\end{array}\right) \\
& =\left(\begin{array}{lll}
1 & x_{1} & x_{2}
\end{array}\right)\left(\begin{array}{ccc}
1 & 0 & 0 \\
0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \\
0 & -\frac{\sqrt{3}}{2} & \frac{1}{2}
\end{array}\right)\left(\begin{array}{ccc}
1 & 0 & 0 \\
0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} \\
0 & \frac{1}{2} & \frac{1}{2}
\end{array}\right)\left(\begin{array}{l}
1 \\
x_{1} \\
x_{2}
\end{array}\right) \\
& =1+\frac{3}{4}\left(x_{1}-x_{2}\right)^{2}+\frac{1}{4}\left(x_{1}+x_{2}\right)^{2}
\end{aligned}
$$

## Sums of squares modulo an ideal

## Goal

Certify $p \geq 0$ over the solutions of a system of polynomial equations.

## Sums of squares modulo an ideal

## Goal

Certify $p \geq 0$ over the solutions of a system of polynomial equations.

## Example

Show that $1-y \geq 0$ whenever $x^{2}+y^{2}=1$

$$
\begin{aligned}
1-y & =\left(\frac{x}{\sqrt{2}}\right)^{2}+\left(\frac{y-1}{\sqrt{2}}\right)^{2}-\frac{1}{2}\left(x^{2}+y^{2}-1\right) \\
& =\frac{1}{2}\left(\begin{array}{lll}
1 & x & y
\end{array}\right)\left(\begin{array}{ccc}
1 & 0 & -1 \\
0 & 1 & 0 \\
-1 & 0 & 1
\end{array}\right)\left(\begin{array}{l}
1 \\
x \\
y
\end{array}\right)-\frac{1}{2}\left(x^{2}+y^{2}-1\right)
\end{aligned}
$$

## Sums of squares modulo an ideal

## Goal

Certify $p \geq 0$ over the solutions of a system of polynomial equations.

## Example

Show that $1-y \geq 0$ whenever $x^{2}+y^{2}=1$

$$
\begin{aligned}
1-y & =\left(\frac{x}{\sqrt{2}}\right)^{2}+\left(\frac{y-1}{\sqrt{2}}\right)^{2}-\frac{1}{2}\left(x^{2}+y^{2}-1\right) \\
& =\frac{1}{2}\left(\begin{array}{lll}
1 & x & y
\end{array}\right)\left(\begin{array}{ccc}
1 & 0 & -1 \\
0 & 1 & 0 \\
-1 & 0 & 1
\end{array}\right)\left(\begin{array}{l}
1 \\
x \\
y
\end{array}\right)-\frac{1}{2}\left(x^{2}+y^{2}-1\right)
\end{aligned}
$$

- Ideal $\mathcal{I} \subseteq \mathbb{R}[\mathbf{x}]$
- $V_{\mathbb{R}}(\mathcal{I})=$ its real variety
- $p$ is sos modulo $\mathcal{I}$ if $p \equiv \sum_{i=1}^{l} f_{i}^{2} \bmod \mathcal{I}$
(i.e., if $\exists h \in \mathcal{I}$ such that $p=\sum_{i=1}^{\prime} f_{i}^{2}+h$ )
- $p$ is $d$-sos $\bmod \mathcal{I}$ if $p \equiv \sum_{i=1}^{l} f_{i}^{2} \bmod \mathcal{I}$ where $\operatorname{deg}\left(f_{i}\right) \leq d \forall i$


## Sums of squares modulo an ideal

## Goal

Certify $p \geq 0$ over the solutions of a system of polynomial equations.

## Example

Show that $1-y \geq 0$ whenever $x^{2}+y^{2}=1$

$$
\begin{aligned}
1-y & =\left(\frac{x}{\sqrt{2}}\right)^{2}+\left(\frac{y-1}{\sqrt{2}}\right)^{2}-\frac{1}{2}\left(x^{2}+y^{2}-1\right) \\
& =\frac{1}{2}\left(\begin{array}{lll}
1 & x & y
\end{array}\right)\left(\begin{array}{ccc}
1 & 0 & -1 \\
0 & 1 & 0 \\
-1 & 0 & 1
\end{array}\right)\left(\begin{array}{l}
1 \\
x \\
y
\end{array}\right)-\frac{1}{2}\left(x^{2}+y^{2}-1\right)
\end{aligned}
$$

- Ideal $\mathcal{I} \subseteq \mathbb{R}[\mathbf{x}]$
- $V_{\mathbb{R}}(\mathcal{I})=$ its real variety
- $p$ is sos modulo $\mathcal{I}$ if $p \equiv \sum_{i=1}^{l} f_{i}^{2} \bmod \mathcal{I}$
(i.e., if $\exists h \in \mathcal{I}$ such that $p=\sum_{i=1}^{\prime} f_{i}^{2}+h$ )
- $p$ is $d$-sos $\bmod \mathcal{I}$ if $p \equiv \sum_{i=1}^{l} f_{i}^{2} \bmod \mathcal{I}$ where $\operatorname{deg}\left(f_{i}\right) \leq d \forall i \Leftrightarrow \exists Q \succeq 0$ such that $p \equiv v^{\top} Q v \bmod \mathcal{I}$ (semidefinite programming can find $Q$ in $n^{O(d)}$-time)


## Our problem

Let $\mathcal{V}_{n, k}=\{0,1\}\binom{n}{k}$ be the $k$-subset discrete hypercube $\rightarrow$ coordinates indexed by $k$-element subsets of [ $n$ ]

## Goal

Minimize a symmetric* polynomial over $\mathcal{V}_{n, k}$
$*$ symmetric $=\mathfrak{S}_{n}$-invariant
$\mathfrak{s} \cdot x_{i_{1} i_{2} \ldots i_{k}}=x_{\mathfrak{s}\left(i_{1}\right) \mathfrak{s}\left(i_{2}\right) \ldots s\left(i_{k}\right)}^{\forall \mathfrak{s} \in \mathfrak{S}_{n}}$

## Our problem

Let $\mathcal{V}_{n, k}=\{0,1\}\binom{n}{k}$ be the $k$-subset discrete hypercube $\rightarrow$ coordinates indexed by $k$-element subsets of [ $n$ ]

## Goal

Minimize a symmetric* polynomial over $\mathcal{V}_{n, k}$
${ }^{*}$ symmetric $=\mathfrak{S}_{n}$-invariant
$\mathfrak{s} \cdot x_{i_{1} i_{2} \ldots i_{k}}=x_{\mathfrak{s}\left(i_{1}\right) \mathfrak{s}\left(i_{2}\right) \ldots s\left(i_{k}\right)} \forall \mathfrak{s} \in \mathfrak{S}_{n}$

How?
By finding sos certificates over $\mathcal{V}_{n, k}$ that exploit symmetry, i.e., that we can find in a runtime independent of $n$.
$k=1$ : see Blekherman, Gouveia, Pfeiffer (2014) $k \geq 2$ : ?

## Examples of such problems

- Turán-type problem

Given a fixed graph $H$, determine the limiting edge density of a $H$-free graph on $n$ vertices as $n \rightarrow \infty$

## Examples of such problems

- Turán-type problem

Given a fixed graph $H$, determine the limiting edge density of a $H$-free graph on $n$ vertices as $n \rightarrow \infty$

- Ramsey-type problem

Color the edges of $K_{n}$ ruby or sapphire. Find the smallest $n$ for which you are guaranteed a ruby clique of size $r$ or a sapphire clique of size $s$


## Examples of such problems

- Turán-type problem

Given a fixed graph $H$, determine the limiting edge density of a $H$-free graph on $n$ vertices as $n \rightarrow \infty$

- Ramsey-type problem

Color the edges of $K_{n}$ ruby or sapphire. Find the smallest $n$ for which you are guaranteed a ruby clique of size $r$ or a sapphire clique of size $s$


Focus on $\mathcal{V}_{n}:=\mathcal{V}_{n, 2}=\{0,1\}^{\binom{n}{2}}$
$\rightarrow$ coordinates are indexed by pairs $i j, 1 \leq i<j \leq n$

## Passing to optimization - Turán-type problem

## Example

Forbidding triangles in a graph on $n$ vertices, find

$$
\begin{array}{|cc|}
\hline \max \frac{1}{\binom{n}{2}} \sum_{1 \leq i<j \leq n} x_{i j} & \\
\text { s.t. } x_{i j}^{2}=x_{i j} & \forall 1 \leq i<j \leq n \\
\quad x_{i j} x_{j k} x_{i k}=0 & \forall 1 \leq i<j<k \leq n \\
\hline
\end{array}
$$

In particular, show that this is at most $\frac{1}{2}+O\left(\frac{1}{n}\right)$
$\rightarrow$ show that $\frac{1}{2}+O\left(\frac{1}{n}\right)-\frac{1}{\binom{n}{2}} \sum_{1 \leq i<j \leq n} x_{i j} \geq 0$

## Issue with passing to optimization - Turán-type problem

Example (continued)
Find $Q \succeq 0$ and $d \in \mathbb{Z}^{+}$such that

$$
\frac{1}{2}+O\left(\frac{1}{n}\right)-\frac{1}{\binom{n}{2}} \sum_{1 \leq i<j \leq n} x_{i j} \equiv v^{\top} Q v \quad \bmod \mathcal{I}
$$

where

$$
\begin{aligned}
& \mathcal{I}=\left\langle x_{i j}^{2}-x_{i j} \forall 1 \leq i<j \leq n,\right. \\
& \left.x_{i j} x_{j k} x_{i k} \forall 1 \leq i<j<k \leq n\right\rangle
\end{aligned}
$$

## Issue with passing to optimization - Turán-type problem

Example (continued)
Find $Q \succeq 0$ and $d \in \mathbb{Z}^{+}$such that

$$
\frac{1}{2}+O\left(\frac{1}{n}\right)-\frac{1}{\binom{n}{2}} \sum_{1 \leq i<j \leq n} x_{i j} \equiv v^{\top} Q v \quad \bmod \mathcal{I}
$$

where

$$
\begin{aligned}
\mathcal{I}= & \left\langle x_{i j}^{2}-x_{i j} \forall 1 \leq i<j \leq n,\right. \\
& \left.x_{i j} x_{j k} x_{i k} \forall 1 \leq i<j<k \leq n\right\rangle
\end{aligned}
$$

Can we do this with semidefinite programming?
The runtime would be $\binom{n}{2} O(d)$

## Issue with passing to optimization - Turán-type problem

Example (continued)
Find $Q \succeq 0$ and $d \in \mathbb{Z}^{+}$such that

$$
\frac{1}{2}+O\left(\frac{1}{n}\right)-\frac{1}{\binom{n}{2}} \sum_{1 \leq i<j \leq n} x_{i j} \equiv v^{\top} Q v \quad \bmod \mathcal{I}
$$

where

$$
\begin{aligned}
& \mathcal{I}=\left\langle x_{i j}^{2}-x_{i j} \forall 1 \leq i<j \leq n,\right. \\
& \left.x_{i j} x_{j k} x_{i k} \forall 1 \leq i<j<k \leq n\right\rangle
\end{aligned}
$$

Can we do this with semidefinite programming?
The runtime would be $\binom{n}{2}^{O(d)} \rightarrow \infty$ as $n \rightarrow \infty$.

## Foreshadowing

## Example

The following is a sos proof of Mantel's theorem

$$
\left(\begin{array}{ll}
1 & q_{1}
\end{array}\right)\left(\begin{array}{cc}
\frac{(n-1)^{2}}{2} & -\frac{2(n-1)}{n} \\
-\frac{2(n-1)}{n} & \frac{8}{n^{2}}
\end{array}\right)\binom{1}{q_{1}}+\operatorname{sym}\left(\left(q_{2}\right)\left(\frac{8}{n^{2}}\right)\left(q_{2}\right)\right)
$$

where $q_{1}=\sum_{i<j} x_{i j}$ and $q_{2}=\sum_{i<j} x_{i j}-\frac{n-2}{2} \sum_{i=1}^{n-1} x_{i n}$

Key features of desired sos certificates:

- exploits symmetry
- constant size
- entries are functions of $n$


## Representation theory needed for exploiting symmetry

- $(\mathbb{R}[x] / \mathcal{I})_{d}=: V=\bigoplus_{\lambda \vdash n} V_{\lambda}$ isotypic decomposition
- partition $\lambda=(5,3,3,1)$ for $n=12$


## Representation theory needed for exploiting symmetry

- $(\mathbb{R}[x] / \mathcal{I})_{d}=: V=\bigoplus_{\lambda \vdash n} V_{\lambda}$ isotypic decomposition
- partition $\lambda=(5,3,3,1)$ for $n=12$
- $V_{\lambda}=\bigoplus W_{\tau_{\lambda}}$
- shape of $\lambda:$|  |  |  |  |  |
| :--- | :--- | :--- | :--- | :--- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
- $\mathfrak{R}_{\tau_{\lambda}}:=$ row group of $\tau_{\lambda}$ (fixes the rows of $\tau_{\lambda}$ )
- $W_{\tau_{\lambda}}:=\left(V_{\lambda}\right)^{\mathfrak{R}_{\tau_{\lambda}}}=$ subspace of $V_{\lambda}$ fixed by $\mathfrak{R}_{\tau_{\lambda}}$
- $n_{\lambda}$ :=number of standard tableaux of shape $\lambda$
- $m_{\lambda}:=$ dimension of $W_{\tau_{\lambda}}$


## Representation theory needed for exploiting symmetry

- $(\mathbb{R}[x] / \mathcal{I})_{d}=: V=\bigoplus_{\lambda \vdash n} V_{\lambda}$ isotypic decomposition
- partition $\lambda=(5,3,3,1)$ for $n=12$
- $V_{\lambda}=\bigoplus W_{\tau_{\lambda}}$
- shape of $\lambda$ :

standard tableau $\tau_{\lambda}$ :

| 1 | 4 | 5 | 6 | 9 |
| :---: | :---: | :---: | :---: | :---: |
| 2 | 7 | 10 |  |  |
| 3 | 8 | 12 |  |  |
| 11 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

- $\mathfrak{R}_{\tau_{\lambda}}:=$ row group of $\tau_{\lambda}$ (fixes the rows of $\tau_{\lambda}$ )
- $W_{\tau_{\lambda}}:=\left(V_{\lambda}\right)^{\Re_{\tau_{\lambda}}}=$ subspace of $V_{\lambda}$ fixed by $\Re_{\tau_{\lambda}}$
- $n_{\lambda}:=$ number of standard tableaux of shape $\lambda$
- $m_{\lambda}:=$ dimension of $W_{\tau_{\lambda}}$

$$
V=\bigoplus_{\lambda \vdash n} \bigoplus_{\tau_{\lambda}} W_{\tau_{\lambda}}
$$

Note: $\operatorname{dim}(V)=\sum_{\lambda \vdash n} m_{\lambda} n_{\lambda}$

## Gatermann-Parrilo symmetry-reduction technique

Recall: $p d$-sos $\bmod \mathcal{I} \Leftrightarrow \exists Q \succeq 0$ s.t. $p \equiv v^{\top} Q v \bmod \mathcal{I}$
where $v=$ vector of basis elements of $(\mathbb{R}[x] / \mathcal{I})_{d}$

## Theorem (Gatermann-Parrilo, 2004)

For each $\lambda$, fix $\tau_{\lambda}$ and find a symmetry-adapted basis $\left\{b_{1}^{\tau_{\lambda}}, \ldots, b_{m_{\lambda}}^{\tau_{\lambda}}\right\}$ for $W_{\tau_{\lambda}}$.

If $p$ is symmetric and $d$-sos $\bmod \mathcal{I}$, then

$$
p \equiv \sum_{\lambda \vdash n} \operatorname{sym}\left(b^{\top} Q_{\lambda} b\right) \quad \bmod \mathcal{I},
$$


where $b=\left(b_{1}^{\tau_{\lambda}}, \ldots, b_{m_{\lambda}}^{\tau_{\lambda}}\right)^{\top}$ and $Q_{\lambda} \succeq 0$ has size $m_{\lambda} \times m_{\lambda}$.

Gain: size of SDP is $\sum_{\lambda \vdash n} m_{\lambda}$ instead of $\sum_{\lambda \vdash n} m_{\lambda} n_{\lambda}$

## Gatermann-Parrilo symmetry-reduction technique

Recall: $p d$-sos $\bmod \mathcal{I} \Leftrightarrow \exists Q \succeq 0$ s.t. $p \equiv v^{\top} Q v \bmod \mathcal{I}$ where $v=$ vector of basis elements of $(\mathbb{R}[x] / \mathcal{I})_{d}$

## Theorem (Gatermann-Parrilo, 2004)

For each $\lambda$, fix $\tau_{\lambda}$ and find a symmetry-adapted basis $\left\{b_{1}^{\tau_{\lambda}}, \ldots, b_{m_{\lambda}}^{\tau_{\lambda}}\right\}$ for $W_{\tau_{\lambda}}$.

If $p$ is symmetric and $d$-sos, then

$$
p=\sum_{\lambda \vdash n} \operatorname{sym}\left(b^{\top} Q_{\lambda} b\right),
$$


where $b=\left(b_{1}^{\tau_{\lambda}}, \ldots, b_{m_{\lambda}}^{\tau_{\lambda}}\right)^{\top}$ and $Q_{\lambda} \succeq 0$ has size $m_{\lambda} \times m_{\lambda}$.

Gain: size of SDP is $\sum_{\lambda \vdash n} m_{\lambda}$ instead of $\sum_{\lambda \vdash n} m_{\lambda} n_{\lambda}$
$\rightarrow$ how much smaller is the size of this SDP?

## Gatermann-Parrilo symmetry-reduction technique

Recall: $p d$-sos $\bmod \mathcal{I} \Leftrightarrow \exists Q \succeq 0$ s.t. $p \equiv v^{\top} Q v \bmod \mathcal{I}$ where $v=$ vector of basis elements of $(\mathbb{R}[x] / \mathcal{I})_{d}$

## Theorem (Gatermann-Parrilo, 2004)

For each $\lambda$, fix $\tau_{\lambda}$ and find a symmetry-adapted basis $\left\{b_{1}^{\tau_{\lambda}}, \ldots, b_{m_{\lambda}}^{\tau_{\lambda}}\right\}$ for $W_{\tau_{\lambda}} \cdot \rightarrow$ complexity of the algorithm depends on $n$ If $p$ is symmetric and $d$-sos, then

$$
p=\sum_{\lambda \vdash n} \operatorname{sym}\left(b^{\top} Q_{\lambda} b\right),
$$


where $b=\left(b_{1}^{\tau_{\lambda}}, \ldots, b_{m_{\lambda}}^{\tau_{\lambda}}\right)^{\top}$ and $Q_{\lambda} \succeq 0$ has size $m_{\lambda} \times m_{\lambda}$.

Gain: size of SDP is $\sum_{\lambda \vdash n} m_{\lambda}$ instead of $\sum_{\lambda \vdash n} m_{\lambda} n_{\lambda}$
$\rightarrow$ how much smaller is the size of this SDP?

## Succinct SOS

## Theorem (RSST, 2016)

If $p$ is symmetric and $d$-sos, then it has a symmetry-reduced sos certificate that can be obtained by solving a SDP of size independent of $n$ by keeping only a few partitions in Gatermann-Parrilo.

## Succinct SOS

## Theorem (RSST, 2016)

If $p$ is symmetric and $d$-sos, then it has a symmetry-reduced sos certificate that can be obtained by solving a SDP of size independent of $n$ by keeping only a few partitions in Gatermann-Parrilo.

## Example

In the sos proof of Mantel's theorem

$$
\left(\begin{array}{ll}
1 & q_{1}
\end{array}\right)\left(\begin{array}{cc}
\frac{(n-1)^{2}}{2} & -\frac{2(n-1)}{2^{n}} \\
-\frac{2(n-1)}{n} & \frac{8}{n^{2}}
\end{array}\right)\binom{1}{q_{1}}+\operatorname{sym}\left(\left(q_{2}\right)\left(\frac{8}{n^{2}}\right)\left(q_{2}\right)\right)
$$

$\rightarrow$ kept partitions $(n)=\overbrace{\square \square \mid \square \square}^{n}$ and $(n-1,1)=\overbrace{\square \square \mid \square}^{n-1}$

## Bypassing symmetry-adapted basis

Theorem (RSST, 2016)
In Gatermann-Parrilo, instead of a symmetry-adapted basis, one can use

- a spanning set for $W_{\tau_{\lambda}}$ for $\lambda \geq \operatorname{lex} \overbrace{\square}^{\overbrace{\square}| | l \mid}$.
- of size independent of $n$
- that is easy to generate


## Bypassing symmetry-adapted basis

## Theorem (RSST, 2016)

In Gatermann-Parrilo, instead of a symmetry-adapted basis, one can use

- a spanning set for $W_{\tau_{\lambda}}$ for $\lambda \geq \operatorname{lex} \overbrace{\square}^{\overbrace{\square}| | l \mid}$.
- of size independent of $n$
- that is easy to generate


## Examples of spanning sets containing $W_{\tau_{\lambda}}$

- $\operatorname{sym}_{\tau_{\lambda}}\left(x^{m}\right):=\frac{1}{\left|\Re_{\tau_{\lambda}}\right|} \sum_{\mathfrak{s} \in \Re_{\tau_{\lambda}}} \mathfrak{s} \cdot x^{m}$
- an appropriate Möbius transformation


## Razborov's flag algebras for Turán-type problems

Use flags (=partially labelled graphs) to certify a symmetric inequality that gives a good upper bound for Turán-type problems

## Key features:

- sums of squares of graph densities
- $n$ disappears
- asymptotic results for dense graphs


Theorem (Razborov, 2010)
If $\mathcal{A}=\left\{K_{4}^{3}\right\}$, then $\max _{G:|V(G)| \rightarrow \infty} d(G) \leq 0.561666$. If $\mathcal{A}=\left\{K_{4}^{3}, H_{1}\right\}$, then $\max _{G:|V(G)| \rightarrow \infty} d(G)=5 / 9$.

## Complexity Theory at Oberwolfach in 2015


"Is there a link between sums of squares theory and flag algebras?"

## Complexity Theory at Oberwolfach in 2015


"Is there a link between sums of squares theory and flag algebras?"

"No."

## Connection of spanning sets to flag algebras

$$
\begin{aligned}
& \mathrm{g}_{2 \cdot{ }_{\bullet \cdot 3}^{\Theta}}:=\operatorname{sym}_{\operatorname{hook}\left(\tau_{\lambda}\right)}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{X}_{14}\right) \\
& =\frac{1}{4}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{15} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{16} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{17} \mathrm{x}_{13} \mathrm{x}_{14}\right)
\end{aligned}
$$

where $\Theta(1)=1, \Theta(2)=4, \Theta(3)=3$, and $g_{2 \cdot 0_{03}}$ is the density of ${ }_{2 \cdot{ }^{\circ} \cdot_{3}}$ as a subgraph in some graph on 7 vertices under $\Theta^{\bullet \cdot 3}$.

Example: $g_{2 \cdot 0_{0}}^{\Theta}(\underbrace{2}_{5}$

## Connection of spanning sets to flag algebras

$$
\begin{aligned}
& \mathrm{g}_{2 \cdot{ }_{\bullet \cdot 3}^{\Theta}}:=\operatorname{sym}_{\operatorname{hook}\left(\tau_{\lambda}\right)}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{X}_{14}\right) \\
& =\frac{1}{4}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{15} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{16} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{17} \mathrm{x}_{13} \mathrm{x}_{14}\right)
\end{aligned}
$$

where $\Theta(1)=1, \Theta(2)=4, \Theta(3)=3$, and $g_{2 \cdot 0_{03}}$ is the density of ${ }_{2 \cdot{ }^{\circ} \cdot_{3}}$ as a subgraph in some graph on 7 vertices under $\Theta^{\bullet \cdot 3}$.

Example: $g_{2 \cdot \bullet_{0}}^{\Theta}\left(\int_{6}^{2}\right.$

## Connection of spanning sets to flag algebras

$$
\begin{aligned}
& \mathrm{g}_{2 \cdot{ }_{\bullet \cdot 3}^{\Theta}}:=\operatorname{sym}_{\operatorname{hook}\left(\tau_{\lambda}\right)}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{X}_{14}\right) \\
& =\frac{1}{4}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{15} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{16} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{17} \mathrm{x}_{13} \mathrm{x}_{14}\right)
\end{aligned}
$$

where $\Theta(1)=1, \Theta(2)=4, \Theta(3)=3$, and $g_{2 \cdot 0_{03}}$ is the density of ${ }_{2 \cdot{ }^{\circ} \cdot_{3}}$ as a subgraph in some graph on 7 vertices under $\Theta^{-3}$.

Example: $g_{2 \cdot 0_{0}}^{\Theta}(\underbrace{2}_{6}$

## Connection of spanning sets to flag algebras

$$
\begin{aligned}
& \mathrm{g}_{2 \cdot{ }_{\bullet \cdot 3}^{\Theta}}:=\operatorname{sym}_{\operatorname{hook}\left(\tau_{\lambda}\right)}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{X}_{14}\right) \\
& =\frac{1}{4}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{15} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{16} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{17} \mathrm{x}_{13} \mathrm{x}_{14}\right)
\end{aligned}
$$

where $\Theta(1)=1, \Theta(2)=4, \Theta(3)=3$, and $g_{2 \cdot 0_{03}}$ is the density of ${ }_{2 \cdot{ }^{\circ} \cdot_{3}}$ as a subgraph in some graph on 7 vertices under $\Theta^{-3}$.

Example: $g_{2 \cdot:_{\cdot 3}}^{\Theta}(\underbrace{2}_{6})=\frac{3}{4}$

## Connection of spanning sets to flag algebras

$$
\begin{aligned}
& \mathrm{g}_{2 \cdot{ }_{\bullet \cdot 3}^{\Theta}}:=\operatorname{sym}_{\operatorname{hook}\left(\tau_{\lambda}\right)}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{X}_{14}\right) \\
& =\frac{1}{4}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{15} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{16} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{17} \mathrm{x}_{13} \mathrm{x}_{14}\right)
\end{aligned}
$$

where $\Theta(1)=1, \Theta(2)=4, \Theta(3)=3$, and $g_{2 \cdot 0_{03}}$ is the density of ${ }_{2 \cdot{ }^{\circ} \cdot_{3}}$ as a subgraph in some graph on 7 vertices under $\Theta^{\bullet \cdot}$.

Example: $g_{2 \cdot 0_{0}}^{\Theta}(\underbrace{2}_{6}$

## Connection of spanning sets to flag algebras

$$
\begin{aligned}
& \mathrm{g}_{2 \cdot{ }_{\bullet \cdot 3}^{\Theta}}:=\operatorname{sym}_{\operatorname{hook}\left(\tau_{\lambda}\right)}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{X}_{14}\right) \\
& =\frac{1}{4}\left(\mathrm{x}_{12} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{15} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{16} \mathrm{x}_{13} \mathrm{x}_{14}+\mathrm{x}_{17} \mathrm{x}_{13} \mathrm{x}_{14}\right)
\end{aligned}
$$

where $\Theta(1)=1, \Theta(2)=4, \Theta(3)=3$, and $g_{2 \cdot 0_{03}}$ is the density of ${ }_{2 \cdot{ }^{\circ} \cdot_{3}}$ as a subgraph in some graph on 7 vertices under $\Theta^{-3}$.

Example: $g_{2 \cdot:_{\cdot 3}}^{\Theta}\left(\int_{6}^{2}\right)=\frac{3}{4}$

## Connection of spanning sets to flag algebras

Möbius transformation $\rightarrow \mathrm{d}_{2,}^{\Theta} \therefore_{1_{3}}$ : density of ${ }_{2 \cdot \therefore_{1}}$ as an induced subgraph in some graph on 7 vertices under $\Theta$ such that $\Theta(1)=1, \Theta(2)=4$, $\Theta(3)=3 \rightarrow$ flag density. Example:

$$
\begin{aligned}
& d_{2}^{\Theta} \therefore_{1_{3}}\left(\int_{4}^{3} \int_{5}^{2}\right)=0, d_{20}^{1} \therefore_{3}\left(\int_{4}^{3} \int_{0}^{2}\right)=0, \\
& \text { and } \mathrm{d}_{2 \cdot}^{\Theta} \dot{A}_{3}\left(\int_{4}^{3} \int_{6}^{2}\right)=\frac{1}{4}
\end{aligned}
$$

## Connection of spanning sets to flag algebras

## Theorem (RSST, 2016)

Flags provide spanning sets for $W_{\tau_{\lambda}}$ of size independent of $n$.
If $p$ is symmetric and $d$-sos, then its nonnegativity can be established through flags on kd vertices (even in restricted cases).

## Example

For the sos proof of Mantel's theorem, need at most flags:

## Connection of spanning sets to flag algebras

Theorem (R., Singh, Thomas, 2015)
Every flag sos polynomial of degree $k d$ can be written as a succinct $d$-sos.

Theorem (RSST, 2016)
Flag methods are equivalent to standard symmetry-reduction methods for finding sos certificates over discrete hypercubes.

## Consequences of this connection

## Corollary (RSST, 2016)

It is possible to use flags for a fixed n, not just asymptotic situations

## Example

The following flag sos yields the Ramsey number $R(3,3) \leq 6$

$$
-1 \equiv \frac{1}{8\binom{6}{2}}\left(\mathrm{~d}_{!}^{\Theta}+\mathrm{d}_{!}^{\Theta}\right)^{2}+\mathbb{E}_{\Theta_{i}}\left[\frac{1}{2}\left(\mathrm{~d}_{\bullet_{1}}^{\Theta_{i}}-\mathrm{d}_{\bullet_{i}}^{\Theta_{i}}\right)^{2}\right] \bmod \mathcal{I}
$$

where

$$
\begin{array}{ll}
\mathrm{d}_{\bullet}^{\Theta}=2 \sum_{1 \leq i<j \leq 6} \mathrm{x}_{i j}, & \mathrm{~d} \cdot=2 \sum_{1 \leq i<j \leq 6}^{\Theta}\left(1-\mathrm{x}_{i j}\right), \\
\mathrm{d}_{\bullet_{1}}^{\Theta_{i}}=\sum_{j \in[6] \backslash\{i\}} \mathrm{x}_{i j}, & \mathrm{~d}_{\bullet 1}^{\Theta_{i}}=\sum_{j \in[6] \backslash\{i\}}^{6}\left(1-\mathrm{x}_{i j}\right)
\end{array}
$$

## Consequences of this connection

## Corollary (RSST, 2016)

It is possible to use flags for extremal graph theoretic problems in the sparse setting.

## Example

The following flag sos yields that the max edge density in $C_{4}$-free graphs is at most $\frac{n^{3 / 2}}{n^{2}-n}+O\left(\frac{1}{n}\right)$ (Sós et al)

$$
\begin{aligned}
& n+\frac{2}{n-1} s-\frac{2}{\binom{n}{2}} s^{2} \equiv \\
& \mathbb{E}_{\Theta_{j k}}\left[n\left(\mathrm{~d}_{1 \bullet \bullet 2}^{\mathrm{\Theta}_{j k}}+\mathrm{d}_{1 \bullet \bullet 2}^{\Theta_{j k}}+\mathrm{d}_{1 \bullet \bullet 2}^{\Theta_{j k}}\right)^{2}+n\left(\underset{1 \bullet \bullet 2}{\mathrm{~d}_{\mathrm{O} k}}+\mathrm{d}_{1 \bullet \bullet 2}^{\Theta_{j k}}+\mathrm{d}_{1 \bullet \bullet 2}^{\Theta_{j k}}\right)^{2}\right. \\
& \left.+\frac{1}{2}\left(\mathrm{~d}_{1 \bullet \bullet 2}^{\Theta_{j k}}-\mathrm{d}_{1 \bullet \bullet 2}^{\Theta_{j k}}\right)^{2}+\frac{1}{2}\left(\mathrm{~d}_{1 \bullet \bullet 2}^{\Theta_{j k}}-\mathrm{d}_{1 \bullet \bullet 2}^{\Theta_{j k}}\right)^{2}\right] \bmod \mathcal{I}
\end{aligned}
$$

## Consequences of this connection

## Example (Grigoriev's family of polynomials, 2001)

The polynomials

$$
\mathrm{f}_{n}=\frac{1}{\binom{n}{2}^{2}}\left(\sum_{e \in E\left(K_{n}\right)} \mathrm{x}_{e}-\left\lfloor\frac{\binom{n}{2}}{2}\right\rfloor\right)\left(\sum_{e \in E\left(K_{n}\right)} \mathrm{x}_{e}-\left\lfloor\frac{\binom{n}{2}}{2}\right\rfloor-1\right)
$$

are nonnegative on $\mathcal{V}_{n, 2}$.
The degree required to write $f_{n}$ as a SOS is at least $\left[\begin{array}{c}n \\ \frac{n}{2} \\ 2\end{array}\right]$
Certifying nonnegativity $f_{n}+O\left(\frac{1}{n^{2}}\right)$ also requires an SOS of degree $\left[\begin{array}{c}\binom{n}{2} \\ 2\end{array}\right]$ (Lee, Prakesh, de Wolf, Yuen, 2016)

## Consequences of this connection

Hatami-Norin (2011) showed that the nonnegativity of graph density inequalities in general is undecidable

## Corollary (RSST, 2016)

There exists a family of symmetric nonnegative polynomials of fixed degree that cannot be certified with any fixed set of flags, namely

$$
\frac{1}{\binom{n}{2}^{2}}\left(\sum_{e \in E\left(K_{n}\right)} x_{e}-\left\lfloor\frac{\binom{n}{2}}{2}\right\rfloor\right)\left(\sum_{e \in E\left(K_{n}\right)} x_{e}-\left\lfloor\frac{\binom{n}{2}}{2}\right\rfloor-1\right)+O\left(\frac{1}{n^{2}}\right)
$$

Note: Razborov allows error of size $O\left(\frac{1}{n}\right)$ in his setting

## Open problems

- Find a concrete family of nonnegative polynomials on $\binom{n}{k}$ variables that one cannot approximate up to an error of order $O\left(\frac{1}{n}\right)$ with finitely many flags or with sums of squares of fixed degree.


## Open problems

- Find a concrete family of nonnegative polynomials on $\binom{n}{k}$ variables that one cannot approximate up to an error of order $O\left(\frac{1}{n}\right)$ with finitely many flags or with sums of squares of fixed degree. (Aaron Potechin?)


## Open problems

- Find a concrete family of nonnegative polynomials on $\binom{n}{k}$ variables that one cannot approximate up to an error of order $O\left(\frac{1}{n}\right)$ with finitely many flags or with sums of squares of fixed degree. (Aaron Potechin?)
- Provide certificates for open problems over $\mathcal{V}_{n, k}$ using symmetric sums of squares.


## Open problems

- Find a concrete family of nonnegative polynomials on $\binom{n}{k}$ variables that one cannot approximate up to an error of order $O\left(\frac{1}{n}\right)$ with finitely many flags or with sums of squares of fixed degree. (Aaron Potechin?)
- Provide certificates for open problems over $\mathcal{V}_{n, k}$ using symmetric sums of squares.


Figure 1: Closure of $\{(\rho(G), \delta(G))\}_{G:|V(G)| \rightarrow \infty}$.

## Thank you!

## Also check out _forall on instagram. . . and let me interview you?

