Analyzing Quantum Circuits Via Polynomials

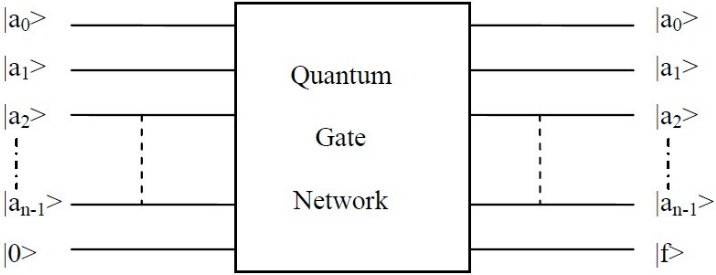
Kenneth W. Regan[1]
University at Buffalo (SUNY)

23 January, 2014

[1] Includes joint work with Amlan Chakrabarti and Robert Surówka

Quantum Circuits

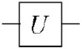
Quantum circuits look more constrained than Boolean circuits:



But Boolean circuits look similar if we do Savage's TM-to-circuit simulation and call each *column* for each tape cell a "cue-bit."

Quantum gates

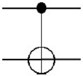
single qubit operation:



controlled-NOT:

control

target

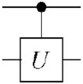


unitary matrix $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

controlled-U:

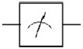
control

target



unitary matrix $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{pmatrix}$

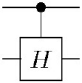
measurement in the $|0\rangle, |1\rangle$ basis:



[Slides concept by D. Bacon, U Washington]

Quantum gates: an example

controlled-gate
(here controlled-H)

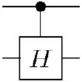


$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

input: $|\psi\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$

output: $|\psi'\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

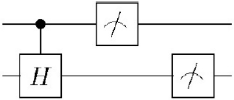
compute: $|1\rangle$ $|1\rangle$



$$= \begin{pmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

measure:

$|1\rangle$ $|1\rangle$



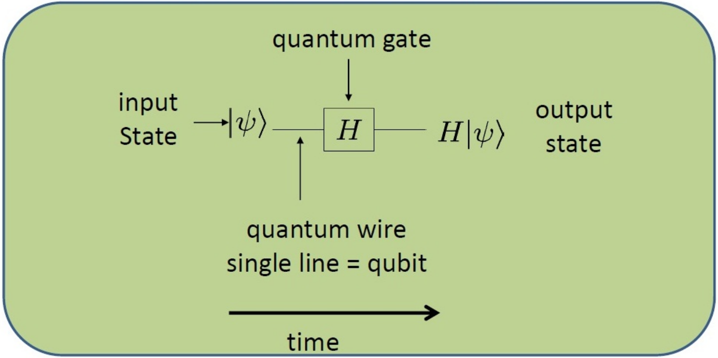
Probability of 10: $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

Probability of 11: $\left|\frac{-1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

Probability of 00 and 01: $|0|^2 = 0$

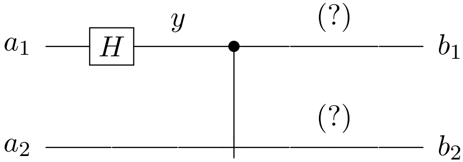
Quantum circuits

Quantum circuit diagrams to visualize a computation:



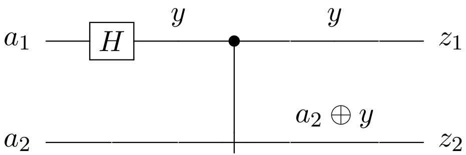
Quantum circuits are sequences of instructions. Describes a series of unitary evolutions (quantum gates) applied to a quantum state.

Does each wire have a local value?



Owing to the non-locality of entanglement, no. Tracing out either "(?)" gives 0+1, but destroys the structure. But can we give each wire a local *label* that preserves essential info?

Local Algebraic Labels and Global Phase

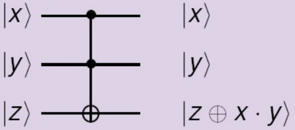


- On standard-basis inputs, labels always have $0, 1$ values.
- Global phase polynomial: $P = 1 - 2a_1y$ into $\{1, -1\}$; $Q = a_1y$ into $\{0, 1\}$.
- Gates like CNOT with $0, 1$ entries do not affect P or Q.

Toffoli Gate, With Labeling

The Toffoli gate "TOF"

x	y	z	x'	y'	z'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Theorem (Toffoli, 1981)

Any reversible computation can be realized by using TOF gates and ancilla (auxiliary) bits which are initialized to 0.

Slides by Martin Rötteler

Target label is just $z + xy$ in characteristic 2; $z + xy - 2xyz$ in general.

Bounded-error Quantum Poly-Time

A language A belongs to BQP if there are uniform poly-size quantum circuits C_n with n data qubits, plus some number $m \geq 1$ of "ancilla qubits," such that for all n and $x \in \{0, 1\}^n$,

$$
\begin{aligned}
x \in A &\implies \Pr[C_n \text{ given } \langle x0^m| \text{ measures 1 on line } n+1] > 2/3; \\
x \notin A &\implies \Pr[\dots] < 1/3.
\end{aligned}
$$

We can instead arrange the circuit to prepare x from actual input 0^{n+m}, and make 0^n10^{m-1} the unique target for acceptance. Two major theorems about BQP are:

(a) C_n can be composed entirely of Hadamard and Toffoli gates [Yaoyun Shi, 2002].

(b) Factoring is in BQP [Peter Shor].

Algebra For Measurement Targets

Boolean equality is enforced by the polynomial

$$e(u, z) = 1 - u - z + 2uz.$$

- Inequality, that is $u \oplus z$, is $e'(u, z) = u + z - 2uz$.
- In characteristic 2 just $e(u, z) = u + z + 1$ and $e'(u, z) = u + z$, both linear.
- Then also CNOT preserves linear labels, but TOF does not.
- If you measure just line 1, accepting result b_1, use $e(u_1, b_1)$.
- To measure all qubits testing a unique target $\vec{b}$, use $e(u_i, b_i)$ for each i.

What is Known About BQP?

- BPP $\subseteq$ BQP.
- BQP $\subseteq$ PP [Adleman-Demarrais-Huang, 1998]
- The acceptance probability p_x of a QC on input x can be written as

$$p_x = \frac{f(x) - g(x)}{\sqrt{2^r}}$$

  where f and g are #P functions whose nondeterminism ranges over $r = n^{O(1)}$ binary variables. Hence [Fortnow-Rogers, 1999] BQP is in a class AWPP ostensibly weaker than PP.
- BQP is not known to include graph-isomorphism or MCS (min.-circuit size).

Translation Into Polynomials

- Dawson et al. [2004] showed that for QC's of Hadamard and Toffoli gates, f and g could be the functions counting solutions to two sets E_1 and E_0 of polynomial equations over $\mathbf{Z}_2$.
- Applied by Gerdt and Severyanov [2006] to build a computer-algebra simulation of these quantum circuits.
- [This talk] We make E_1 and E_0 each a single equation, over any desired field or ring, with direct translation of a much wider set of quantum gates. *Some motivations*:
  - Build more extensive simulations—Chakrabarti.
  - Understand which QC's can be simulated "classically."
  - Ideas for algebraic metrics of multi-partite entanglement.
  - Limitations on scalability of QC's?

Target Rings

- Given a QC C, define $k(C)$ to be the least integer such that all phase angles of gates in C are multiples of $2\pi/k$.
- A ring is *adequate* for C if it embeds the k-th roots of unity, either multiplicatively or additively.
- Also embed $e(0) = 0$ in the multiplicative case ("p-case") and $e(0) =$ a set of dummy variables w in the additive case ("q-case") (a key trick, given below).
- For Toffoli+Hadamard, $k = 2$, and Dawson et al. gave an additive embedding into $\mathbf{Z}_2$. Whereas the p-case needs $\mathbf{Z}_3$ inside the field, so $-1 \neq +1$.
- For the T-gate which has entries $e^{\pi i/4}$, $k = 8$.
- The gates in Shor's QFT circuits have large k. But, they can be approximated by circuits with Hadamard and Toffoli only, with $k = 2$!

Polynomials and Equation Solving

We will translate quantum circuits with n lines and s gates. Each interior *juncture* is denoted by a variable z_i^j $(1 \leq i \leq n;\ 1 \leq j \leq s-1)$.

- A gate is *balanced* if all non-zero entries in its gate matrix have the same magnitude r.
- All the most prominent gates are balanced.
- Given a QC of balanced gates, let R be the product of the balancing magnitudes r over its gates.
- For a polynomial p in variables a_i, b_i, z_i^j and arguments $a, b \in \{0, 1\}^n$, $p_{a,b}$ denotes the polynomial in variables z_i^j resulting from substituting the arguments.
- $N_B[p_{a,b}(z_i^j) = v]$ denotes the number of *binary* solutions to the equation, i.e. with an assignment from $\{0, 1\}^{n(s-1)}$ to the z_i^j variables.

Now we can state the theorem for the multiplicative case.

Main Theorem—Multiplicative Case

Theorem

There is an efficient uniform procedure that transforms any balanced n-qubit quantum circuit C with s gates into a polynomial p such that for all $a, b \in \{0,1\}^n$:

$$\langle a| \, C \, |b\rangle = R \sum_{\ell=0}^{k-1} \omega^{\ell} N_B[p_{a,b}(z_i^j) = e(\omega^{\ell})] \tag{1}$$

over any adequate ring. The size of p as a product-of-sums-of-products of z_i^j and $(1 - z_i^j)$ is $O(2^{2m} ms)$ where m is the maximum arity of a gate in C, and the time to write p down is the same ignoring factors of $\log n$ and $\log s$ for variable labels.

Main Theorem—Additive Case For $\mathbf{Z}_k$

Theorem

There is an efficient uniform procedure that transforms any balanced n-qubit quantum circuit C with s gates, whose nonzero entries have phase a multiple of $2\pi/k$ for k a power 2^r, into a polynomial $q(\vec{a}, \vec{b}, \vec{z}, \vec{w})$ over $\mathbf{Z}_k$ such that for all $a, b \in \{0, 1\}^n$:

$$\langle a| \; C \; |b\rangle = Rk^{-s} \sum_{\ell=0}^{k-1} \omega^{\ell} N_B[q_{a,b}(z_i^j, w_s^j) = e(\omega^{\ell})], \tag{2}$$

with R and the size of q the same as for p in Theorem 1.

Substitution and Nondeterminism

- When there is no gate between junctures $j-1$ and j on qubit line i, or if the gate in column j leaves qubit i unchanged (as with a control), then one can substitute:

$$z_j^i = z_{j-1}^i.$$

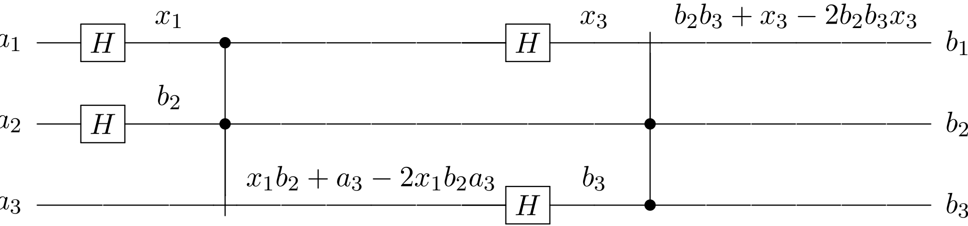
- Thus a new internal variable is introduced only when one cannot substitute.
- This happens with Hadamard gates.
- Nondeterminism = the number of internal variables.
- P' denotes polynomials obtained from the P formally given by Theorem 1 by substitution.
- Q' likewise from Q in Theorem 2.
- P'' denotes a particular embedding into the ring $\mathbf{Z}_2[u]$ where the adjoined element u satisfies $u^4 = 1$, so it translates i.

Examples of Gate and Circuit Simulations

Projected from a draft of the paper. . .

Definition. Two polynomials are *equivalent* if they arise from annotations of two equivalent quantum circuits.

Annotating a circuit



What to do with all this—in theory?

Two central theoretical problems are:

(1) Which subsets of quantum gates can be simulated efficiently with classical computation alone?

(2) What (classical) upper and lower bounds can be given for BQP?

Both problems involve one in subcases of the classic #P-complete problem of counting solutions to polynomial equations. Unlike the case of SAT, there has not been a comparable classification theorem, though Leslie Valiant and Jin-Yi Cai and their students have undertaken one.

Case of Stabilizer Circuits

- Are QC's with only Hadamard, S, and CNOT and/or CZ gates.
- Have efficient classical simulations: $O(s^3)$ by Gottesmann-Knill, $O(s^2)$ by Aaronson-Gottesmann, $O(s)$ by Peter Hoyer (give-and-take $\log n$ factors).
- Additive translation into equations over $\mathbf{Z}_4$:
  1. Hadamard: $2yz$, with no substitution; and
  2. S: y^2, substituting $z := y$; and
  3. CZ: $2y_1y_2$, substituting $z_1 := y_1$, $z_2 := y_2$; *or*
  4. CNOT: 0, substituting $z_1 := y_1$, $z_2 := y_1 + y_2$, with the latter being sound in place of the proper $z_2 := y_1 + y_2 - 2y_1y_2$ owing to the invariance under adding 2.

Yet Another Proof of Dequantization

Theorem (Cai-Chen-Lipton-Lu, 2010)

Quadratic n-variable polynomials over $\mathbf{Z}_{2^r}$ for fixed r have polynomial-time solution colunting.

Open for variable $r = n^{O(1)}$.

Corollary

The exact acceptance probability for stabilizer circuits can be computed in deterministic polynomial time.

General running time from CCLL is inferior to best-known "graph state" methods for stabilizer circuits. *Can this be matched for the particular polynomials we get over $\mathbf{Z}_4$?*

Graininess of Solution Set Sizes

Theorem (Surówka)

Let $P(x)$ be a multivariate polynomial of n variables over $\mathbb{Z}_m$ where $m = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ and all $p_1, p_2, \dots, p_k$ are different primes. Then for any $g \in \mathbb{Z}_m$ there is an integer T_g such that:

$$N_P[g] = T_g \prod_{i:2|r_i} p_i^{\frac{r_i}{2}(n-1)} \prod_{i:2\nmid r_i} p_i^{\frac{r_i-1}{2}(n-1)}$$

Graininess of Solution Set Sizes

Theorem (Surówka)

Let $P(x)$ be a multivariate polynomial of n variables over $\mathbb{Z}_m$ where $m = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ and all $p_1, p_2, \ldots, p_k$ are different primes. Then for any $g \in \mathbb{Z}_m$ there is an integer T_g such that:

$$N_P[g] = T_g \prod_{i:2|r_i} p_i^{\frac{r_i}{2}(n-1)} \prod_{i:2\nmid r_i} p_i^{\frac{r_i-1}{2}(n-1)}$$

Proof applies Hensel lifting. But we believe we can go beyond what Hensel's techniques, as used by Ax and others, give.

Beyond Lifting...

Also in terms of the degree, we conjecture the following stronger result, with supportive computer runs:

Conjecture

Let $P(x)$ be a multivariate polynomial of degree d, of n variables over $\mathbb{Z}_{p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}}$ where all $p_1, p_2, \dots, p_k$ are different primes. Then for any $g \in \mathbb{Z}_{p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}}$ there is an integer T_g such that:

$$N_P[g] = T_g \prod_{i:r_i=1} p_i^{\lceil \frac{n}{d} \rceil - 1} \prod_{i:r_i>1} p_i^{\lceil \frac{r_i n}{2} \rceil - 1}.$$

The Other Goals—Ideas Welcome

- Extend notion of equivalence to manipulations giving polynomials that *do not* come from QC's.
- Try to *increase* the R factor without introducing more nondeterminism. That makes Stockmeyer approximation "better."
- What notions from algebraic geometry might yield measures of entanglement?
- Idea: It should reflect constraints on solution spaces. This aligns it with the idea of *geometric degree* of algebraic varieties.
- Ultimately goal is to apply Strassen's lower-bound ideas to QC's.