Quantum complexity theory meets TFNP: Product Quantum Satisfiability on qudits

Marco Aldi* Sevag Gharibian† Dorian Rudolph†

*Department of Mathematics and Applied Mathematics, Virginia Commonwealth University

†Department of Computer Science and Institute for Photonic Quantum Systems (PhoQS), Paderborn University

Introduction

How to characterize the complexity of a problem with a guaranteed, but hard to find, solution?

TFNP is the class of NP *search* problems with a *guaranteed* witness [MP91].

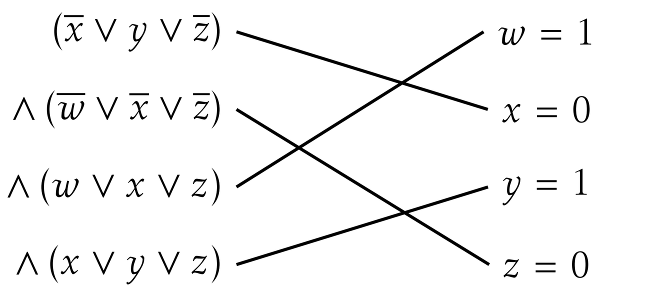
- There exists a solution, it can be efficiently verified, but we don't necessarily know how to efficiently compute it!
- PPAD ⊆ TFNP [JPY88; Pap94]: Given succinct description of exp-large graph G with deg ≤ 2, node u with $\deg(u) = 1$, find $v \neq u$ with $\deg(v) = 1$ (End-Of-The-Line Problem).
  Complete problems: approximate Brouwer fixed point [Pap94], Nash equilibrium [DGP06; CDT09]

Quantum: Surprisingly, TFNP rears its head again:

Definition (Quantum k-SAT). Given set of k-local rank-1 projectors $\Pi = \{\Pi_i\} \subseteq \mathbb{C}^{2^n \times 2^n}$ on n qubits, decide whether the Π_i have a common nullspace.

- 3-QSAT is QMA_1-complete [GN13].

However, something unexpected happens for the "easy" case of 3-SAT with a *System of Distinct Representatives (SDR)* (i.e. matching between clauses and variables).

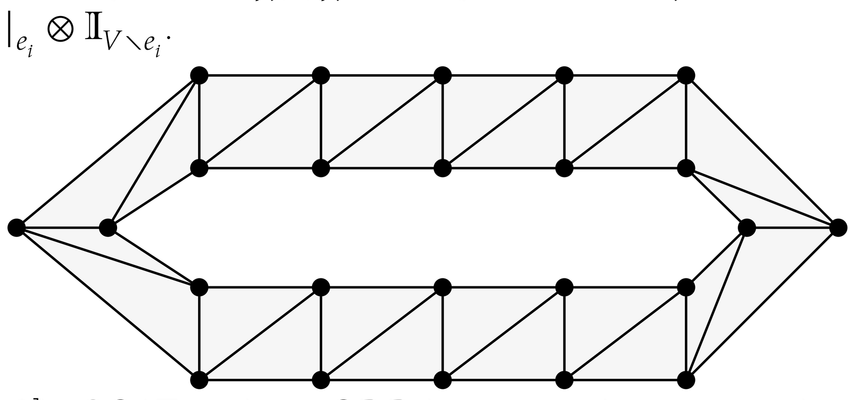


⇒ Trivial: just set each representative to satisfy its clause.

QSAT with SDR is much harder! Model QSAT as hypergraph $G = (V, E)$ with n qubits V:

- Clauses are rank-1 projectors $|\phi_i\rangle\langle\phi_i|$ acting on qubits $e_i \subseteq V$.
- $H = \sum_{i=1}^m |\phi_i\rangle\langle\phi_i|_{e_i} \otimes \mathbb{I}_{V \setminus e_i}$.

Example: "Full cycle", each face represents a 3-local projector.



Theorem ([LLMSS10]). QSAT with an SDR has a *product state* solution $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle \in \mathbb{C}^{2^n}$.

⇒ PRODSAT with SDR is in TFNP.

- There exists a parameterized algorithm to solve a special class of QSAT with SDR efficiently [ABGS21] (requires *generic** instances).
- Finding *real-valued* PRODSAT solution is NP-hard [Goe19].

**Generic* means constraints which are not "edge cases", e.g., chosen uniformly at random.

Where does PRODSAT lie in the TFNP hierarchy?

Results

*1. Product state solutions for **qudit systems**.*

Definition (Weighted SDR). Let $G = (V, E)$ and $w : V \to \mathbb{Z}_{\geq 0}$ be a *weighted hypergraph*. A WSDR is an assignment $f : E \to V$ with $f(e) \in e$ and $|f^{-1}(v)| \leq w(v)$ for all $e \in E, v \in V$.
For QSAT on *qudits*, set $w(v_i) := d_i - 1$, where d_i is the dimension of the i-th qudit.

- *Note:* If $\forall v \in V : w(v) = 1$, then WSDR is equivalent to SDR.
- Each qu-d-it can be assigned to $d - 1$ edges.

Theorem. Let Π be a QSAT-instance on qudits of dimensions $d_1, \ldots, d_n$.
- If (G, w) has a WSDR, then Π has a product solution.
- If (G, w) does not have a WSDR, and Π is *generic**, then Π has *no* product solution.

- Generalization of [LLMSS10] from qubits to qudits.

Two independent proofs:
- Using algebraic geometry (*Chow ring*).
- Reduction from qudits to qubits, plugging into [LLMSS10].

Demonstrating the power of WSDRs, we recover result of [Par04]:

Corollary ([Par04]). Let $V \subseteq \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$ be a completely entangled subspace (contains no product states). Then $\dim(V) \leq \prod_{i=1}^k d_i - \sum_{i=1}^k d_i + k - 1$, where $d_i = \dim(\mathcal{H}_i)$.

2. Completeness for a new subclass of TFNP.

- Define MHS ⊆ TFNP as set of relations poly-time reducible to computing ϵ-approximate solutions to systems of multihomogeneous equations, with a solution guaranteed by Bézout's theorem.
- First "quantum-inspired" subclass of TFNP.

Theorem. Computing an ϵ-approximate product state solution to k-QSAT with SDR is MHS-complete.

- Evidence that QSAT with SDR is intractable, even finding roots of homogeneous systems remains an open problem [Gre14].
- We can embed *sparse univariate polynomials* into QSAT with SDR.

NP-hard to decide whether 3-QSAT with SDR has prod. solution
- with $|x| = |y|$, where x, y are entries of a given qubit.
- with one additional constraint (cf. [Goe19]).

3. Efficiently solving special cases of QSAT with WSDR.

We extend the parameterized algorithm of [ABGS21] to apply even to *non-generic* QSAT-instances.

Theorem. Let Π be a k-QSAT instance of qubits whose hypergraph has an *almost extending edge order* of radius r. Compute ϵ-approximate solution in time $\mathrm{poly}(L, \log \epsilon^{-1}, k^r)$ for input size L.

- *almost extending edge order*: Ordering of the edges so that all but one add a new vertex.

Algorithm: Suppose each edge adds 1 vertex, then *transfer functions* set all qubits. Remove *redundant* vertices. Single *non-extending* edge induces polynomial constraint (degree $2^{O(r)}$). *Non-generic* instances can "zero" transfer functions ⇒ restart.

Finally, we sketch how to extend [ABGS21] to qudits with WSDR:

- Construct (artificial) non-trivial family: *Pinwheel graphs*
- Find product solutions efficiently (brute force would take exp-time).

WSDR

Lemma ((Weighted) Hall's Marriage Theorem). Let (G, w) be a weighted hypergraph. (G, w) has a WSDR iff $|V_X|_w \geq |X|$ for all $X \subseteq E(G)$, where $|V_X|_w = \sum_{v \in e \in X} w(v)$.

Corollary. (G, w) has an SDR if $\deg(v) \leq |e|_w$ for all e, v.

Note: Product solutions are points in complex projective variety

$$\mathcal{X}_{d_1,\ldots,d_n} = \mathbb{P}^{d_1-1}(\mathbb{C}) \times \cdots \times \mathbb{P}^{d_n-1}(\mathbb{C}),$$

- Each clause Π_i defines hypersurface $V_i \subseteq \mathcal{X}_{d_1,\ldots,d_n}$ of degree 1 in e_i and degree 0 in $V \setminus e_i$.
- Count points in intersection $V_1 \cap \cdots \cap V_n$ with algebraic geometry:

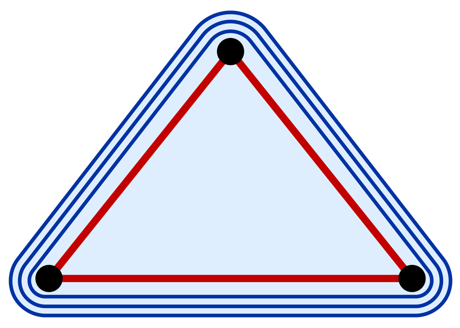
Definition (Chow ring).
$CH(\mathcal{X}_{d_1,\ldots,d_n}) = \mathbb{Z}[H_1, \ldots, H_n]/(H_1^{d_1}, \ldots, H_n^{d_n})$.

- Example: $CH(\mathcal{X}_{2,2}) = \mathbb{Z}[H_1, H_2]/(H_1^2, H_2^2)$ with $(a + bH_1 + cH_1H_2) \cdot (d + eH_2) = ad + aeH_2 + bdH_1 + (be + cd)H_1H_2$
- Subvariety representative for $V \subseteq \mathcal{X}_{d_1,\ldots,d_n}$: $[V] := \delta_1 H_1 + \cdots + \delta_n H_n$, where δ_i degree in the homogeneous coordinates of $\mathbb{P}^{d_i-1}(\mathbb{C})$.

Fact (Bézout number). Let $V_1, \ldots, V_r \subseteq \mathcal{X}_{d_1,\ldots,d_n}$ be hypersurfaces.
- If $[V_1] \cdots [V_r] \neq 0$, then $V_1 \cap \cdots \cap V_r \neq \emptyset$.
- If $[V_1] \cdots [V_r] = 0$, then $W_1 \cap \cdots \cap W_r = \emptyset$ for *almost all* hypersurfaces W_i with $[W_i] = [V_i]$.
- If $[V_1] \cdots [V_r] = mH_1^{d_1-1} \cdots H_n^{d_n-1}$, then the generic intersection $W_1 \cap \cdots \cap W_n$ consists of m points (Bézout number).

- For QSAT instance on (G, w), we get $[V_i] = \sum_{j \in e_i} H_j$.
- Intersection of all constraints: $\prod_i [V_i] = \sum_{j_1 \in e_1, \ldots, j_m \in e_m} H_{j_1} \ldots H_{j_m}$
- $H_{j_1} \cdots H_{j_m} \neq 0$ iff each H_j appears at most $d_j - 1$ times ⇔ WSDR.

Example: 3 qutrits, 6 edges
$e_1 = \{1, 2\}, e_2 = \{2, 3\}$,
$e_3 = \{3, 1\}$ (red),
$e_4 = e_5 = e_6 = \{1, 2, 3\}$ (blue).



- Image of intersection in chow ring: ⇒ 30 generic solutions
$(H_1 + H_2)(H_2 + H_3)(H_3 + H_1)(H_1 + H_2 + H_3)^3 = 30 \cdot H_1^2 H_2^2 H_3^2$

Reduction from qudits to qubits: (qu-$(d+1)$-it) ↦ (qubit and qu-d-it)

Theorem. Let Π be a QSAT instance on $\mathcal{H} = \mathbb{C}^{d+1} \bigotimes_{i=2}^n \mathbb{C}^{d_i}$ with a WSDR. We can efficiently compute
- Π' on $\mathcal{H}' = \mathbb{C}^2 \otimes \mathbb{C}^d \bigotimes_{i=2}^n \mathbb{C}^{d_i}$ with WSDR,
- mapping of product solutions between Π' and Π.

- Replace first qu-$(d+1)$-it z of Π with qubit x and qu-d-it y.
- Let $f : \mathbb{P}^1 \times \mathbb{P}^{d-1} \to \mathbb{P}^d$ be bilinear.
- f is surjective and well defined: $\forall (x, y) \in \mathbb{P}^1 \times \mathbb{P}^{d-1} : f(x, y) \neq 0$
- Computing $f^{-1}(z)$ reduces to finding roots of degree d polynomial.

$$f(x, y) := \begin{pmatrix} x_1 y_1 \\ x_2 y_d \\ x_1 y_2 - x_2 y_1 \\ x_1 y_3 - x_2 y_2 \\ \vdots \\ x_1 y_d - x_2 y_{d-1} \end{pmatrix}$$

Constructing Π': Let $\Pi_i = |\phi\rangle\langle\phi|$ on $e_i = \{z, v_2, \ldots, v_k\}$.

- $p(z, v_2, \ldots, v_k) = \langle \phi | z, v_2, \ldots, v_k \rangle$ is a homogeneous polynomial in the coefficients of the qudits.
- Replace z_j in p with $f(x, y)_j$ to obtain $p'(x, y, v_2 \ldots, v_k) = \langle \phi' | x, y, v_2, \ldots, v_k \rangle$.

Going from $\Pi \to \Pi' \to \Pi'' \to \cdots \to \Pi^*$, we eventually construct a QSAT instance on qubits with SDR.

- *Note:* each step increases number of product solutions by factor d.

Embedding Sparse Polynomials

Transfer functions [ABGS21] give a necessary and sufficient condition for a rank-1 k-local clause $|\phi\rangle$ to be satisfied, given a partial assignment $|\psi_1, \ldots, \psi_{k-1}\rangle$ to first $k - 1$ qubits.

Lemma (Transfer function). There exists a multilinear polynomial $g : (\mathbb{C}^2)^{k-1} \to \mathbb{C}^2$ such that any partial assignment $v_1, \ldots, v_{k-1}$ satisfies clause $|\phi\rangle$ iff $|v_k\rangle \propto g(v_1, \ldots, v_{k-1})$ or $g(v_1, \ldots, v_{k-1}) = 0$.

- For $k = 2$, $|\phi\rangle = |01\rangle - |10\rangle$ sets $g(x) = x$ ⇒ enforce equality.
- For $k = 3$, we can set $g(x, y) = \sum_{i,j \in [2]} \begin{bmatrix} a_{ij} x_i y_j \\ b_{ij} x_i y_j \end{bmatrix}$ for any a_{ij}, b_{ij}.

Embedding a polynomial: Let $p(x) = \sum_{i=0}^n c_i x^i$.

- Homogenize $p(x, y) = \sum_{i=0}^n c_i x^i y^{n-i}$
- First qubit $v_0 = (x, y)^T$. Use 2-local constraint to enforce $v_1 = v_0$.
- Use 3-local constraints to construct $v_i = (x^i, y^i)^T$.
- Factor $p(x, y) = x^j \underbrace{\sum_{i=j} c_i x^{i-j} y^{n-i}}_{q(x,y)} + c_0 y^j y^{n-j}$ with $c_0, c_j \neq 0$.

- Recursively construct $v = (q(x, y), y^{n-j})$ with 3-local constraints.
  – Important for intermediate terms: $v \neq 0$ for all $(x, y) \neq 0$.
- Final qubit: $\begin{bmatrix} p(x, y) \\ y^n \end{bmatrix} \propto \begin{bmatrix} y^n \\ p(x, y) \end{bmatrix} \Rightarrow \frac{p(x, y)}{y^n} = p\left(\frac{x}{y}\right) = 1$.
- *Sparse polynomials:* Construct (x^i, y^i) in $O(\log(i))$ steps using square-and-multiply.

Multihomogeneous Systems

Definition ([MS87]). f is *multihomogeneous* if there are m sets of variables $Z_j = \{z_{0,j}, \ldots, z_{n_j,j}\}$ and $d_1, \ldots, d_m \in \mathbb{Z}_{\geq 0}$ such that f is homogeneous in Z_j of degree d_j.

- Example: $f = x_0 y_0 y_1 + x_1 y_1 y_2$ with $Z_1 = \{x_0, x_1\}, Z_2 = \{y_0, y_1, y_2\}$
- Homogeneous of degree $d_1 = 1, d_2 = 2$ in each group.

Theorem (Bézout [MS87; Sha74]). Let $F = \{f_1, \ldots, f_n\}$ be a system of $n = n_1 + \cdots + n_m$ multihom. polynomials with f_j of degree $d_{j,k}$ in Z_k. Let $d_{Béz}$ be the coefficient of $\alpha_1^{n_1} \cdots \alpha_m^{n_m}$ in $\prod_{k=1}^n \sum_{j=1}^m d_{j,k} \alpha_j$, where α_j are symbolic variables representing Z_j.
⇒ $F(Z)$ has $d_{Béz}$ solutions if not infinite, counting multiplicities.

Ex.: $F = \{f_1, f_2, f_3\}, n_1 = 1, n_2 = 2, Z_1 = \{x_0, x_1\}, Z_2 = \{y_0, y_1, y_2\}$

$f_1 = x_0 y_0 y_1 + x_1 y_1 y_2$		$d_{1,1} = 1$	$d_{2,1} = 2$
$f_2 = x_0 y_0 + x_1 y_1$		$d_{1,2} = 1$	$d_{2,2} = 1$
$f_3 = y_0 y_1 + y_1 y_2$		$d_{1,3} = 0$	$d_{2,3} = 2$

- $d_{Béz} = 3$ as $(\alpha_1 + 2\alpha_2)(\alpha_1 + \alpha_2)(\alpha_2) = \alpha_1^2 + 3\alpha_1\alpha_2^2 + 2\alpha_2^3$.

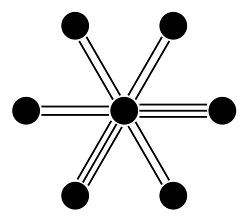
Definition (Multi-Homogeneous Systems). MHS ⊆ TFNP is the set of relations poly-time reducible to finding an ϵ-approximate solution to multihomogeneous systems with $d_{Béz} > 0$, $O(1)$ group size and $O(1)$ total degree in each polynomial.

1. Represent variable group Z_j with qu-$(n_j + 1)$-it.
2. Create copies of groups with degree > 1.
3. Add 1-local projector for each polynomial constraint.
4. Reduction to qubits (efficient due to $O(1)$ degree).
5. Enforce equality of copies with 2-local constraints.

Theorem. $O(1)$-approximate PRODSAT on $O(1)$-local qubit systems with SDR is MHS-complete.

[SS18] can find *non-singular solutions* in time polynomial in the number WSDRs after removing one edge (generally > exp · #WSDRs).

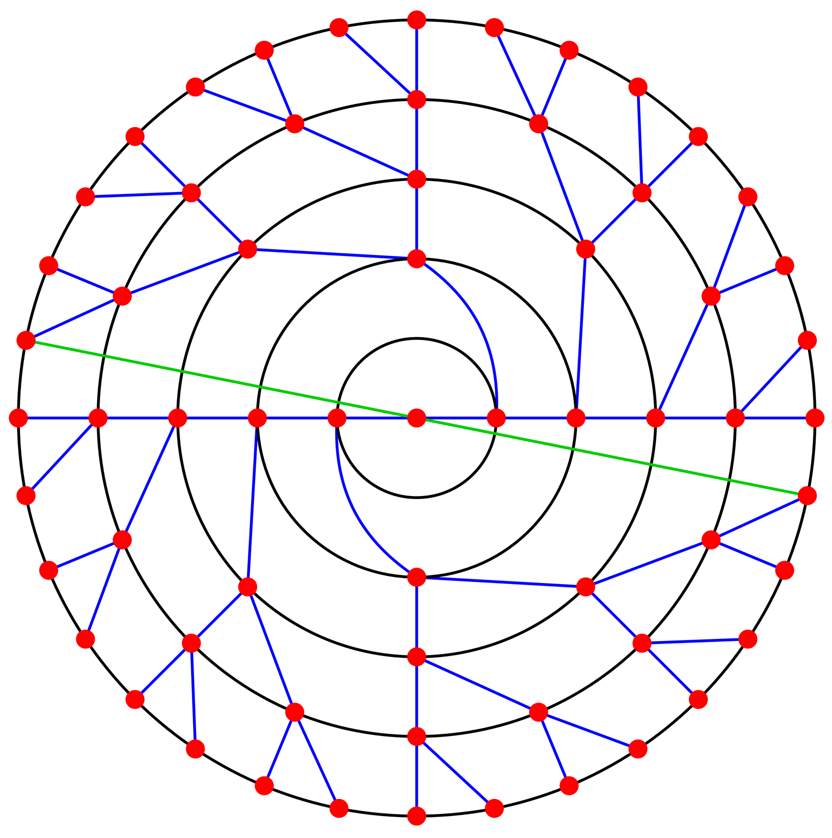
- Star of $n+1$ qu-d-its (here $n = 6, d = 3$). For fixed d, #WSDR = poly(n), even after removing an edge.



Pinwheel Graph

Infinite family of efficiently solvable 2-QSAT instances on qutrits:

- Γ_n: Binary tree of height n (blue) with circularly connected layers (black), and two edges from root to leaf (green).



- WSDR: assign green edges to center, black to left, blue to child.

Solution: Arbitrary assignment $v_0 = (x, y, z)$ (dehomogenize $z = 1$).

- This imposes rank-1 constraints on first ring v_1, v_2 (dep. on v_0) ⇒ eff. reduces dim. of qutrits to 2
- Replace qutrits with qubits, solve ring of qubits as linear system. ⇒ qubits are polynomials in x, y.
- Reduce second ring to qubits with blue edges. Iterate until all rings are reduced to qubits and assigned to polynomials in x, y.
- Finally, green edges induce system of two bivariate polynomials of degree $2^{O(n)}$. Solve using resultant.

Outlook

We have a a quantum problem that guarantees "simple/classical" solution, but is also likely intractable.
⇒ Either QSAT with WSDR *can* be solved efficiently, or MHS-completeness is a strong indicator for intractability.

- Are there more complete problems for MHS?
- Where does MHS lie in the TFNP hierarchy?
- Is there an FPT for QSAT with WSDR?

References

[ABGS21] M. Aldi, N. de Beaudrap, S. Gharibian, and S. Saeedi. In: *Commun. Math. Phys.* 381.1 (Jan. 2021), pp. 209–256.
[CDT09] X. Chen, X. Deng, and S.-H. Teng. In: *J. ACM* 56.3 (2009), 14:1–14:57.
[DGP06] C. Daskalakis, P. W. Goldberg, and C. H. Papadimitriou. In: *Thirty-Eighth Annual ACM Symposium on Theory of Computing*. 2006, pp. 71–78.
[GN13] D. Gosset and D. Nagaj. In: *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. 2013, pp. 756–765.
[Goe19] A. Goerdt. In: *Computer Science – Theory and Applications*. 2019, pp. 156–167.
[Gre14] B. Grenet. Talk at *XXVth Rencontres Arithmétiques de Caen*. 2014.
[JPY88] D. S. Johnson, C. H. Papadimitriou, and M. Yannakakis. In: *J. Comput. Syst. Sci.* 37.1 (1988), pp. 79–100.
[LLMSS10] C. R. Laumann, A. M. Läuchli, R. Moessner, A. Scardicchio, and S. L. Sondhi. In: *Phys. Rev. A* 81.6 (2010), p. 062345.
[MP91] N. Megiddo and C. H. Papadimitriou. In: *Theor. Comput. Sci.* 81.2 (1991), pp. 317–324.
[MS87] A. Morgan and A. Sommese. In: *Appl. Math. Comput.* 24.2 (1987), pp. 101–113.
[Pap94] C. H. Papadimitriou. In: *J. Comput. Syst. Sci.* 48.3 (1994), pp. 498–532.
[Par04] K. R. Parthasarathy. In: *Proc. Math. Sci.* 114.4 (Nov. 2004), pp. 365–374.
[Sha74] I. R. Shafarevich. 1974.
[SS18] M. Safey El Din and É. Schost. In: *J. Symb. Comput.* 87 (2018), pp. 176–206.