SDP hierarchies and quantum states

Aram Harrow (MIT)

Simons Institute 2014.1.17

a theorem

Let $M \in \mathbb{R}_+^{m \times n}$.
Say that a set $S \subseteq [n]^k$ is δ-good if $\exists\, \phi : [m]^k \to S$ such that $\forall (j_1, \ldots, j_k) \in S$,

$$\delta \sum_{\substack{(i_1,\ldots,i_k) \\ \in \phi^{-1}(j_1,\ldots,j_k)}} M_{i_1,j_1} \cdots M_{i_k,j_k} \geq \sum_{\substack{(i_1,\ldots,i_k) \\ \notin \phi^{-1}(j_1,\ldots,j_k)}} M_{i_1,j_1} \cdots M_{i_k,j_k}$$

$f(k, \delta) := \max\{ |S| : \exists\, S \subseteq [n]^k,\ S \text{ is } \delta\text{-good}\}$
Then

$$\lim_{\delta \to 0} \lim_{k \to \infty} \frac{1}{k} \ln(f(k,\delta)) = \sup_{x \in \mathbb{R}_+^n} \sum_{i,j} \frac{M_{i,j} x_j}{\sum_{i',j'} M_{i',j} x_{j'}} \ln \left(\frac{M_{i,j} \sum_{j'} x_{j'}}{\sum_{i'} M_{i',j} \cdot \sum_{j'} \frac{x_{j'} M_{i,j'}}{\sum_{i'} M_{i',j'}}} \right)$$

a theorem

The capacity of a noisy channel equals the maximum over input distributions of the mutual information between input and output.

[Shannon '49]

2->4 norm

Define $||x||_p := (\mathbb{E}_i\ |x_i|^p)^{1/p}$
Let $A \in \mathbb{R}^{m\times n}$.
$||A||_{2\to 4} := \max \{\ ||Ax||_4 : ||x||_2 = 1\}$

How hard is it to estimate this?

$$\|A\|_{2\to 4}^4 = \max_x \mathbb{E}_i \left(\sum_j A_{i,j} x_j \right)^4$$

$$= \max_x \sum_{j_1,j_2,j_3,j_4} \left(\mathbb{E}_i A_{i,j_1} A_{i,j_2} A_{i,j_3} A_{i,j_4} \right) x_{j_1} x_{j_2} x_{j_3} x_{j_4}$$

$$= \max_x \sum_{j_1,j_2,j_3,j_4} M_{j_1,j_2,j_3,j_4} x_{j_1} x_{j_2} x_{j_3} x_{j_4}$$

optimization problem over a degree-4 polynomial

SDP relaxation for 2->4 norm

$$\|A\|_{2\to 4}^4 \le \max_L \sum_{j_1,j_2,j_3,j_4} M_{j_1,j_2,j_3,j_4} L[x_{j_1} x_{j_2} x_{j_3} x_{j_4}]$$

where L is a linear map from deg ≤k polys to $\mathbb{R}$
L[1] = 1
$L[p(x)\ (\mathbb{E}_i\ x_i^2 - 1)] = 0$ if p(x) has degree ≤ k-2
$L[p(x)^2] \ge 0$ if p(x) has degree ≤ k/2

Converges to correct answer as k→∞. [Parrilo '00, Lasserre '01]

Runs in time $n^{O(k)}$

Why is this an SDP?

Constraint: $L[p(x)^2] \geq 0$ whenever $\deg(p) \leq k/2$

$p(x) = \Sigma_\alpha \, p_\alpha \, x^\alpha$

$\alpha = (\alpha_1, \ldots, \alpha_n)$

$\alpha_i \geq 0$

$\Sigma_i \alpha_i \leq k/2$

$L[p(x)^2] = \Sigma_{\alpha,\beta} \, L[x^{\alpha+\beta}] \, p_\alpha \, p_\beta$

≥ 0 for all $p(x)$ iff
M is positive semi-definite (PSD),
where $M_{\alpha,\beta} = L[x^{\alpha+\beta}]$

Why care about 2->4 norm?

Unique Games (UG):

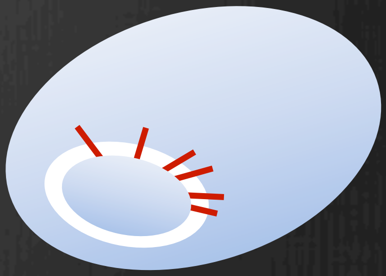
Given a system of linear equations: $x_i - x_j = a_{ij} \bmod k$.

Determine whether $\geq 1-\epsilon$ or $\leq \epsilon$ fraction are satisfiable.

Small-Set Expansion (SSE):

Is the minimum expansion of a set with $\leq \delta n$ vertices $\geq 1-\epsilon$ or $\leq \epsilon$?

UG ≈ SSE ≤ 2->4



G = normalized adjacency matrix

P_λ = largest projector s.t. $G \geq \lambda P$

Theorem:

All sets of volume $\leq \delta$ have expansion $\geq 1 - \lambda^{O(1)}$

iff

$\|P_\lambda\|_{2\to 4} \leq 1/\delta^{O(1)}$

quantum states

Pure states

- A quantum (pure) state is a unit vector $v \in \mathbb{C}^n$
- Given states $v \in \mathbb{C}^m$ and $w \in \mathbb{C}^n$, their joint state is $v \otimes w \in \mathbb{C}^{mn}$, defined as $(v \otimes w)_{i,j} = v_i \, w_j$.
- u is entangled iff it cannot be written as $u = v \otimes w$.

Density matrices

- ρ satisfying $\rho \geq 0$, $\mathrm{tr}[\rho]=1$
- extreme points are pure states, i.e. vv^*.
- can have classical correlation and/or quantum entanglement

correlated

$$\frac{e_0 e_0^* \otimes e_0 e_0^* + e_1 e_1^* \otimes e_1 e_1^*}{2}$$

entangled

$$\left(\frac{e_0 \otimes e_0 + e_1 \otimes e_1}{\sqrt{2}}\right)\left(\frac{e_0 \otimes e_0 + e_1 \otimes e_1}{\sqrt{2}}\right)^*$$

when is a mixed state entangled?

<u>Definition</u>: ρ is separable (i.e. not entangled) if it can be written as

$$\rho = \Sigma_i\, p_i\, v_i\, v_i^* \otimes w_i\, w_i^*$$

probability distribution

unit vectors

$$\text{Sep} = \text{conv}\{vv^* \otimes ww^*\}$$

Weak membership problem: Given ρ and the promise that $\rho \in \text{Sep}$ or ρ is far from Sep, determine which is the case.

Optimization: $h_{Sep}(M) := \max \{ \text{tr}[M\rho] : \rho \in \text{Sep} \}$

monogamy of entanglement

Physics version: ρ^{ABC} a state on systems ABC
AB entanglement and AC entanglement trade off.

"proof": If ρ^{AB} is very entangled, then measuring B can reduce the entropy of A, so ρ^{AC} cannot be very entangled.

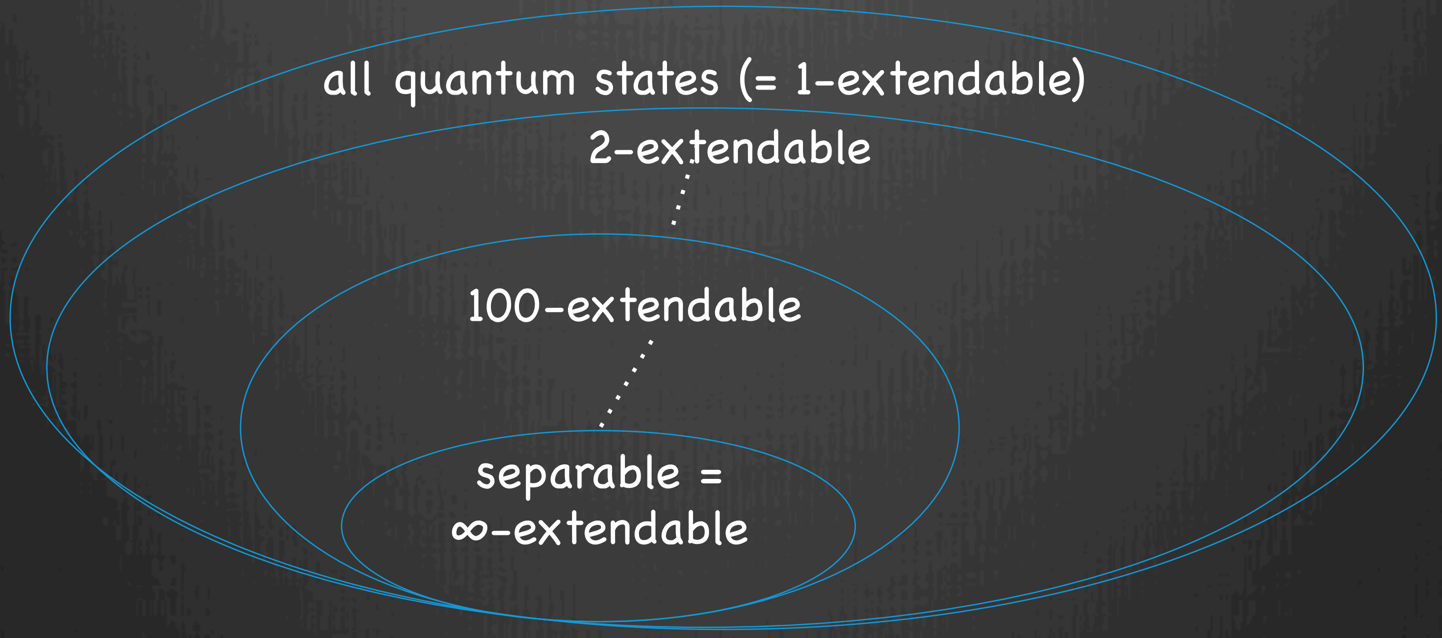
Partial trace: $\rho^{AB} = \mathrm{tr}_C\ \rho^{ABC}$

$$\rho^{AB}_{i_1,i_2;j_1,j_2} := \sum_{i_3} \rho^{ABC}_{i_1,i_2,i_3;j_1,j_2,i_3}$$

Works for any basis of C. Interpret as different choices of measurement on C.

A hierachy of tests for entanglement

Definition: ρ^{AB} is k-extendable if there exists an extension $\rho^{AB_1 \ldots B_k}$ with $\rho^{AB} = \rho^{AB_i}$ for each i.



Algorithms: Can search/optimize over k-extendable states in time $n^{O(k)}$.

Question: How close are k-extendable states to separable states?

2->4 norm ≈ h_{Sep}

$A = \Sigma_i\ e_i\ a_i^T$

$M = \mathbb{E}_i\ a_i\ a_i^T \otimes a_i\ a_i^T$

Easy direction:

$h_{Sep} \geq$ 2->4 norm

$$\|Ax\|_4^4 = \mathbb{E}_i \langle a_i, x\rangle^4 = \mathrm{tr} M\rho$$

$\rho = xx^* \otimes xx^*$

$$\|A\|_{2\to 4}^4 = h_{\mathrm{Sep}}(M)$$

Harder direction:

2->4 norm $\geq h_{Sep}$

Given an arbitrary M, can we make it look like $\mathbb{E}_i\ a_i a_i^* \otimes a_i a_i^*$?

Answer: yes, using techniques of [H, Montanaro; 1001.0017]

the dream

SSE <---> 2->4 <---> h_{Sep}

hardness

algorithms

...quasipolynomial (=exp(polylog(n)) upper and lower bounds for unique games

progress so far

SSE hardness??

1. Estimating $h_{Sep}(M) \pm 0.1$ for n-dimensional M is at least as hard as solving 3-SAT instance of length $\approx\log^2(n)$.
[H.-Montanaro 1001.0017] [Aaronson-Beigi-Drucker-Fefferman-Shor 0804.0802]

2. The Exponential-Time Hypothesis (ETH) implies a lower bound of $\Omega(n^{\log(n)})$ for $h_{Sep}(M)$.

3. ∴ lower bound of $\Omega(n^{\log(n)})$ for estimating $||A||_{2\text{->}4}$ for some family of projectors A.

4. These A might not be $P_{\geq\lambda}$ for any graph G.

5. (Still, first proof of hardness for constant-factor approximation of $||\cdot||_{2\to4}$).

positive results about hierarchies: 1. use dual

Primal: max $L[f(x)]$ over L such that
L is a linear map from deg $\leq k$ polys to $\mathbb{R}$
$L[1] = 1$
$L[p(x)\,(\Sigma_i\, x_i^2 - 1)] = 0$
$L[p(x)^2] \geq 0$

Dual: min λ such that
$f(x) + p(x)\,(\mathbb{E}_i\, x_i^2 - 1) + \Sigma_i\, q_i(x)^2 = \lambda$
for some polynomials $p(x)$, $\{q_i(x)\}$ s.t. all degrees are $\leq k$.

Interpretation: "Prove that $f(x)$ is $\leq \lambda$ using only the facts that $\mathbb{E}_i\, x_i^2 - 1 = 0$ and sum of square (SOS) polynomials are ≥ 0. Use only terms of degree $\leq k$."

"Positivestellensatz" [Stengel '74]

SoS proof example

$$z^2 \leq z \leftrightarrow 0 \leq z \leq 1$$

Axiom: $z^2 \leq z$

Derive: $z \leq 1$

$$1 - z = z - z^2 + (1-z)^2$$

$$\geq z - z^2 \quad \text{(non-negativity of squares)}$$

$$\geq 0 \quad \text{(axiom)}$$

SoS proof of hypercontractivity

Hypercontractive inequality:
Let $f:\{0,1\}^n \mapsto \mathbb{R}$ be a polynomial of degree $\leq d$. Then $\|f\|_4 \leq 9^{d/4} \|f\|_2$.

equivalently:
$\|P_d\|_{2\to 4} \leq 9^{d/4}$ where P_d projects onto deg $\leq d$ polys.

Proof:
uses induction on n and Cauchy-Schwarz.
Only inequality is $q(x)^2 \geq 0$.

Implication: SDP returns answer $\leq 9^{d/4}$ on input P_d.

SoS proofs of UG soundness

[BBHKSZ '12]

Result: Degree-8 SoS relaxation refutes UG instances based on long-code and short-code graphs

Proof: Rewrite previous soundness proofs as SoS proofs.

Ingredients:

1. Cauchy-Schwarz / Hölder
2. Hypercontractive inequality
3. Influence decoding
4. Independent rounding
5. Invariance principle

UG Integrality Gap:

Feasible SDP solution

SoS upper bound

Upper bound to actual solutions

actual solutions

positive results about hierarchies: 2. use q. info

[Brandão-Christandl-Yard '10] [Brandão-H. '12]

Idea:

Monogamy relations for entanglement imply performance bounds on the SoS relaxation.

Proof sketch:

ρ is k-extendable, lives on $AB_1 \ldots B_k$.

M can be implemented by measuring Bob, then Alice. (1-LOCC)

Let measurement outcomes be $X, Y_1, \ldots, Y_k$.

Then

$\log(n) \geq I(X:Y_1 \ldots Y_k) = I(X:Y_1) + I(X:Y_2|Y_1) + \ldots + I(X:Y_k|Y_1 \ldots Y_{k-1})$

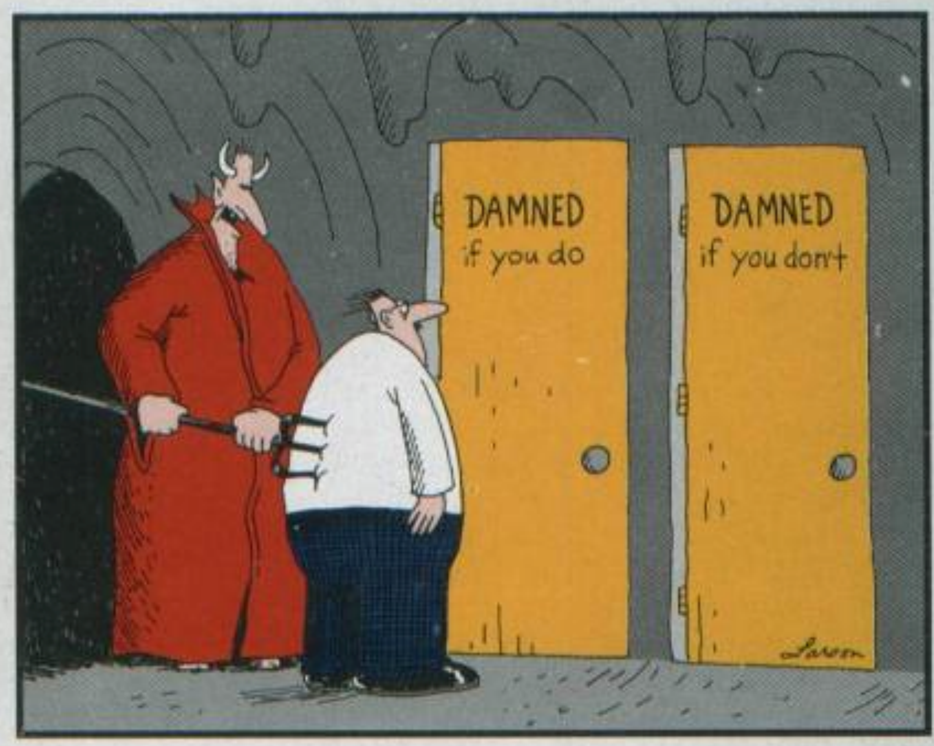
...algebra...

$h_{Sep}(M) \leq h_{k\text{-}ext}(M) \leq h_{Sep}(M) + c(\log(n) / k)^{1/2}$

Alternate perspective

For i=1,...,k

- Measure B_i.
- If entropy of A doesn't change, then $A:B_i$ are ≈product.
- If entropy of A decreases, then condition on B_i.



"C'mon, c'mon — it's either one or the other."

the dream: quantum proofs for classical algorithms

1. Information-theory proofs of de Finetti/monogamy, e.g. [Brandão-Christandl-Yard, 1010.1750] [Brandão-H., 1210.6367]
 $h_{Sep}(M) \leq h_{k\text{-}Ext}(M) \leq h_{Sep}(M) + (\log(n) / k)^{1/2} \|M\|$
 if $M \in$ 1-LOCC

2. $M = \sum_i a_i a_i^* \otimes a_i a_i^*$ is $\propto$ 1-LOCC.

3. Constant-factor approximation in time $n^{O(\log(n))}$?

4. Problem: $\|M\|$ can be $\gg h_{Sep}(M)$. Need multiplicative approximaton or we lose dim factors.

5. Still yields subexponential-time algorithm.

SDPs in quantum information

1. Goal: approximate Sep
   Relaxation: k-extendable + PPT

2. Goal: $\lambda_{\min}$ for Hamiltonian on n qudits
   Relaxation: L : k-local observables → $\mathbb{R}$
   such that $L[X^\dagger X] \geq 0$ for all k/2-local X.

3. Goal: entangled value of multiplayer games
   Relaxation: L : products of ≤k operators → $\mathbb{R}$
   such that $L[p^\dagger p] \geq 0$ $\forall$ noncommutative poly p of degree ≤ k,
   and operators on different parties commute.

Non-commutative positivstellensatz [Helton-McCullough '04]

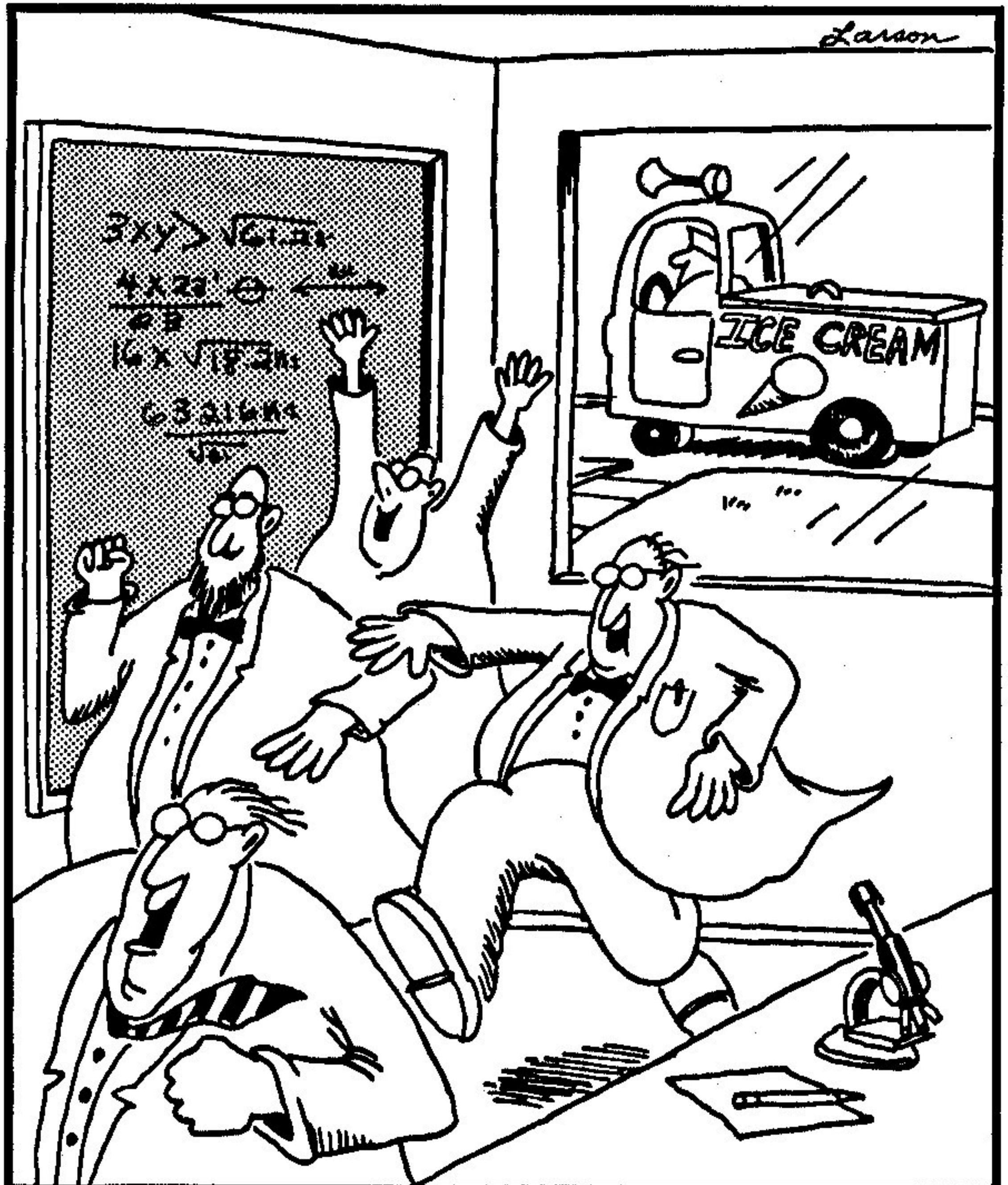
relation between these? tools to analyze?

questions

We are developing some vocabulary for understanding these hierarchies (SoS proofs, quantum entropy, etc.).
Are these the right terms?
Are they on the way to the right terms?

Unique games, small-set expansion, etc: quasipolynomial hardness and/or algorithms

Relation of different SDPs for quantum states.
More tools to analyze #2 and #3.


Larson
ICE CREAM

Why is this an SDP?

$$M = \begin{pmatrix} L[1] & L[x_1] & L[x_2] & L[x_1^2] & L[x_1x_2] & L[x_2^2] \\ L[x_1] & L[x_1^2] & L[x_1x_2] & L[x_1^3] & L[x_1^2x_2] & L[x_1x_2^2] \\ L[x_2] & L[x_1x_2] & L[x_2^2] & L[x_1^2x_2] & L[x_1x_2^2] & L[x_2^3] \\ L[x_1^2] & L[x_1^3] & L[x_1^2x_2] & L[x_1^4] & L[x_1^3x_2] & L[x_1^2x_2^2] \\ L[x_1x_2] & L[x_1^2x_2] & L[x_1x_2^2] & L[x_1^3x_2] & L[x_1^2x_2^2] & L[x_1x_2^3] \\ L[x_2^2] & L[x_1x_2^2] & L[x_2^3] & L[x_1^2x_2^2] & L[x_1x_2^3] & L[x_2^4] \end{pmatrix}$$