Simulation of quantum computers with probabilistic models

Vlad Gheorghiu

Department of Physics
Carnegie Mellon University
Pittsburgh, PA 15213, U.S.A.

April 6, 2010

- A summary of this talk is available online at http://quantum.phys.cmu.edu/QIP
- Reference: Maarten Van den Nest, arXiv:0911.1624 [quant-ph], arXiv:0811.0898 [quant-ph]

- Why are some quantum algorithms believed to have no efficient classical efficient counterpart?
- Why some others quantum algorithms *can* be simulated clasically?
- First thought: Entanglement...
- Indeed, certain computations are simulatable due to the absence of high amount of entanglement.
- Second thought: Entanglement is not always a key ingredient.
- Gottesman-Knill theorem, classical simulation of matchgate circuits, exhibit large degrees of entanglement, but cannot achieve computational speed-up over classical computers.

- What exactly is *classical simulation*?
- Strong simulation: classically compute the measurement probabilities (or expectation values) with high precision in poly-time.
- Weak simulation: Classically sample in poly-time from the resulting output probability distribution.
- Quantum mechanics is probabilistic. Weak simulation is more natural.
- There are examples of quantum circuits for which strong simulation is intractable ($\#$P), whereas weak simulation is achieved by elementary sampling methods, see e.g. arXiv: 0811.0898 [quant-ph].

- Computationally-tractable states (CT states): a state $|\psi\rangle$ is CT if it is possible to classically simulate computational basis measurements on $|\psi\rangle$ *and* if the coefficients of $|\psi\rangle$ in this basis can be efficiently computed.
- Examples: MPS, Stabilizer states, poly-size matchgate states, etc.
- Efficiently computable sparse operations (ECS). An n-qubit operation is ECS if its matrix representation in the standard basis has at most poly(n) nonzero entries per row and per column, and if these entries can be determined efficiently.
- Examples: Pauli products, k-local operators with $k = O(\log n)$, poly-size Toffoli gates etc.

Theorem

Consider a poly-size quantum circuit U acting on a state $|\psi\rangle$ and followed by measurement of an observable O. If $|\psi\rangle$ is CT and if $U^\dagger O U$ is ECS, then this quantum computation can be simulated classically.

- The unitary operation U *is not* required to be sparse. Example: U is some Clifford operation – then $U^\dagger Z U$ is a Pauli product, which is an ECS operation.
- Sparse circuits, composability:

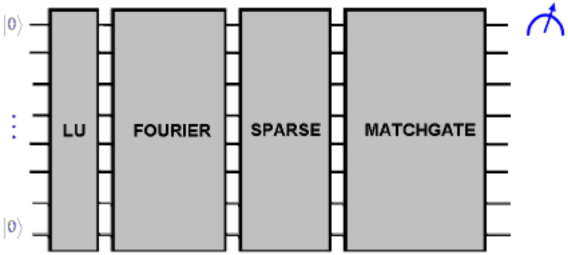

Figure: Concatenated sparse circuits

- Sparse unitaries are of interest: highlight the role of *interference* in quantum computation, as opposed to *entanglement*. Can produce highly entangled states, but the interference is always limited.
- Weak simulation is efficiently possible, whereas strong simulation is #P-hard.
- Concatenation of simulatable blocks of very different nature may remain efficiently simulatable
- CNOT-$e^{i\theta X}$: Poly-size circuits composed of CNOT and $e^{i\theta X}$ gates, acting on product inputs and followed by Z measurements on any single qubit, can be simulated classically.
- Interesting, since CNOT together with any *real* one-qubit gate V such that V^2 is not basis-preserving, is universal for quantum computation.

- Quantum algorithms:

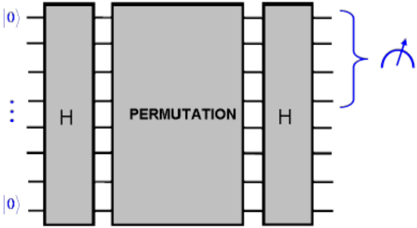

Figure: Schematic model of Simon's and Shor's algorithms

Theorem (Rough version)

Consider a quantum circuit with the above structure. If the function computed in the round of postprocessing is promised to have a sufficiently "peaked" Fourier spectrum, then the entire circuit cab be simulated efficiently classically, independent of the specific forms of the other rounds.

Definition

An n-qubit state is CT if the following hold:

1. it is possible to sample in poly(n) time with classical means from the probability distribution $Prob(x) = |\langle x|\psi\rangle|^2$ on the set of n-bit strings x, and
2. upon input of any bit string x, the coefficient $\langle x|\psi\rangle$ can be computed in poly(n) time on a classical computer.

- There are states that satisfy 2 but not 1!
- Example: Consider any *efficiently computable* function $f : \{0,1\}^n \to \{0,1\}$ for which it is promised that there exists a unique x_0 such that $f(x_0) = 1$, and define $|\psi\rangle = \sum_x f(x)|x\rangle$. The function satisfies 2.
- Assuming that 2 implies 1, it follows that it is possible to sample from a distribution that has 0 probability except for x_0 (probability 1), so x_0 can be determined efficiently by sampling.
- Regard f as a verifier for an *NP* problem with a unique witness!

Examples:

1. Product states.
2. $\sum_x e^{i\theta(x)}$, where $\theta(x)$ is efficiently computatble.
3. Matrix product states of polynomial bond dimension. A state $|\psi\rangle$ is an MPS of poly bond dimension if there exists $2n$ $N \times N$ matrices $A_i[0]$, $A_i[1]$ with $N = \mathrm{poly}(n)$ such that $\langle x|\psi\rangle = Tr(A_1[x_1] \ldots A_n[x_n])$, for every n-bit string $x = (x_1, \ldots, x_n)$.
4. Stabilizer states.
5. Poly-size matchgate circuits applied to a computational basis state, where all gates are restricted to act on nearest neighbors.
6. Fourier transform applied to an arbitrary product state.

Basis-preserving operations:

- There are operations that map the family of CT states to itself.
- An n-qubit operation M is called *basis-preserving* if the computational basis states are mapped to $M|x\rangle = \gamma_x|\pi(x)\rangle$, for some permutation π and complex γ_x.
- M is efficiently computable if $x \to \gamma_x$, $x \to \pi(x)$ and $x \to \pi^{-1}(x)$ can be evaluated in poly(n) time.
- Examples: Pauli products, $\sum_x (-1)^{f(x)}|x\rangle\langle x|$ where $f : \{0,1\}^n \to \{0,1\}$ is efficiently computable, every poly-sized circuit composed of elementary basis-preserving gates.

Lemma

If $|\psi\rangle$ is a CT state and if M is an efficiently computable unitary basis-preserving operation, then $M|\psi\rangle$ is CT.

Sparse operations:

- An n-qubit operation A is s-sparse if for every basis state $|x\rangle$, both $A|x\rangle$ and $A^T|x\rangle$ is a linear combination of at most s computational basis states.
- Efficiently computable sparse (ECS) operations: for given $|x\rangle$, list in poly(n) time the non-zero row/column entries associated with $|x\rangle$, together with the row/column index.

Examples:

1. Efficiently computable basis-preserving operations are ECS.
2. Every d-qubit gate G acting within an n-qubit circuit, $G \otimes I$, is 2^d sparse. If $d = O(\log n)$, then it is ECS.
3. Linear combinations of poly(n) ECS operations.
4. Let U be an n-qubit poly-size circuit of basis-preserving gates, interspersed with $V_1, \ldots, V_k$ at arbitrary places, each of which act on at most d qubits, with $kd = O(\log n)$. Then U is ECS.

Main technical results:

Theorem

Let $|\psi\rangle$ and $|\phi\rangle$ be CT n-qubit states and let A be ECS (not necessarily unitary), with $||A|| \leq 1$. Then there exists an efficient classical algorithm to approximate $\langle\phi|A|\psi\rangle$ with polynomial accuracy.

Corollary

Let $|\psi\rangle$ be an n-qubit CT and let O be a d-local observable with $d = O(\log n)$ and $||O|| \leq 1$. Then there exists an efficient classical algorithm to estimate $\langle\psi|O|\psi\rangle$ with polynomial accuracy.

Corollary

Let $|\psi\rangle$ and $|\phi\rangle$ be n-qubit CT states, let $|\xi\rangle$ and $|\chi\rangle$ be k-qubit CT states $(k \leq n)$ and let A, B be ECS n-qubit operations, with $||A||, ||B|| \leq 1$. Then there exists an efficient classical algorithm to approximate $\langle\phi|A(|\xi\rangle\langle\chi| \otimes I)B|\psi\rangle$ with polynomial accuracy.

Classical simulation of sparse circuits:

- Let U be a circuit composed of m ECS s-sparse unitaries, with s^m =poly(n). The circuit acts on an arbitrary product input state and is followed by a Z measurement. Can be efficiently simulated classically.
- Sparse operations highlight the role of interference, as opposed to entanglement.
- Consider graph states, U consists of poly(n) CPHASE gates (which are basis-preserving, hence very simple sparse operations). The cluster state is highly entangled, but does not have "enough interference", since it has at most poly(n) coefficients.

Composability:

Corollary

Consider poly-size n-qubit circuits U_1 and U_2, an input state $|\psi_{in}\rangle$ and an observable O such that: (i) $U_1|\psi\rangle$ is CT and (ii) $U_2^\dagger O U_2$ is ECS. Then $U = U_2 U_1$ acting on $|\psi_{in}\rangle$ and followed by measurement of O can be simulated efficiently classically.

Examples of pairs (U, O) where $U^\dagger O U$ is ECS:

- U circuit of constant depth, O acts non-trivially on $O(\log n)$ qubits.
- U Clifford, O linear combination of poly(n) Pauli products.
- U nearest-neighbor matchgates and let $O = Z_1$, the Pauli operator on the first qubit. U maps Z_1 to a linear combination of poly(n) Pauli products, which is ECS.

Simulating quantum algorithms.

Potts models: estimating the partition functions of spin systems (generalization of the Ising model). A proposed quantum algorithm in arXiv:0805.0040 [quant-ph] for estimating the partition function can be efficiently classically simulated, since the estimation can be written as the overlap $\langle\alpha|\psi\rangle$ between a matrix product state and a stabilizer state, both of which are CT.

Deutsch-Jozsa: constant vs balanced functions $f:\{0,1\}^n \to \{0,1\}$. A randomized classical algorithm can solve DJ using $O(n)$ queries, with exponentially low probability of error.

1. Apply a local unitary V_1.
2. Apply an ECS V_2.
3. Apply another local unitary V_3.
4. Measure $O = |0\rangle\langle 0|^k \otimes I$, for some $k \leq n$

- After round 1, the state is CT.
- The operation in round 2 is ECS.
- Finally the observable $V_3^\dagger O V_3$ has the form $|\gamma\rangle\langle\gamma| \otimes I$ for some k-qubit product–and hence CT–state $|\gamma\rangle$.
- The result now follows from the corollary.
- The form of f is *irrelevant*. The lack in computational power is a *structural* feature of the circuit.
- Changing the oracle is not enough!

Simon's algorithm

- Very simple quantum algorithm that achieves an exponential speed-up.
- Oracle access to $f : \{0,1\}^n \to \{0,1\}^n$. It is promised that there exists an unknown n-bit string a such that $f(x) = f(y)$ *if and only if* $y = x + a \pmod 2$. The goal is to find a.
- Suffices to determine the i=th bit of a for some i, efficiently; fix $i = 1$ for simplicity. Simon's algorithm consists of the following steps:
  1. 2 registers of n qubits, both initially in $|0\rangle^n$.
  2. Apply H^n to every qubit in the first register.
  3. The oracle U_f is applied, yielding $\sum_x |x\rangle|f(x)\rangle$.
  4. Again a Hadamard is applied to the first register, yielding $|\psi_{out}\rangle = \sum_{u\in\mathcal{V}} |u\rangle|\psi_u\rangle$. The sum is over all n-bit strings u that are orthogonal to a w.r.t. mod 2 arithmetic. Denote by $\mathcal{V}$ the subspace over $\mathbb{Z}_2$ of all such u.
  5. Run N times, measure all qubits in the first register, group them as a $N \times n$ matrix with rows $u_1, u_2, \ldots, u_N$. If $N = O(n)$ then the probability that $u_1, \ldots, u_N$ *do not span* $\mathcal{V}$ is exponentially small in n.
  6. Use a classical computer to compute $\mathbf{u}x = 0 \bmod 2$ (find x with the first bit=1).

Simon's algorithm, structure:

1. Apply a round of Hadamards to some subset of qubits.
2. Apply an ECS basis-preserving unitary.
3. Apply another round of Hadamards to some subset S.
4. Perform a computational measurement of all qubits in S. Denote by $\mathbf{u}$ the bit string containing all measurement outcomes.
5. Classically compute the value $g(\mathbf{u})$–which represents the output of the algorithm– where g is some efficiently computable Boolean function.