Polynomial Identity Testing and the Combinatorics of Completely Positive Operators

Berlin Mathematical School

Technische Universität Berlin

Josué Tonelli-Cueto

Polynomial Identity Testing

Polynomial Identity Testing (**PIT**) is the problem of deciding if a given "program" in an algebraic computational model computes the zero polynomial.
Example: One of the **PIT** coming from the Symbolic Determinant is the following:

SING: Given square matrices $A_1, \dots, A_m$ over K, are all the matrices in $\mathrm{span}(A_1, \dots, A_m)$ singular?

This version has the advantage of being related to problems in invariant theory, linear algebra and algebraic geometry.
Question: Can we solve efficiently **PIT**?
Probabilistic solution. Using the DeMillo-Lipton-Schwartz–Zippel lemma, one can show that, for all reasonable algebraic computational models, **PIT** can be solved efficiently by evaluating at a randomly chosen point.
Open question: Can we solve efficiently **PIT** in a deterministic way?
Why do we care? (Kabanaets, Impagliazzo; 2004) showed that providing better algorithms for **PIT**, even for **SING**, would provide non-trivial unknown lower bounds in complexity theory.

Completely Positive Operators

A *completely positive operator* is a positive map $\Phi : \mathrm{PSD}^{\mathcal{H}} \to \mathrm{PSD}^{\mathcal{H}'}$ such that for all $r \geq 0$,

$$\Phi \otimes \mathrm{id}_{\mathrm{PSD}^{\mathbb{C}^r}} : \mathrm{PSD}^{\mathcal{H}\otimes\mathbb{C}^r} \to \mathrm{PSD}^{\mathcal{H}'\otimes\mathbb{C}^r} \text{ is positive.}$$

Theorem. *(Hill; 1973) (Choi; 1975) Every completely positive operator $\Phi : \mathrm{PSD}^{\mathcal{H}} \to \mathrm{PSD}^{\mathcal{H}'}$ has the form $X \mapsto \sum_{i=1}^m A_i X A_i^*$ where $A_1, \dots, A_m \in \mathrm{hom}(\mathcal{H}, \mathcal{H}')$. Even more, this translates into an isomorphism*

$$\mathrm{Ch} : \mathrm{hom}_+(\mathrm{PSD}^{\mathcal{H}}, \mathrm{PSD}^{\mathcal{H}'}) \to \mathrm{PSD}^{\mathrm{hom}(\mathcal{H},\mathcal{H}')}$$

of convex cones, called the Choi-Hill isomorphism.

A *Kraus representation* of Φ is a tuple $(A_1, \dots, A_m)$ such that Φ has the form $X \mapsto \sum_{i=1}^m A_i X A_i^*$.
It is important to note that $\mathrm{hom}_+(\mathrm{PSD}^{\mathcal{H}}, \mathrm{PSD}^{\mathcal{H}'})$ and $\mathrm{hom}(\mathrm{PSD}^{\mathcal{H}}, \mathrm{PSD}^{\mathcal{H}'})$ are very different in general.

Fast introduction to information theory, convex geometry and the discrete/classical vs. continuous/quantum analogy

	Information theory	Convex Geometry	Discrete Classical	Continuous Quantum
Probabilistic	Configuration space	Convex cone K	$\mathbb{R}^S_\geq$	$\mathrm{PSD}^{\mathcal{H}}$
	Probability	Strictly positive functional	1-norm $\|\cdot\|_1$	Trace map Tr
	Uniform event	Interior point	$\mathbb{1}_S := (1)_{s\in S}$	$\mathbb{I}_{\mathcal{H}}$
	Transformation	Class of positive maps	Positive map: $\phi : x \mapsto Ax$, $A \in \mathbb{R}^{T\times S}$ with $A^t_s \geq 0$	Completely positive map: $\Phi : S \mapsto \sum_{i=1}^m A_i S A_i^*$, $A_i \in \mathrm{hom}(\mathcal{H}, \mathcal{H}')$
	Set of transformations	$\mathcal{C} \subseteq \mathrm{hom}(K, K')$	$\mathrm{hom}(\mathbb{R}^S_\geq, \mathbb{R}^T_\geq) \cong \mathbb{R}^{T\times S}_\geq$	$\mathrm{hom}_+(\mathrm{PSD}^{\mathcal{H}}, \mathrm{PSD}^{\mathcal{H}'}) \cong \mathrm{PSD}^{\mathrm{hom}(\mathcal{H},\mathcal{H}')}$
	Reverse transformation	Dual	$\phi^* : x \mapsto A^* x$, * transposition	$\Phi^* : S \mapsto \sum_{i=1}^m A_i^* S A_i$, * conjugate transposition
	Stochastic transformation	Strictly positive functional preserving	1-norm preserving: $\forall x$, $\|\phi(x)\|_1 = \|x\|_1$	Trace preserving: $\forall S$, $\mathrm{Tr}(\Phi(S)) = \mathrm{Tr}(S)$
	Doubly Stochastic transformation	Strictly positive funct. and uniform event preserving	ϕ, ϕ^* 1-norm preserving: $\phi(\mathbb{1}_S) = \mathbb{1}_T$, $\phi^*(\mathbb{1}_T) = \mathbb{1}_S$	Φ, Φ^* trace preserving: $\Phi(\mathbb{I}_{\mathcal{H}}) = \mathbb{I}_{\mathcal{H}'}$, $\Phi^*(\mathbb{I}_{\mathcal{H}'}) = \mathbb{I}_{\mathcal{H}}$
	Composite system	"Tensor product" $K_1 \hat{\otimes} K_2$	$\mathbb{R}^{S_1}_\geq \otimes \mathbb{R}^{S_2}_\geq \cong \mathbb{R}^{S_0\times S_1}_\geq$	$\mathrm{PSD}^{\mathcal{H}_1} \hat{\otimes} \mathrm{PSD}^{\mathcal{H}_2} := \mathrm{PSD}^{\mathcal{H}_1\otimes\mathcal{H}_2}$
	Composite transformation	Tensor product $F_1 \otimes F_2$	$\phi \otimes \psi$	$\Phi \otimes \Psi$
Deterministic	Configuration space	Extreme rays $\mathbb{P}(K)$	finite set S	$\mathbb{P}(\mathcal{H})$, $\mathcal{H}$ complex Hilbert space
	Transformation	Partial map $\mathbb{P}(K) \to \mathbb{P}(K')$ induced by positive map	Partial map $f : S \to T$	Linear map $A : \mathcal{H} \to \mathcal{H}'$
	Set of transformations	$\mathrm{map}(\mathbb{P}(K), \mathbb{P}(K'))$	$\mathrm{map}_p(S, T)$	$\mathrm{hom}(\mathcal{H}, \mathcal{H}')$
	Information preserving transformation	Injective map $\mathbb{P}(K) \to \mathbb{P}(K')$ induced by positive map	injective map $f : S \to T$	unitary map $U : \mathcal{H} \to \mathcal{H}'$
	Composite system	$\mathbb{P}(K_1 \hat{\otimes} K_2)$	$S_1 \times S_2$	$\mathcal{H}_1 \otimes \mathcal{H}_2$
	Composite transformation	$G_1 \otimes G_2$	$f_1 \times f_2$	$A_1 \otimes A_2$
Non-Deterministic	Configuration space	Face lattice $\mathcal{L}(K)$	Lattice of subsets of S $\mathcal{P}(S) := \{A \mid A \subseteq A\}$	Lattice of linear subspaces of $\mathcal{H}$ $L(\mathcal{H}) := \{U \mid U \leq \mathcal{H}\}$
	Transformation	Faces of $\mathcal{C}$ and induced lattice morphisms $F_* : \mathcal{L}(K) \to \mathcal{L}(K')$	Correspondence $\mathfrak{c} : S \to T$ Formally: $\mathfrak{c} \subseteq T \times S$ $\mathfrak{c}_*(A) = \{t \mid \exists a \in A : (t, a) \in c\}$	"Linear correspondence" $\mathcal{A}$ Formally: $\mathcal{A} \leq \mathrm{hom}(\mathcal{H}, \mathcal{H}')$ $\mathcal{A}_*(U) = \{Au \mid (A, u) \in \mathcal{A} \times U\}$
	Set of transformations	$\mathcal{L}(\mathcal{C})$	$\mathcal{P}(T \times S)$	$L(\mathrm{hom}(\mathcal{H}, \mathcal{H}'))$
	Reverse transformation	Dual face in $\mathcal{C}^*$	$\mathfrak{c}^* \subseteq S \times T$ $\mathfrak{c}^* := \{(s, t) \mid (t, s) \in \mathfrak{c}\}$	$\mathcal{A}^* \leq \mathrm{hom}(\mathcal{H}', \mathcal{H})$ $\mathcal{A}^* := \{A^* \mid A \in \mathcal{A}\}$
	Composition of transformations	"Composition of faces"	$\mathfrak{c}_2 \circ \mathfrak{c}_1 \subseteq S_2 \times S_0$ $\{(s_2, s_0) \mid \exists s_1 \in S_1 : (s_i, s_{i-1}) \in \mathfrak{c}_i\}$	$\mathcal{A}_2 \circ \mathcal{A}_1 \leq \mathrm{hom}(\mathcal{H}_0, \mathcal{H}_2)$ $\{A_2 A_1 \mid A_i \in \mathcal{A}_i\}$
	Composite system	$\mathcal{L}(K_1 \hat{\otimes} K_2)$	$\mathcal{P}(S_1 \times S_2)$	$L(\mathcal{H}_1 \otimes \mathcal{H}_2)$
	Composite transformation	$F_1 \hat{\otimes} F_2$	$\mathfrak{c}_1 \otimes \mathfrak{c}_2 \subseteq (T_1 \times T_2) \times (S_1 \times S_2)$ $\{((t_1, t_2), (s_1, s_2)) \mid (t_i, s_i) \in \mathfrak{c}_i\}$	$\mathcal{A}_1 \otimes \mathcal{A}_2 \leq \mathrm{hom}(\mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{H}_1' \otimes \mathcal{H}_2')$ $\{A_1 \otimes A_2 \mid A_i \in \mathcal{A}_i\}$

Combinatorics of Positive Operators

In general, the face on which a positive map $\alpha : K \to K'$ lies in $\mathrm{hom}(K, K')$, i.e., the combinatorics of ϕ, is determined by how this map sends faces to faces, i.e., by the combinatorial pushforward α_*. This is the map

$$\alpha_* : F \mapsto \bigcap \{G \in \mathcal{L}(K') \mid G \supseteq \alpha(F)\}$$

which sends F to the minimum face containing $\alpha(F)$.
In the particular case of positive maps $\phi : \mathbb{R}^S_\geq \to \mathbb{R}^T_\geq$, the combinatorics of ϕ are determined by the correspondence

$$\mathfrak{c}(\phi) := \{(t, s) \in T \times S \mid e_t^* \phi(e_s) > 0\},$$

also known as the support of ϕ, which is the set of non-zero entries of the matrix representing ϕ.
Interpreting correspondences as edge sets, one gets the following graph-theoretical interpretation:

Correspondence	Graph theory
$\mathfrak{c} : S \to T$	Bipartite graph
$\mathfrak{c} : S \to S$	Digraph
$\mathfrak{c} : S \to S$ such that $\mathfrak{c} = \mathfrak{c}^*$	Graph

This allows to generalize graph theoretical problems to the context of positive operators.

Combinatorics of Completely Positive Operators

Since $\mathrm{hom}_+(\mathrm{PSD}^{\mathcal{H}}, \mathrm{PSD}^{\mathcal{H}'}) \neq \mathrm{hom}(\mathrm{PSD}^{\mathcal{H}}, \mathrm{PSD}^{\mathcal{H}'})$, the combinatorics of a completely positive operator Φ are not determined by its combinatorial pushforward Φ_*.
By the Choi-Hill isomorphism, one can see that they are determined by the subspace of linear maps

$$\mathfrak{c}(\Phi) := \mathrm{im}(\mathrm{Choi}(\Phi))$$

which, when Φ has Kraus representation $(A_1, \dots, A_m)$, satisfies

$$\mathfrak{c}(\Phi) = \mathrm{span}(A_1, \dots, A_m).$$

One can see this as an indication that linear subspaces of matrices are the quantum generalization of graphs.
Is a linear subspace of matrices determined by how it acts on linear subspaces? There are explicit completely positive operators Φ and Ψ such that $\dim \mathfrak{c}(\Phi) > \dim \mathfrak{c}(\Psi)$ but for which $\Phi_* = \Psi_*$.
This answers negatively the question. However, up to now, many results rely on looking at how $\mathcal{A}_*$ looks like. What are the limits of these techniques?

Matching problems and SING

Using our graph theoretical interpretation, a perfect matching of a correspondence $\mathfrak{c} : S \to T$ is a bijective function $\mathfrak{m} : S \to T$ such that $\mathfrak{m} \subseteq \mathfrak{c}$.
How does this generalize? In the continuous setting, a bijective function becomes an invertible linear map. Therefore a *continuous perfect matching* of $\mathcal{A} \leq \mathrm{hom}(\mathcal{H}, \mathcal{H}')$ is an invertible linear map $A \in \mathcal{A}$.
In other words, the perfect matching inexistence problem in the context of completely positive operators becomes equivalent to **SING**.
Hall blocks. (Ivanyos, Qiao, Subrahmanyam; 2016) and (Garg, Gurvits, Oliveira, Widgerson; 2016) showed that this obstruction to perfect matching existence can be generalized to completely positive operators, but it only solves a non-commutative weaker version of **SING**.
Question: The above techniques are based on properties of the combinatorial pushforward. Are these enough to solve **SING**? More concretely, are there completely positive operators Φ and Ψ such that $\Phi_* = \Psi_*$ but such that $\mathfrak{c}(\Phi)$ contains an invertible map, but $\mathfrak{c}(\Psi)$ doesn't?

Based on the Master's thesis *On the Complexity of some Null-Cone Membership Problems* of Josué Tonelli-Cueto. This thesis was written at the Berlin Mathematical School and the Technische Universität Berlin under the supervision of Peter Bürgisser. During this period, the author was supported by an scholarship awarded by the *Obra Social "la Caixa"* and the *Deutscher Akademischer Austauschdienst (DAAD)*. This scholarship was part of the program *Becas de Posgrado en Europa*, call of 2014, created by the *Obra Social "la Caixa"*.