Models of Quantum Computation:
Sum Estimation Oracles

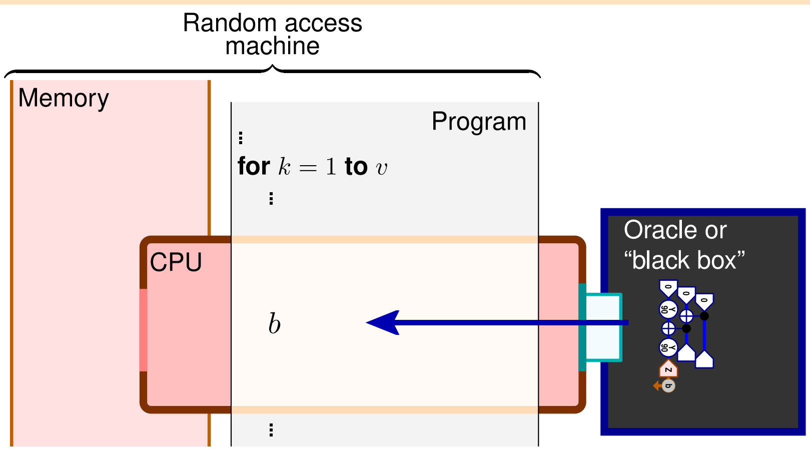
- Deterministic computation with oracles.
- QWGTs ("queue-widgets").
- Promise problems.
- Quantum network oracles.
- Equivalence to QWGT estimation.

E. "Manny" Knill: knill@lanl.gov, http://www.lanl.gov/~knill

Why Study Quantum Information?

- QI is a tool.
  - A language for quantum control.
  - Generalization of information theory.
  - Linearization of the theory of computation.
- QI's potential.
  - Efficient quantum physics simulation.
  - Communication security.
  - Efficient factoring and other number theory algorithms.
  - Insights into complexity theory?
- QI may be realizable.
  - Quantum noise is in principle controllable.
  - Numerous experimental proposals.
- . . . when?

Computation with Oracles



- Quantum computation = deterministic computation + $\begin{cases} \text{quantum network queries} \\ \text{or} \\ \text{sum estimation queries} \end{cases}$ Yao 1993 [1]

QWGTs

- *Quadratically signed weight enumerators*: Knill&Laflamme 2001 [2]

$$S_{A,B}(x,y) = \sum_{b:Ab=0} (-1)^{b^T B b} x^{|b|} y^{n-|b|}$$

$$\text{where} \begin{cases} b: & \text{0-1 vectors, e.g. } b = (1,0,0,1,0\ldots) \\ A,B: & \text{0-1 matrices, } A \text{ is } m\times n \text{ and } B \text{ is } n\times n. \\ & \text{Arithmetic involving } a,b,A,B \text{ is modulo } 2. \\ |b|: & \textit{weight} \text{ of } b\text{, i.e. \# of 1's in } b. \end{cases}$$

- **Theorem 1:** "$S_{A,B}(k,l) > r$?" is P$^{\#P}$ complete$_{\text{Poly-Turing}}$.

Proof (outline).

$\Rightarrow$: $S_{A,B}(k,l)$ is the difference between two #P functions.
$\Leftarrow$: $S_{A,0}(k,l)$ is the weight enumerator of a binary code. Its evaluation is #P hard.

Vertigan 1992 [3]

Approximating QWGTs

- $|S_{A,B}(x,y)| \le (|x|+|y|)^n$.
- Monte Carlo estimate.
  1. Compute the dimension d of $C=\{b : Ab=0\}$.
  2. Randomly choose $b \in C$.
  3. $S \leftarrow 2^d\Big((-1)^{b^TBb}x^{|b|}y^{n-|b|}\Big)$.

  - Expectation: $\langle S\rangle = S_{A,b}(x,y)$.
  - Variance: $$\begin{aligned}\mathrm{var}(S) &= 2^d\textstyle\sum_{b\in C} x^{2|b|}y^{2(n-|b|)} - S_{A,B}(x,y)^2\\ \mathrm{std}(S) &\le 2^{d/2}\big(x^2+y^2\big)^{n/2}\end{aligned}$$
- **Theorem 2:** One can efficiently approximate $S_{A,B}(x,y)$ to $o\big(2^{d/2}(x^2+y^2)^{n/2}\big)$ with high probability.
- **Problem 1:**
  Efficient approximation of $S_{A,B}(x,y)$ to $o\big((x^2+y^2)^{n/2}\big)$?

Rem.: $S_{A,B}(x,y) = \sum_{b:Ab=0}(-1)^{b^TBb}x^{|b|}y^{n-|b|}$

Promise Problems

- *Promise problem* for predicates $R(x)$,$P(x)$. $P(x)$ need not be r.e.
  "$R(x)$ given the promise $P(x)$?"
- Let C be a computation with probabilistic output $C(x)$.
  C *solves* promise problem $\mathcal{P}(R,P)$ if for all x,
  $$\left.\begin{aligned} P(x)\wedge R(x) &\Rightarrow \mathrm{prob}(C(x)=1) > .75\\ P(x)\wedge \neg R(x) &\Rightarrow \mathrm{prob}(C(x)=0) < .25\end{aligned}\right\}\text{"bounded error"}$$
- **Problem 2:** Given A,B,k,l and the promise that
  $|S_{A,B}(k,l)| \ge (k^2+l^2)^{n/2}/2$.
  Determine the sign of $S_{A,B}(k,l)$.

Rem.: $S_{A,B}(x,y) = \sum_{b:Ab=0}(-1)^{b^TBb}x^{|b|}y^{n-|b|}$

BQPP-complete QWGTs

- For square A, let $\mathrm{ltr}(A)$ be the lower triangular part of A.
  Ex.: $A = \begin{pmatrix}0&1&1\\1&1&0\\0&1&0\end{pmatrix} \rightarrow \mathrm{ltr}(A) = \begin{pmatrix}0&0&0\\1&0&0\\0&1&0\end{pmatrix}$
- **Problem 3:** Given square A with $\mathrm{diag}(A)=\mathbb{I}$, $k,l\in\mathbb{N}$,
  and the promise $\big|S_{A,\mathrm{ltr}(A)}(k,l)\big| \ge (k^2+l^2)^{n/2}/2$.
  Determine the sign of $S_{A,\mathrm{ltr}(A)}(k,l)$. [Can take $k=4, l=3$.]
- For matrices C,D, define $[C;D] = \begin{pmatrix}C\\D\end{pmatrix}$
- **Problem 4:** Given square A with $\mathrm{diag}(A)=\mathbb{I}$, $k,l\in\mathbb{N}$,
  and the promise $\big|S_{[A,A^T],\mathrm{ltr}(A)}(k,l)\big| \ge (k^2+l^2)^{n/2}/2$.
  Determine the sign of $S_{[A,A^T],\mathrm{ltr}(A)}(k,l)$. [Can take $k=4, l=3$.]

Rem.: $S_{A,B}(x,y) = \sum_{b:Ab=0}(-1)^{b^TBb}x^{|b|}y^{n-|b|}$

Promise Problem Reductions

- Reductions are deterministic polynomial time many-one.

  "$R(x)$ with promise $P(x)$?"
  reduces to
  "$S(x)$ with promise $Q(x)$?"
  $\Updownarrow$
  There exists a function $f \in$ PolyTime
  such that
  $$P(x) \rightarrow \big(Q(f(x)) \wedge (R(x) \leftrightarrow S(f(x)))\big)$$
- BQPP: Bounded error quantum poly-time promise probs.
- **Theorem 3:** Problem 3 is BQPP complete.

Rem.: $S_{A,\mathrm{ltr}(A)} = \sum_{b:Ab=0}(-1)^{b^T\mathrm{ltr}(A)b}4^{|b|}3^{n-|b|}$, promise: $|S_{A,\mathrm{ltr}(A)}| \ge 5^n/2$

Promise Problem Reductions

- Reductions are deterministic polynomial time many-one.

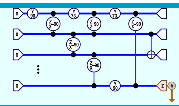
"$R(x)$ with promise $P(x)$?"
reduces to
"$S(x)$ with promise $Q(x)$?"

$\Updownarrow$

There exists a function $f \in$ PolyTime
such that

$$P(x) \rightarrow (Q(f(x)) \wedge (R(x) \leftrightarrow S(f(x))))$$

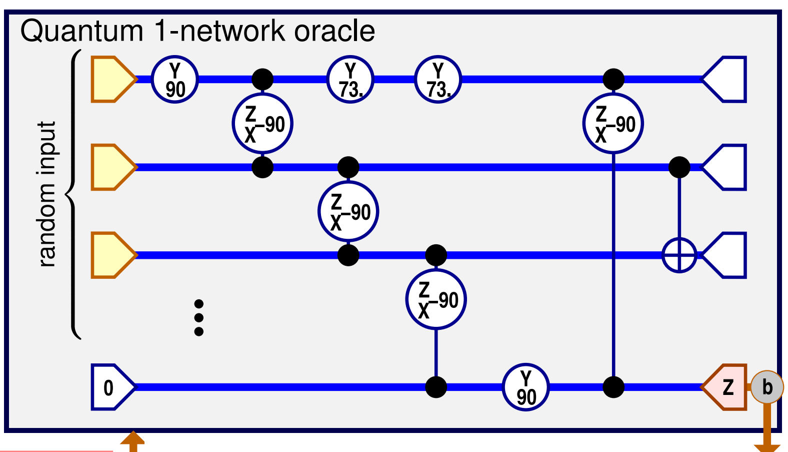
Goto: Quantum network primer.

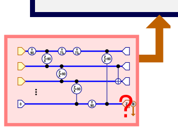


- **Theorem 3:** Problem 3 is BQPP complete.

Rem.: $S_{A,\mathrm{ltr}(A)} = \sum_{b:Ab=0} (-1)^{b^T \mathrm{ltr}(A) b} 4^{|b|} 3^{n-|b|}$, promise: $|S_{A,\mathrm{ltr}(A)}| \geq 5^n/2$

One Qubit Quantum Computer





Motivation: Liquid state nuclear magnetic resonance.

Knill&Laflamme 1998 [4]

Models of Quantum Computation

- RAM$^{q\mathcal{N}}$: Random access machine (RAM) + quantum network oracle ($q\mathcal{N}$).
  RAM$^{q_1\mathcal{N}}$: RAM + quantum 1-network oracle ($q_1\mathcal{N}$).

- Theorems:
  - There exist $\mathcal{O}$ such that RAM$^{q_1\mathcal{N},\mathcal{O}} <_{\text{poly}}$ RAM$^{q\mathcal{N},\mathcal{O}}$.
  - Efficient spectral density estimation with RAM$^{q_1\mathcal{N}}$.
  - RAM$^{q\mathcal{N}} \not\leq_{\text{faithful poly}}$ RAM$^{q_1\mathcal{N}}$. Ambainis&Schulman&Vazirani 2000 [5]

Path Sums

- RAM$^{q\mathcal{N}}$: Random access machine (RAM) + oracle ($q\mathcal{N}$).
- Notation. $\mathcal{G}$ is a sequence of unitary gates $(G_1 \ldots, G_N)$
  $U(\mathcal{G}) = G_N G_{N-1} \ldots G_1$
  $|\mathbf{b}\rangle = |b_1 \ldots b_n\rangle$
- $\mathrm{prob}(q\mathcal{N}(\mathcal{G}) \equiv \mathfrak{o})$

$$= \sum_{\mathbf{b}} \left| \sum_{\mathbf{a_1},\mathbf{a_2},\ldots} \langle \mathfrak{o}\mathbf{b}|G_N \ldots |\mathbf{a_2}\rangle\langle \mathbf{a_2}|G_2|\mathbf{a_1}\rangle\langle \mathbf{a_1}|G_1|\mathbf{0}\rangle \right|^2$$

- $\mathrm{prob}(q_1\mathcal{N}(\mathcal{G}) \equiv \mathfrak{o})$

$$= \sum_{\mathbf{a},\mathbf{b}} \frac{1}{2^{n-1}} \left| \sum_{\mathbf{a_1},\mathbf{a_2},\ldots} \langle \mathfrak{o}\mathbf{b}|G_N \ldots |\mathbf{a_2}\rangle\langle \mathbf{a_2}|G_2|\mathbf{a_1}\rangle\langle \mathbf{a_1}|G_1|\mathfrak{o}\mathbf{a}\rangle \right|^2$$

- Entries of G_i in PSpace $\rightarrow$ $\mathrm{prob}(q\mathcal{N}(\mathcal{G}) \equiv \mathfrak{o})$ is in PSpace
  $\rightarrow$ $\mathrm{prob}(q_1\mathcal{N}(\mathcal{G}) \equiv \mathfrak{o})$ is in PSpace

Two Operator Bases

- Let U be a unitary n-qubit operator.
- *Transition* basis.

$$U = \sum_{\mathbf{a},\mathbf{b}} \underbrace{\langle \mathbf{a}|U|\mathbf{b}\rangle}_{U_{\mathbf{a},\mathbf{b}}} |\mathbf{a}\rangle\langle\mathbf{b}|$$

- *Pauli* basis.

$$U = \sum_{\mathbf{b}} \tfrac{1}{2^n}\mathrm{tr}\,(\sigma_{\mathbf{b}}U)\,\sigma_{\mathbf{b}}$$

Def.: $\sigma_{00} = \mathbb{I}$, $\sigma_{01} = \sigma_x$, $\sigma_{11} = \sigma_y$, $\sigma_{10} = \sigma_z$
$\sigma_{\mathbf{b}} = \sigma_{b_0 b_{1(1)}}\sigma_{b_2 b_{3(2)}}\cdots$
$\mathrm{tr}(A) = \sum_{\mathbf{a}} \langle \mathbf{a}|A|\mathbf{a}\rangle$

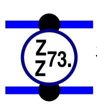
- **Problem 5:**
"Sign of $\alpha = \langle \mathbf{a}|U(\mathcal{G})|\mathbf{b}\rangle$ with promise $|\alpha| \geq 1/2?$"
  - Polynomially equivalent to $q\mathcal{N}$. [Can take $\mathbf{a} = \mathbf{b} = \mathbf{0}$]
- **Problem 6:**
"Sign of $\beta = \frac{1}{2^n}\mathrm{tr}\,(\sigma_{\mathbf{b}}U(\mathcal{G}))$ with promise $|\beta| \geq 1/2?$"
  - PolyTime given $q_1\mathcal{N}$. [Can take $\sigma_{\mathbf{b}} = \mathbb{I}$]

Pauli Product Gates

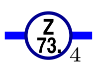
- A set of unitary gates $\mathcal{U}$ on n qubits is *universal* if $\langle\mathcal{U}\rangle$ contains all unitaries up to a phase.

Def.: $\langle\mathcal{U}\rangle$ is the closure of the set of products of operators in $\mathcal{U}$.

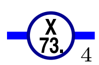
- A universal set $\mathcal{U}_r$ of rational unitaries. Bernstein&Vazirani 1993 [6]



$\frac{4}{5} - i\frac{3}{5}\sigma_{z(\mathrm{A})}\sigma_{z(\mathrm{B})}$

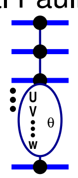


$\frac{4}{5} - i\frac{3}{5}\sigma_{z(\mathrm{C})}$



$\frac{4}{5} - i\frac{3}{5}\sigma_{x(\mathrm{D})}$

- Standard q.comp. is defined by universal gate sets poly-equivalent to $\mathcal{U}_r$.
- General Pauli product gates.



$$e^{-i\sigma_{\mathbf{b}}\theta/2} = \cos(\theta/2) - i\sin(\theta/2)\sigma_{\mathbf{b}}$$

...polynomially equivalent.

Calculating with Pauli Products

- For $\mathbf{b} = (b_0b_1, b_2b_3, \ldots, b_{2n-2}b_{2n-1})$: ...toward QWGTs ≡ BQPP

$|\mathbf{b}|_y$ is the number of σ_y in $\sigma_{\mathbf{b}}$.

$$\tilde{\sigma}_{\mathbf{b}} = (-i)^{|\mathbf{b}|_y}\sigma_{\mathbf{b}}. \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} B & 0 & \cdots \\ 0 & B & \\ \vdots & & \ddots \end{pmatrix}$$

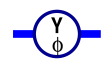
- **Lemma 4:** $\tilde{\sigma}_{\mathbf{b}}\tilde{\sigma}_{\mathbf{c}} = (-1)^{\mathbf{b}^T\mathbf{B}\mathbf{c}}\tilde{\sigma}_{\mathbf{b}+\mathbf{c}}$

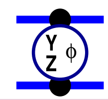
$\frac{1}{2^n}\mathrm{tr}(\sigma_{\mathbf{b}}) = \delta_{\mathbf{b},0}$ $\qquad \langle\mathbf{0}|\tilde{\sigma}_{\mathbf{b}}|\mathbf{0}\rangle = \begin{cases} 1 & \text{if } \mathbf{B}\mathbf{b} = \mathbf{0} \\ 0 & \text{otherwise} \end{cases}$

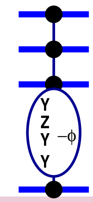
- A universal set of Pauli product gates.

$$\mathcal{U} = \{\tfrac{4}{5} + \tfrac{3}{5}\tilde{\sigma}_{\mathbf{b}} \,|\, |\mathbf{b}|_y \text{ is odd}\}$$

Ex.: Let $\phi = 2 * \arccos(4/5) = 73.7398°$.







Pauli Product Sums

- Let $\mathcal{G} = (G_1 \ldots, G_N)$, $G_k = \frac{1}{5}(4 + 3\tilde{\sigma}_{\mathbf{b}_k})$
-
$$\begin{aligned} U(\mathcal{G}) &= G_N \ldots G_1 \\ &= \tfrac{1}{5^N}(4 + 3\tilde{\sigma}_{\mathbf{b}_N})\ldots(4 + 3\tilde{\sigma}_{\mathbf{b}_1}) \\ &= \tfrac{1}{5^N}\textstyle\sum_{\mathbf{a}}(-1)^{\mathbf{a}^T \mathrm{ltr}(H^T\mathbf{B}H)\mathbf{a}}\, 4^{N-|\mathbf{a}|}3^{|\mathbf{a}|}\tilde{\sigma}_{H\mathbf{a}} \end{aligned}$$

  - $H = (\mathbf{b}_1, \ldots, \mathbf{b}_N)$.
  - By assumption: $\mathrm{diag}\,(H^T\mathbf{B}H) = \mathbb{I}$
- RAM$^{q\mathcal{N}}$: $\langle\mathbf{0}|U(\mathcal{G})|\mathbf{0}\rangle = \frac{1}{5^N}\sum_{\mathbf{a}:\mathbf{B}H\mathbf{a}=\mathbf{0}}(-1)^{\mathbf{a}^T\mathrm{ltr}(H^T\mathbf{B}H)\mathbf{a}}\, 4^{N-|\mathbf{a}|}3^{|\mathbf{a}|}$ to within $o(1)$.
- RAM$^{q_1\mathcal{N}}$: $\frac{1}{2^n}\mathrm{tr}U(\mathcal{G}) = \frac{1}{5^N}\sum_{\mathbf{a}:H\mathbf{a}=\mathbf{0}}(-1)^{\mathbf{a}^T\mathrm{ltr}(H^T\mathbf{B}H)\mathbf{a}}\, 4^{N-|\mathbf{a}|}3^{|\mathbf{a}|}$ to within $o(1)$.

Compare to: $\sum_{b:[A;A^T]b=0}(-1)^{b^T\mathrm{ltr}(A)b}3^{|b|}4^{N-|b|}$ to within $o(5^N)$

- See [2] for the remaining steps of the reductions.

Conclusion

- Hierarchy of problems:

$S_{A,\mathrm{ltr}(A)}(4,3) > m$?
given $\mathrm{diag}(A) = \mathbb{I}$

$\mathrm{P}^{\#\mathrm{P}}$

[2],prob(ans=1)
$\propto$ #NP sols.

$S_{A,B}(k,l) > m$?

$S_{[A;A^T],\mathrm{ltr}(A)}(4,3) > m$?
given $\mathrm{diag}(A) = \mathbb{I}$

$\alpha = S_{A,\mathrm{ltr}(A)}(4,3) > 0$?
given $\mathrm{diag}(A) = \mathbb{I}$, $|\alpha| \geq 5^n/2$

BQPP = $\mathrm{BPPP}^{q\mathcal{N}}$

$S_{[A;A^T],\mathrm{ltr}(A)}(4,3) > 0$?
given $\mathrm{diag}(A) = \mathbb{I}$, $|\alpha| \geq 5^n/2$

$\mathrm{BQ_1PP} = \mathrm{BPPP}^{q_1\mathcal{N}}$

...some reductions are poly-Turing.

- **Problem 7:** $\mathrm{RAM}^{q_1\mathcal{N}} \equiv_{\text{poly}}$ probabilistic RAM?
- **Problem 8:** Improve probabilistic approximation of $S_{A,B}(k,l)$ to better than $\frac{1}{\mathrm{POLY}} 2^d (k^2 + l^2)^{n/2}$?

Take advantage of algs for permanent? Jerrum&Sinclair&Vigoda 2000 [7]

Rem.: $S_{A,B}(x,y) = \sum_{b:Ab=0} (-1)^{b^T B b} x^{|b|} y^{n-|b|}$

References

[1] A. Yao. Quantum circuit complexity. In ?, editor, *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*, pages 352–360, Los Alamitos, California, 1993. IEEE Press.

[2] E. Knill and R. Laflamme. Quantum computation and quadratically signed weight enumerators. *Information Processing Letters*, 79:173–179, 2001. quant-ph/9909094.

[3] D. L. Vertigan. Bycycle dimension and special points of the Tutte polynomial. *J. of Comb. Theory A*, 220:53–162, 1992.

[4] E. Knill and R. Laflamme. On the power of one bit of quantum information. *Phys. Rev. Lett.*, 81:5672–5675, 1998.

[5] A. Ambainis, L. J. Schulman, and U. Vazirani. Computing with highly mixed states. In *Proceedings of the 32th Annual ACM Symposium on the Theory of Computation (STOC)*, pages 697–704, New York, New York, 2000. ACM Press.

[6] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26:1411–1473, 1997.

[7] M. Jerrum, A. Sinclair, and E. Vigoda. A polynomial-time approximation algorithm for the permanent of a matrix with non-negative entries. Technical Report TR00-079, Electronic Colloquium on Computational Complexity, 2000.

Contents