

Generalized matrix completion and algebraic natural proofs

Markus Bläser

Saarland University

with Christian Ikenmeyer, Gorav Jindal, and Vladimir Lysikov

Natural proofs

Definition (Razborov & Rudich)

A property \mathcal{P} of Boolean functions is *natural* if it has the following properties:

Usefulness: If $f : \{0, 1\}^n \rightarrow \{0, 1\}$ has $\text{poly}(n)$ -sized circuits, then $f \in \mathcal{P}$.

Constructivity: Given f by a truthtable of size $N = 2^n$, we can decide $f \in \mathcal{P}$ in time $\text{poly}(N)$.

Largeness: A random function is not in \mathcal{P} with probability at least $1/\text{poly}(N) = 2^{-O(n)}$.

The Razborov–Rudich barrier

- ▶ A function $f : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}$ is *pseudorandom* if when sampling the key $k \in \{0, 1\}^\ell$ uniformly at random, the resulting distribution $f(\cdot, k)$ is computationally indistinguishable from a truly random function.
- ▶ If oneway functions exists, so do pseudorandom functions.

Theorem (Razborov & Rudich)

A natural property \mathcal{P} distinguishes a pseudorandom function having $\text{poly}(n)$ -size circuits from a truly random function in time $2^{O(n)}$.

Conclusion

If you believe in private key cryptography, then no natural proof will show superpolynomial circuit lower bounds.

Algebraic natural proofs

Definition (Forbes, Shpilka & Volk)

Let $M \subseteq K[X]$ be a set of monomials.

Let $\mathcal{C} \subseteq \langle M \rangle$ and let $\mathcal{D} \subseteq K[T_m : m \in M]$.

A polynomial $D \in \mathcal{D}$ is an *algebraic \mathcal{D} -natural proof against \mathcal{C}* , if

1. D is a nonzero polynomial and
2. for all $f \in \mathcal{C}$, $D(f) = 0$, that is, D vanishes on the coefficient vectors of all polynomials in \mathcal{C} .

A similar concept was defined independently by Grochow, Kumar, Saks & Saraf.

Succinct hitting sets

Definition

A *hitting set* for $\mathcal{P} \subseteq K[X_1, \dots, X_\mu]$ is a set $\mathcal{H} \subseteq K^\mu$ such that for all $p \in \mathcal{P}$, there is an $h \in \mathcal{H}$ such that $p(h) \neq 0$.

Definition (Succinct hitting sets)

Let $M \subseteq K[X]$ be a set of monomials.

Let $\mathcal{C} \subseteq \langle M \rangle$ and let $\mathcal{D} \subseteq K[T_m : m \in M]$.

\mathcal{C} is a *\mathcal{C} -succinct hitting set* for \mathcal{D} if \mathcal{C} viewed as a set of vectors of coefficients of length $|M|$ is a hitting set for \mathcal{D} .

The Forbes–Shpilka–Volk barrier

Theorem

Let $M \subseteq K[X]$ be a set of monomials.

Let $\mathcal{C} \subseteq \langle M \rangle$ and let $\mathcal{D} \subseteq K[T_m : m \in M]$.

There are algebraic \mathcal{D} -natural proofs against \mathcal{C} iff \mathcal{C} is not a \mathcal{C} -succinct hitting set for \mathcal{D} .

Corollary

Let $\mathcal{C} \subseteq K[X_1, \dots, X_n]$ with degree $\leq d$ and computable by $\text{poly}(n, d)$ -size circuits.

Then there is an algebraic $\text{poly}(N_{n,d})$ -natural proof against \mathcal{C} iff there is no $\text{poly}(n, d)$ -succinct hitting set for $\text{poly}(N_{n,d})$ -size circuits in $N_{n,d}$ variables.

The Forbes–Shpilka–Volk barrier (2)

Typical regime:

- ▶ $N_{n,d} = \binom{n+d}{d}$
- ▶ $d = \text{poly}(n) \longrightarrow \text{poly}(n) = \text{poly} \log(N_{n,d})$

Conjecture/Wish/Fear

There $\text{poly} \log(N)$ -succinct hitting sets for $\text{poly}(N)$ -size circuits.

Tensor rank

Definition

1. A tensor $t \in K^{k \times m \times n}$ has rank-one if $t = u \otimes v \otimes w := (u_h v_i w_j)$ for $u \in K^k$, $v \in K^m$, and $w \in K^n$.
2. The rank $R(t)$ of a tensor $t \in K^{k \times m \times n}$ is the smallest number r of rank-one tensors s_1, \dots, s_r such that $t = s_1 + \dots + s_r$.
3. S_r denotes the set of all tensors of rank r .

Definition

$D \in K[X_1, \dots, X_{kmn}]$ is a $\text{poly}(k, m, n)$ -natural proof against S_r if

- ▶ D is nonzero,
- ▶ D vanishes on S_r , and
- ▶ D is computed by circuits of size $\text{poly}(k, m, n)$.

Tensor rank (2)

Good news:

Theorem (Håstad)

Tensor rank is NP-hard.

Theorem (Shitov; Schaefer & Stefankovic)

Tensor rank is as hard as the existential theory over K .

Bad news:

- ▶ S_r is not the zero set of a set of polynomials.
- ▶ When D vanishes on S_r , it also vanishes on its closure $\overline{S_r}$.
- ▶ $X_r := \overline{S_r}$ is the set of tensors of *border rank* $\leq r$.
- ▶ X_r contains tensors of rank $> r$.

(Generalized) matrix completion

Definition

Let $A_0, A_1, \dots, A_m \in \mathbb{K}^{n \times n}$. The *completion rank* of A_0, A_1, \dots, A_m is the minimum number r such that there are scalars $\lambda_1, \dots, \lambda_m$ with

$$\text{rk}(A_0 + \lambda_1 A_1 + \dots + \lambda_m A_m) \leq r.$$

We denote the completion rank by $\text{CR}(A_0, A_1, \dots, A_m)$.

- ▶ Can also be phrased in terms of an affine linear matrix $A_0 + X_1 A_1 + \dots + X_m A_m$.

(Generalized) matrix completion (2)

- ▶ The set of all $(m + 1)$ -tuples of $n \times n$ -matrices together with m scalars $\lambda_1, \dots, \lambda_m$

$$(\mathbf{A}_0, \mathbf{A}_1, \dots, \mathbf{A}_m, \lambda_1, \dots, \lambda_m) \in \mathbb{K}^{(m+1)n^2+m}$$

such that

$$\text{rk}(\mathbf{A}_0 + \lambda_1 \mathbf{A}_1 + \dots + \lambda_m \mathbf{A}_m) \leq r$$

is a closed set, since it is defined by vanishing of all $(r + 1) \times (r + 1)$ -minors.

- ▶ Denote this set by $P_r^{m,n}$.
- ▶ Let $C_r^{m,n}$ be the projection of $P_r^{m,n}$ onto the first $(m + 1)n^2$ components, that is, $C_r^{m,n}$ is the set of all $(\mathbf{A}_0, \mathbf{A}_1, \dots, \mathbf{A}_m)$ with $\text{CR}(\mathbf{A}_0, \mathbf{A}_1, \dots, \mathbf{A}_m) \leq r$.
- ▶ $C_r^{m,n}$ is not closed.

Example

- ▶ Let

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad A_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

$$\text{CR}(A_0, A_1) = 2.$$

- ▶ Let

$$\underbrace{\begin{pmatrix} 1 & 0 \\ \epsilon & 1 \end{pmatrix}}_{=: A_{0,\epsilon}} + \frac{1}{\epsilon} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1/\epsilon \\ \epsilon & 1 \end{pmatrix}.$$

$$\text{CR}(A_{0,\epsilon}, A_1) = 1 \text{ for every } \epsilon \neq 0.$$

- ▶ $(A_{0,\epsilon}, A_1)$ converges to (A_0, A_1) in the Euclidean topology.
- ▶ (A_0, A_1) is contained in the Euclidean closure of C_1 .

Closure

Example:

- ▶ Let B be any rank-one matrix.
- ▶ The completion rank of (I, B) is at least $n - 1$.
- ▶ We can approximate B by $B + \epsilon I$.
- ▶ But $I - \frac{1}{\epsilon}(B + \epsilon I)$ has rank 1.

Conclusion:

- ▶ The rank of the approximating matrices should not be larger than the rank of the matrix itself.
- ▶ We take the closure in $K^{n \times n} \times K_{r_1}^{n \times n} \times \dots \times K_{r_m}^{n \times n}$, where $K_{\rho}^{n \times n}$ denotes the closed set of matrices of rank at most ρ and $r_i = \text{rk}(A_i)$.

Border completion rank

Definition

Let $A_0, A_1, \dots, A_m \in K^{n \times n}$. The *border completion rank* of A_0, A_1, \dots, A_m is the minimum number r such that there are approximations $\tilde{A}_i \in K(\epsilon)^{n \times n}$ with $\tilde{A}_i = A_i + O(\epsilon)$, $0 \leq i \leq m$, and rational functions $\lambda_1, \dots, \lambda_m \in K(\epsilon)$ with

$$\text{rk}(\tilde{A}_0 + \lambda_1 \tilde{A}_1 + \dots + \lambda_m \tilde{A}_m) \leq r.$$

We denote the border completion rank by $\underline{\text{CR}}(A_0, A_1, \dots, A_m)$.

Hardness of completion rank

- ▶ ϕ formula in 2-CNF over the variables x_1, \dots, x_t with clauses c_1, \dots, c_s .
- ▶ Given b , it is NP-hard to decide whether there is an assignment satisfying at least b clauses.

Clause gadget: $c_i = L_1 \vee L_2$

$$\begin{pmatrix} 1 - \ell_1 & 1 \\ 0 & 1 - \ell_2 \end{pmatrix}$$

- ▶ ℓ_j in the matrix is x_k if the literal $L_j = x_k$ and it is $1 - x_k$ if $L_j = \neg x_k$, $j = 1, 2$.

Observation

The clause gadget has rank 1 iff at least one of the literals ℓ_1, ℓ_2 is set to be 1. Otherwise, it has rank 2.

Hardness of completion rank (2)

- ▶ All clause gadgets are blocks of our desired block diagonal matrix.
- ▶ We get a matrix $A_0 + x_1 A_1 + \dots + x_t A_t$ with affine linear forms as entries

Proposition

$\text{CR}(A_0, A_1, \dots, A_t) \leq 2s - b$ iff b clauses of ϕ can be satisfied.

Thus the problem $\text{CR}(A_0, A_1, \dots, A_t) \stackrel{?}{\leq} k$ is NP-hard.

Hardness of border completion rank

Observation

Each A_i , $i \geq 1$, is a diagonal matrix with diagonal entries ± 1 . If the j^{th} diagonal entry of A_i is nonzero, then the j^{th} diagonal entry of any other A_k is zero, $i, k \geq 1$.

Let $\tilde{A}_0, \tilde{A}_1, \dots, \tilde{A}_t$ be approximations to A_0, A_1, \dots, A_t , that is, $\tilde{A}_i = A_i + O(\epsilon)$.

Lemma

There are (invertible) matrices $S = I_n + O(\epsilon)$ and $T = I_n + O(\epsilon)$ such that $S \cdot (\tilde{A}_0 + \lambda_1 \tilde{A}_1 + \dots + \lambda_t \tilde{A}_t) \cdot T = \hat{A}_0 + \lambda_1 A_1 + \dots + \lambda_t A_t$ for some $\hat{A}_0 = A_0 + O(\epsilon)$.

Hardness of border completion rank (2)

Lemma

$\underline{\text{CR}}(A_0, A_1, \dots, A_t) \leq 2s - b$ iff b clauses of ϕ can be satisfied.

- ▶ \Leftarrow follows from hardness proof for CR.
- ▶ Assume there are $\lambda_i = \alpha_{i,0}\epsilon^{d_i} + \alpha_{i,1}\epsilon^{d_i+1} + \dots$ with $\alpha_{i,0} \neq 0$ such that $\text{rk}(\tilde{A}_0 + \lambda_1 A_1 + \dots + \lambda_t A_t) \leq 2s - b$.
- ▶ λ_i induce an assignment to the x_i and thus to literals ℓ_j .
- ▶ A clause gadget looks like

$$\begin{pmatrix} 1 + O(\epsilon) - \ell_1 & 1 + O(\epsilon) \\ O(\epsilon) & 1 + O(\epsilon) - \ell_2 \end{pmatrix}$$

To have rank 1, $\ell_1 = 1 + O(\epsilon)$ or $\ell_2 = 1 + O(\epsilon)$. We call such clauses “ ϵ -satisfied”.

- ▶ If we have at least b “ ϵ -satisfied” clauses, then we substitute $\epsilon = 0$ in corresponding λ_i and get an exact assignment.
- ▶ If there are $< b$ ϵ -satisfied clauses, then $\underline{\text{CR}}(A_0, A_1, \dots, A_t) > 2s - b$.

Algebraic natural proofs for border completion rank

Let $t \in \mathbb{K}^{n \times n \times (m+1)}$. An *algebraic poly(n)-natural proof* for the border completion rank of t being $> r$ is a polynomial

$P \in \mathbb{K}[X_{h,i,j} | 1 \leq h, i \leq n, 1 \leq j \leq m]$ such that

1. $P(t) \neq 0$,
2. $P(s) = 0$ for every $s \in \mathbb{K}^{n \times n \times (m+1)}$ with $\underline{\text{CR}}(s) \leq r$.
3. P is computed by a constant-free algebraic circuit of size $\text{poly}(n)$.

Universal tensors

Observation

Let $U_{i,j}, V_{i,j}$, $1 \leq i \leq \rho$, $1 \leq j \leq n$ be indeterminates. If we substitute arbitrary constants for the indeterminates in $\sum_{i=1}^{\rho} (U_{i,1}, \dots, U_{i,n})^T (V_{i,1}, \dots, V_{i,n})$, then we get all matrices in $\mathbb{K}_{\rho}^{n \times n}$.

Lemma

Let Q_0, Q_1, \dots, Q_t be polynomial matrices as in the observation above having ranks r_0, \dots, r_t , respectively. We use fresh variables for each Q_i .

Let $g := (Q_0 - Z_0 Q_1 - \dots - Z_t Q_t, Q_1, \dots, Q_t)$, where Z_1, \dots, Z_t are new variables. If we substitute arbitrary constants for the indeterminates, then we get all tensors of completion rank $\leq r_0$ with the i^{th} slice having rank $\leq r_i$, $1 \leq i \leq t$.

Main result

Theorem

For infinitely many n , there is an m , a tensor $t \in K^{n \times n \times m}$ and a value r such that there is no algebraic $\text{poly}(n)$ -natural proof for the fact that $\underline{\text{CR}}(t) > r$ unless $\text{coNP} \subseteq \exists\text{BPP}$.

- ▶ Let ϕ be a formula in 2-CNF and let $b \in \mathbb{N}$. We want to check whether every assignment satisfies $< b$ clauses of ϕ . This problem is coNP-hard.
- ▶ Let $T_\phi = (A_0, \dots, A_t)$ be the tensor constructed above.
- ▶ Guess a circuit C of polynomial size computing some P .
- ▶ Decide whether $P(g) = 0$ using polynomial identity testing.
- ▶ Check whether $P(T_\phi) \neq 0$. If yes, then accept. Otherwise reject.

Relation to tensor (border) rank

Theorem (Derksen)

If $\mathbf{t} = (A_0, A_1, \dots, A_m)$ is a concise tensor such that $\text{rk}(A_1) = \dots = \text{rk}(A_m) = 1$. Then

$$R(\mathbf{t}) = \text{CR}(\mathbf{t}) + m.$$

Proposition

If $\mathbf{t} = (A_0, A_1, \dots, A_m)$ is a tensor such that $\text{rk}(A_1) = \dots = \text{rk}(A_m) = 1$. Then

$$\underline{R}(\mathbf{t}) \leq \underline{\text{CR}}(\mathbf{t}) + m.$$

Tensor rank is hard to approximate

- ▶ Let ϕ be a formula in 3-CNF with t variables and s clauses such that every variable appears in a constant number c of clauses. Note that $s = O(t)$.
- ▶ We construct a matrix completion problem as before.
- ▶ We will have variable gadgets and clause gadgets.
- ▶ They will appear as blocks on the main diagonal.
- ▶ **Problem:** Everything needs to be of rank 1.

Variable gadget

$$\begin{pmatrix} 1 & x & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & u & 0 & u - u_1 & 0 & u - u_2 & 0 & 0 \\ 0 & u - u_3 & 1 & u & 0 & u - u_4 & 0 & 0 \\ 0 & 0 & 1 & v & 0 & 0 & 0 & 2v - v_1 \\ 0 & u - u_5 & 0 & u - u_6 & 1 & u & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & w & 2w - w_1 & 0 \\ 0 & 0 & 0 & v - v_2 & 0 & 0 & 1 & 2(v - 1/2) \\ 0 & 0 & 0 & 0 & 0 & w - w_2 & 2(w - 1/2) & 1 \end{pmatrix}$$

Lemma

1. If x is set to 0 or 1, then the local variables in the variable gadget can be set such that the resulting matrix has rank 4.
2. If the variables are set in such a way that the rank of the variable gadget is 4, then x is set to 0 or 1.

Variable gadget

$$\begin{pmatrix} 1 & x & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & u & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & u & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & v & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & u & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & w & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2(v - 1/2) \\ 0 & 0 & 0 & 0 & 0 & 0 & 2(w - 1/2) & 1 \end{pmatrix}$$

Lemma

1. If x is set to 0 or 1, then the local variables in the variable gadget can be set such that the resulting matrix has rank 4.
2. If the variables are set in such a way that the rank of the variable gadget is 4, then x is set to 0 or 1.

Clause gadget

$$\begin{pmatrix} 1 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & u & 0 & 0 & 0 & 0 & s(u) - u_1 & 0 & 0 \\ 0 & 0 & 1 & y & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & v & 0 & 0 & 0 & s(v) - v_1 & 0 \\ 0 & 0 & 0 & 0 & 1 & z & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & w & 0 & 0 & s(w) - w_1 \\ 0 & u - u_2 & 0 & 0 & 0 & 0 & 1 - \ell(u) & 1 & 0 \\ 0 & 0 & 0 & v - v_2 & 0 & 0 & 0 & 1 - \ell(v) & 1 \\ 0 & 0 & 0 & 0 & 0 & w - w_2 & 0 & 0 & 1 - \ell(w) \end{pmatrix}$$

- ▶ $\ell(u) = u$ if x appears positive in the clause and $\ell(u) = 1 - u$ otherwise.
- ▶ $s(u) = -u$ if x appears positive in the clause and $s(u) = u$ otherwise.

Hardness of approximation

Lemma

Assume that ϕ is either satisfiable or any assignment satisfies at most $(1 - \epsilon)$ of the clauses for some $\epsilon > 0$.

1. If ϕ is satisfiable, then the completion rank of T_ϕ is $4t + 5s$.
2. If ϕ is not satisfiable, then the completion rank of T_ϕ is at least $4t + 5s + \delta t$ for some constant $\delta > 0$.

Theorem

Tensor rank is NP-hard to approximate.

Matrices with permanent zero

Let X be an $n \times n$ matrix. Construct a matrix Z as follows:

$$\begin{cases} z_{ij} = x_{ij} & \text{for } i \leq n-1, \\ z_{nj} = x_{nj} \operatorname{per} X_{nn} & \text{for } j \leq n-1, \\ z_{nn} = -\sum_{j=1}^{n-1} x_{nj} \operatorname{per} X_{nj}, \end{cases}$$

where X_{ij} is the matrix obtained from X by removing the i^{th} row and the j^{th} column.

Observation

We have $\operatorname{per} Z = 0$. Moreover, any matrix with $\operatorname{per} Z = 0$ and $\operatorname{per} Z_{nn} \neq 0$ can be obtained in this way.

Natural proofs for matrices with permanent zero

Theorem

Let $\mathcal{Z}_n \subseteq \mathbb{K}^{n \times n}$ be the set of matrices with permanent 0. If \mathcal{Z}_n has algebraic VP^0 -natural proofs, then $P^{\#P} \subseteq \exists BPP$.

- ▶ Construct iteratively a polynomial size circuit computing per_k .
- ▶ Using the circuit for per_{k-1} compute a small circuit computing Z_k .
- ▶ Guess a polynomial size circuit C_k vanishing on \mathcal{Z}_k
- ▶ Verify this by checking $C_k(Z_k) = 0$.
- ▶ By Hilbert's Nullstellensatz, per_k^e divides C_k .
- ▶ Compute a small circuit of per_k using Kaltofen's factoring algorithm.

GCT breaks the algebraic natural proofs barrier

- ▶ $\mathcal{Z} \subseteq \mathbb{C}^{n \times n}$ all matrices with permanent 0.
- ▶ $GL_n \times GL_n$ acts on $\mathbb{C}^{n \times n}$ via left-right multiplication:

$$(g_1, g_2) \cdot A := g_1 A (g_2)^T.$$

- ▶ Let $Q_n \subseteq GL_n$ denote the group of monomial matrices, i.e., matrices with nonzero determinant that have a single nonzero entry in each row and column.
- ▶ \mathcal{Z} is closed under the action of the group $G := Q_n \times Q_n \subseteq GL_n \times GL_n$, which means that if $A \in \mathcal{Z}$, then $gA \in \mathcal{Z}$ for all $g \in G$.

The GCT framework

- ▶ Assume that $A \in \mathcal{Z}$.
- ▶ $GA := \{gA \mid g \in G\}$ is contained in \mathcal{Z}
- ▶ $\overline{GA} \subseteq \mathcal{Z}$ as a subvariety.
- ▶ For a Zariski-closed subset $Y \subseteq \mathbb{C}^{n \times n}$ let $I(Y) \subseteq \mathbb{C}[\mathbb{C}^{n \times n}]$ denote the *vanishing ideal* of Y .
- ▶ $I(Y)_d$ the homogeneous degree d component of $I(Y)$.
(inherits grading)
- ▶ *Coordinate ring* $\mathbb{C}[Y]$ of Y is the quotient
 $\mathbb{C}[Y] := \mathbb{C}[\mathbb{C}^{n \times n}] / I(Y)$,
inherits the grading $\mathbb{C}[Y]_d := \mathbb{C}[\mathbb{C}^{n \times n}]_d / I(Y)_d$.
- ▶ Since $\overline{GA} \subseteq \mathcal{Z}$, $I(\mathcal{Z})_d \subseteq I(\overline{GA})_d$ for all d .
- ▶ Canonical surjection by restriction: $\mathbb{C}[\mathcal{Z}]_d \twoheadrightarrow \mathbb{C}[\overline{GA}]_d$

Representations

Definition

- ▶ An *H-representation* is a finite dimensional vector space V with a group homomorphism $\rho : H \rightarrow GL(V)$.
We write gf for $(\rho(g))(f)$.
- ▶ A linear map $\varphi : V_1 \rightarrow V_2$ between two H -representations is called *equivariant* if for all $g \in H$ and $f \in V_1$, $\varphi(gf) = g\varphi(f)$.
- ▶ A bijective equivariant map is called an H -isomorphism.
- ▶ Two H -representations are called *isomorphic* if an H -isomorphism exists from one to the other.
- ▶ A linear subspace of an H -representation that is closed under the action of H is called a *subrepresentation*.
- ▶ An H -representation whose only subrepresentations are itself and 0 is called *irreducible*.

Representations (2)

- ▶ *Canonical pullback*: $(gf)(B) := f(g^T B)$
for $g \in G$, $f \in \mathbb{C}[Y]$, $B \in \mathbb{C}^{n \times n}$.
- ▶ Turns $\mathbb{C}[\mathcal{Z}]_d$ and $\mathbb{C}[\overline{GA}]_d$ into G -representations.
- ▶ G is *linearly reductive*, which means that every G -representation V decomposes into a direct sum of irreducible representations.
- ▶ For each type λ the *multiplicity* $\text{mult}_\lambda(V)$ of λ in V is unique.

Lemma (Schur)

For an equivariant map $\varphi : V \rightarrow W$, the image $\varphi(V)$ is a G -representation and $\text{mult}_\lambda(V) \geq \text{mult}_\lambda(\varphi(V))$.

- ▶ The map $\mathbb{C}[\mathcal{Z}]_d \rightarrow \mathbb{C}[\overline{GA}]_d$ is equivariant, thus

$$\text{mult}_\lambda(\mathbb{C}[\mathcal{Z}]_d) \geq \text{mult}_\lambda(\mathbb{C}[\overline{GA}]_d).$$

- ▶ A λ that violates this is an *obstruction* and proves “ $A \notin \mathcal{Z}$ ”.

Main result

Theorem

Let $G := Q_n \times Q_n$ and $\nu := (((1^n), (n)), ((1^n), (n)))$. Then

- ▶ $\text{mult}_\nu(\mathbb{C}[Z]_n) = 0$ and
- ▶ $\text{mult}_\nu(\mathbb{C}[\overline{GA}]_n) = \begin{cases} 0 & \text{if } A \in Z \\ 1 & \text{otherwise} \end{cases}$.

- ▶ Subrepresentation is $\langle \text{per} \rangle$ with $\text{mult}_\nu \mathbb{C}[\mathbb{C}^{n \times n}]_n = 1$.
- ▶ $\text{mult}_\nu(I(Z)_n) = 1$ and thus $\text{mult}_\nu(\mathbb{C}[Z]_n) = 0$.
- ▶ For $A \in Z$, $\overline{GA} \subseteq Z$. Therefore $\text{mult}_\nu(\mathbb{C}[\overline{GA}]_n) = 0$.
- ▶ For $A \notin Z$, $\text{mult}_\nu(I(\overline{GA})_n) = 0$ and therefore $\text{mult}_\nu(\mathbb{C}[\overline{GA}]_n) = 1$.

Thank You!