Quantum Circuit Polynomials In Search of Invariants and Physical Meaning

Open problem session, OCIT workshop 2018, Princeton IAS

Kenneth W. Regan[1]
University at Buffalo (SUNY)

8 June, 2018

[1] Joint with Amlan Chakrabarti, U. Calcutta, and Chaowen Guan, UB.

More-general forms of a known relation

- Assume all nonzero entries $re^{i\theta}$ of gate matrices in quantum circuits C have equal magnitude $|r|$ and θ an integer multiple of $2\pi/K$.
- Suppose C has h nondeterministic gates H, $\mathsf{X}^{1/2}$, and/or $\mathsf{Y}^{1/2}$.
- Let G be a field or ring such that G^* embeds the K-th roots of unity ω^j by a multiplicative homomorphism $\iota(\omega^j)$.

Theorem (multiplicative form, case $G = \mathbb{F}_2$ is Dawson et al. (2004) + ...)

Any QC C of n qubits can be quickly transformed into a polynomial P_C of the form $\prod_g P_g$ and a constant $R > 0$ such that for all $x, z \in \{0,1\}^n$:

$$\langle z \mid C \mid x \rangle = \frac{1}{R} \sum_{j=0}^{K-1} \omega^j (\# y : P_C(x,y,z) = \iota(\omega^j)) = \frac{1}{R} \sum_y P_C(x,y,z).$$

Here g ranges over all gates and outputs of C and y ranges over $\{0,1\}^h$.

Degree is $\Theta(s)$ where s is the number of gates in C.

Additive Case

Theorem (RCG (2017), RC (2007-9), cf. Bacon-van Dam-Russell (2008))

Given C and K, we can efficiently compute a polynomial $Q_C(x_1, \ldots, x_n, y_1, \ldots, y_h, z_1, \ldots, z_n, w_1, \ldots, w_t)$ of degree $O(1)$ over $\mathbb{Z}_K$ and a constant R' such that for all $x, z \in \{0,1\}^n$:

$$\langle z \mid C \mid x \rangle = \frac{1}{R'} \sum_{j=0}^{K-1} \omega^j (\#y, w : Q_C(x, y, z, w) = j) = \frac{1}{R'} \sum_{y,w} \omega^{Q_C(x,y,z,w)},$$

where Q_C has the form $\sum_{gates\ g} q_g + \sum_{constraints\ c} q_c$.

- Gives a particularly efficient reduction from BQP to #P.
- In P_C, illegal paths that violate some constraint incur the value 0.
- In Q_C, any violation creates an additive term $T = w_1 \cdots w_{\log_2 K}$ using fresh variables whose assignments give all values in 0 .. $K-1$, which *cancel*. (This trick is my main truly original contribution.)

Constructing the Polynomials

- Initially $P_C = 1$, $Q_C = 0$.
- For Hadamard on line i (u_i—H–), allocate new variable y_j and do:

$$\begin{aligned} P_C \quad &*= \quad (1 - u_i y_j) \\ Q_C \quad &+= \quad 2^{k-1} u_i y_j. \end{aligned}$$

- CNOT with incoming terms u_i on control, u_j on target: u_i stays, $u_j := 2u_i u_j - u_i - u_j$. No change to P_C or Q_C.
- In characteristic 2, linearity is preserved.
- TOF: controls u_i, u_j stay, target u_k changes to $2u_i u_j u_k -$ $u_i u_j$ $-u_k$.
- Linearity not preserved. Similar considerations in [BvDR08].
- Phase and Twist gates change both P_C and Q_C with terms that use higher K... Details in [RCG17], also earlier draft linked from 2012 post "Grilling Quantum Circuits" on the *Gödel's Lost Letter* blog.

The Polynomials Are Natural — An Example

- The expression for $\langle z \mid C \mid x \rangle$ is the *partition function* of the circuit.
- For Clifford C, Q_C is quadratic over $\mathbb{Z}_4$ and every term has form

$$x^2 \qquad \text{or} \qquad 2xy.$$

So Q_C is **invariant** under $x \mapsto x + 2$ and there is a fixed 1-to-2^m correspondence between solutions over $\mathbb{Z}_4$ and solutions over $\{0, 1\}$. Hence "yet another" Gottesman-Knill proof follows from:

Theorem (Cai-Chen-Lipton-Lu 2010, cf. Ehrenfeucht-Karpinski (+ ...))

For quadratic $p(x_1, \ldots, x_m)$ over $\mathbb{Z}_K$, and all $a < K$, the function $N_a(p) = \#(x \in \mathbb{Z}_K^m) : p(x) = a$ is computable in $\mathsf{poly}(mK)$ time.

- Also noted by Cai-Guo-Williams (2017).
- Open: replace K by $\log K$ in the time?

A Sharp 'Dichotomy' Phenomenon / What Else?

- Adding the controlled-phase gate CS makes a universal set.
- Then Q_C is *still quadratic over* $\mathbb{Z}_4$ but now has terms of the form

$$xy,$$

  which are not invariant under $x \mapsto x + 2$. So the correspondence between $\{0,1\}^m$ and $\mathbb{Z}_4^m$ breaks down.
- A nicely sharp example of the P vs. #P *dichotomy* phenomenon.
- So the polynomials are natural and "have bite." Thus reasonable to ask:

What else are the polynomials P_C and Q_C expressing about C?

- In particular, can they supplement the simple gate count s regarding the "effort" needed to operate C, and/or help to measure the "entangling capacity" $e(C)$?

Analogies, Ideas and Open Questions

- Invariants based on Strassen's *geometric degree* $\gamma(f)$ concept?
- Baur-Strassen showed that $\Omega(\log_2 \gamma(f))$ lower-bounds the arithmetical complexity of f, indeed the number of binary multiplication gates. Apply similar to quantum circuits?
- Already hard to formulate n-partite entanglement of (pure or mixed) *states*. How to define for *circuits*? Plausible axioms:

$$\begin{aligned} e(C^*) &= e(C), \\ e(C_1 \otimes C_2) &= e(C_1) + e(C_2), \\ e(C; \mathit{measure}) &\leq e(C), \\ e(C + \mathrm{LOCC}) &=? \; e(C) \\ C \equiv C' &\implies ?? \; e(C) = e(C')? \end{aligned}$$

- Are there natural candidates for $e(C)$ in terms of geometric properties of varieties associated to P_C and/or Q_C?
- Study actions that leave P_C or Q_C invariant (modulo some $\equiv$).