The Permutations Paper for non Algebraic Speakers.

David Ponarovsky

May 21, 2023

Abstract

A guide for reading Becker, Lubotzky, and Mosheiff's paper for computer scientists. The goal is to help the reader by providing analogs and examples from the combinatorics field.

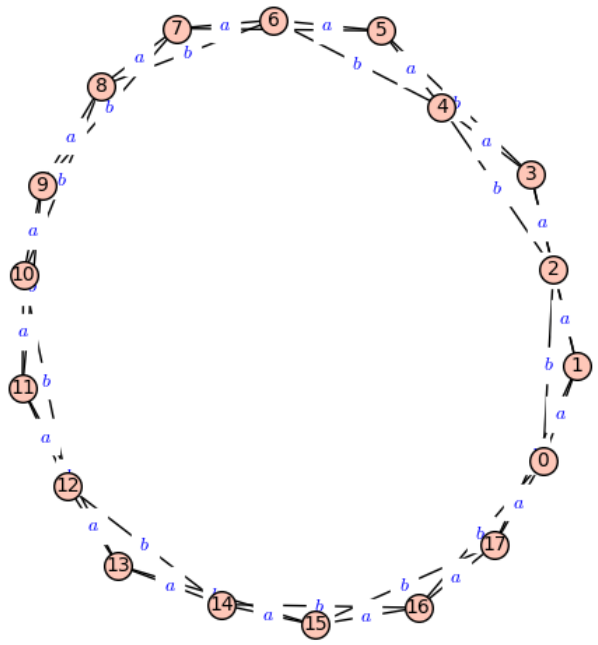
1 Motivation (Use Cases List).

We start by presenting several use cases that may be of interest to computer scientists.

1. Testing candidates for LTC/QLDPC codes. One of the resources needed for the available constructions is a square complex in which the encoding associates each bit with a face. We can obtain these structures by taking the Left-Right Cayley graph generated by a pair of generator sets A, B, such that $[A, B] = 0$.

2. Testing if a set of stabilizers forms a stabilizer code. Here the stabilizers are subsets of the Pauli group and they form a code only if they all commute.

3. Classical toy-version of QMA complete problem. It's known that decide if two quantum circuits over n qubits are $1/poly$-equivalent is QMA-complete problem. So, One question that could be interesting is to ask given prem' $P = \prod p_i$ and $Q = \prod q_i$ such that p_i (q_i) act over a constant size of bits (assuming binary encoding), then ask whether $P = Q$.



We think about the testability of hardness as a property of the equations, not the permutations. To motivate this, we can consider the implementation of memory, with the motion of each particle governed by the configuration of the system, which are our encoded codewords.

One illustrate is the commuting equation, in which we ask to decide if two given permutations X, Y are commute or not. It's know that this relation is stable, meaning that if they almost commute then they are close to groups which are completely commute. An example for relation which is not stable is $Y^2X = XY^2$. In general it is an open question whether exist $m \neq n$ such that $Y^m X = XY^n$.

Fact 1. *Locally testable preserved under isomorphism over* ***finite*** *groups.*

- $\Rightarrow$ *Abelian group are locally testable.*
-

2 Example.

Let us define the permutations f, g over $n = 2m$ elements defined as follow:

$$f(i) = \begin{cases} i+1 & i < m \\ i-1 & i \geq m \end{cases}$$

$$g(i) = \overbrace{n-i}^{\text{reflection}} +1$$

3 The S-graph.

Theorem 1. *Denote by $FGSol_E$ union over the finite connected entities of GSol, and by α the asymptotic (ifimum) Cheeger constant of them. If the α is positive, then E is not testable.*

4 Not Locally Testable.

Abels's group is solvable, residually finite, but not locally testable.

$$G = diag(1, p^m, p^n, 1) + \text{ upper}$$

5 Defs.

Definition 1. *The uniform local defect of $f : \Gamma \to Sym(n)$ is*

$$def_\infty(f) = \sup_{\gamma_1,\gamma_2 \in \Gamma} \left\{ d^H\left(f(\gamma_1\gamma_2)\right), f(\gamma_1) f(\gamma_2) \right\}$$

The uniform distance between $f, g : \Gamma \to Sym(n)$ is

$$d_\infty(f,h) = \sup_{\gamma \in \Gamma} \{ d^H(f(\gamma), h(\gamma)) \}$$

Definition 2. *For $\sigma, \tau \in Sym(n), Sym(N), n \leq N$*

$$d^H(\sigma,\tau) = d^H(\tau,\sigma)$$
$$= \frac{1}{N}\left(|\{x \in [n] | \sigma(x) \neq \tau(x)\}| + N - n \right)$$

d^H is a metric on $\bigcup_{n\in\mathbb{N}} Sym(n)$ and the idea is to punish permutations that use much more space then σ.

6 Facts.

Fact 2. *Amenable + Locally testable $\Rightarrow$ Every finitely generated normal subgroup is closed.*

Fact 3. *The discrete Heisenberg group $H_3(\mathbb{Z}) = \langle x, y, z | [x,z] = [y,z] = 1, [x,y] = z \rangle$ is locally testable.*

Fact 4. *the Bamuslag-Solitar BS(1,2) $= \langle x, y | yx = x^2 y \rangle$ is locally testable.*

Fact 5. *Infinite + Sofic + Property(T) $\Rightarrow$ not locally testable.*

Fact 6. *(Kazhdan 82) Let H be an Hilbert space and $f : \Gamma \to U(H)$ such that:*

$$\sup_{\gamma_1,\gamma_2 \in \Gamma} |f(\gamma_1\gamma_2) - f(\gamma_1) f(\gamma_2)|_{op} \leq \delta$$

then there is representation $h : \Gamma \to U(H)$ such that $\sup_{\gamma\in\Gamma} |h(\gamma) - f(\gamma)|_{op} \leq 2\delta$ In other words, any function which approximate a distance between groups elements is close to homomorphism.

Fact 7. *If Γ is finite and $f : \Gamma \to Sym(n)$ then there is a homomorphism $h : \Gamma \to Sym(n)$ such that:*

$$d_\infty(h,f) \leq C def_\infty(f)$$

where C depends only on Γ (and not on n)

Definition 3. *If Γ acts transitively on $[n]$ then there is $f : Sym(n-1)$ such that:*

$$def_\infty(f) \leq \frac{2}{n-1}$$

but

$$d_\infty(h,f) \geq \frac{1}{2} - \frac{1}{n-1}$$

for every homomorphism $h \to Sym(n-1)$

Fact 8. *If Γ is amenable $f:\Gamma\to U(n),\delta>0$ and*

$$|f(\gamma_1\gamma_2)-f(\gamma_1)f(\gamma_2)|_h\leq\delta\quad\forall\gamma_1\gamma_2\in\Gamma$$

then there is a representation $h:\Gamma\to U(N)$and an isometry $T:\mathbb{C}^n\to U(N)$ such that:

$$|h(\gamma)-T^{\dagger}f(\gamma)T|_h\leq 211\delta\quad\forall\gamma\in\Gamma$$

and $n\leq N\leq\left(1+2500\delta^2\right)n$. Here $|A|_h=\left(\frac{1}{n}tr(A^{\dagger}A)\right)^{\frac{1}{2}}$

Fact 9. *For amenable Γ and function $f:\Gamma\to Sym(N)$ such that:*

$$d_{\infty}(h,f)\leq\varepsilon\quad and\ n\leq\leq(1+\varepsilon)n$$

where $\varepsilon\leq 2039\cdot def_{\infty}(f)$

Fact 10. *Let $f:SL_r(\mathbb{Z})\to Sym(n),r\geq 3$ Then there is a homomorphism $h:SL_r(\mathbb{Z})\to Sym(N)$ such that:*

$$d_{\infty}(h,f)\leq Cdef_{\infty}(f)$$
$$andn\leq N\leq(1+Cdef_{\infty}(f))n$$

7 Randomized Banchmark.

Definition 4 (unitary t-design.)**.** *A set of unitray operations on $\mathbb{C}^D$ such that , for every polynomail $P_{(t,t)}(U)$ of degree at most t in the matrix elements of U and at most t in the complex conjugates of those matrix elements we have:*

$$\frac{1}{K}\sum_{k=1}^{K}P_{(t,t)}(U_k)=\int_{U(D)}dUP_{(t,t)}(U)$$

where the integral is respect to the unitarily invariant Haar measure. Example for $P_{(1,0)}:U,P_{(2,2)}:U_kU_jU_k^{\dagger}U_j^{\dagger}$

Definition 5. *The super operator $\mathbb{E}_{\mu}(\Lambda)$ define to be:*

$$\mathbb{E}_{\mu}(\Lambda):\rho\mapsto\int_{U(D)}d\mu(U)U^{\dagger}\Lambda\left(U\rho U^{dagger}\right)U$$

Fact 11. *A unitary 2 - design has the property that sampling uniformly form $\{U_1..U_K\}$ is operationally equivalent to sampling from the Haar measure. Namely $\mathbb{E}_{\mu}(\Lambda)=\mathbb{E}_{Harr}(\Lambda)$.*

Fact 12. *The uniform distribution over the Clifoerd group on n qubits is a unitary 2-design with $D=2^n$.*

Fact 13. *An ε-approximate unitary 2-design can be explicitly constructed in terms of circuits that are in-place, of size $O\left(n\log\frac{1}{\varepsilon}\right)$ and of depth $O(\log n\log\frac{1}{\varepsilon})$. (probabilistic construction).* ***[COMMENT]*** *gentle point.*

Fact 14. *The average fidelity of a quantum channel Λ acting on n qubits, can be estimated to within $\delta>0$ with error probability $\varepsilon>0$ at a cost of $O(\log\frac{1}{\varepsilon})$ evaluations of the channel conjugated by in-place circuits of size $O\left(n\log\frac{1}{\varepsilon}\right)$ and depth $O\left(\log n\log\frac{1}{\varepsilon}\right)$.*

Question. *Assume that we have a big quantum computer that works, and suppose that we wish to find other 2-approximate- design. Is the design equation stable?*