E Abrams-Lloyd theorem

E.1 Overview

All experiments to date confirm the linearity of QM, but what would be the consequences of slight nonlinearities?[21] We will see that nonlinearities can be exploited to solve NP problems (and in fact harder problems) in polynomial time. This fact demonstrates clearly that computability and complexity are not purely mathematical matters. Because computation is inherently physical, fundamental physics is intertwined with fundamental computation theory. It also exposes the fact that there are hidden physical assumptions in the traditional theory of computation.

How could nonlinearities be exploited in quantum computation? Recall that quantum state vectors lie on the unit sphere and unitary transformations preserve "angles" (inner products) between vectors. Nonunitary transformations would, in effect, stretch the sphere, so the angles between vectors could change. Unitary transformations could be used to position the vectors to the correct position for subsequent nonunitary transformations. The following algorithm exploits a nonlinear operator to separate vectors that are initially close together.

E.2 Basic algorithm

The *Lyapunov exponent* λ describes the divergence of trajectories in a dynamical system. If $\Delta\theta(0)$ is the initial separation, then the separation after time t is given by $|\Delta\theta(t)| \approx e^{\lambda t}|\Delta\theta(0)|$. If $\lambda > 0$, the system is usually chaotic.

Suppose there is some nonlinear operation $\mathfrak{N}$ with a positive Lyapunov exponent over some finite region of the unit sphere. Further suppose we have an *oracle* $P : \mathbf{2}^n \to \mathbf{2}$. We want to determine if there is an $\mathbf{x}$ such that $P(\mathbf{x}) = 1$. Next suppose we are given a quantum gate array U_P as in

[21] This section is based on Daniel S. Abrams and Seth Lloyd (1998), "Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems." *Phys. Rev. Lett.* 81, 3992–3995 (1998), preprint available at `http://arxiv.org/abs/quant-ph/9801041v1`. See also Scott Aaronson, "NP-complete Problems and Physical Reality," *SIGACT News*, Complexity Theory Column, March 2005. `quant-ph/0502072`. `http://www.scottaaronson.com/papers/npcomplete.pdf` (accessed 2012-10-27).

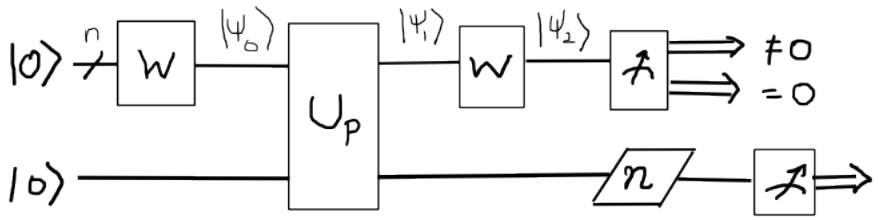

Figure III.39: Quantum circuit for Abrams-Lloyd algorithm. The first measurement produces **0** with probability greater than 1/4, but if it yields a nonzero state, we try again. The $\mathfrak{N}$ parallelogram represents a hypothetical nonlinear quantum state transformation, which may be repeated to yield a macroscopically observable separation of the solution and no-solution vectors.

Grover's algorithm. It is defined on a n-qubit data register and a 1-qubit result register. See Fig. III.39.

algorithm Abrams-Lloyd:

Step 1: As usual, apply the Walsh-Hadamard transform to a zero data register to get a superposition of all possible inputs:

$$|\psi_0\rangle = (W_n|\mathbf{0}\rangle)|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\mathbf{2}^n} |\mathbf{x}, 0\rangle.$$

Step 2 (apply oracle): Apply the oracle to get a superposition of input-output pairs:

$$|\psi_1\rangle = U_P|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\mathbf{2}^n} |\mathbf{x}, P(\mathbf{x})\rangle.$$

Step 3 (measure data register): First, apply the Walsh transformation to the data register to get:

$$|\psi_2\rangle \;\; = \;\; (W_n \otimes I)|\psi_1\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\mathbf{2}^n} (W_n|\mathbf{x}\rangle)|P(\mathbf{x})\rangle$$
$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\mathbf{2}^n} \left[\frac{1}{\sqrt{2^n}} \sum_{\mathbf{z}\in\mathbf{2}^n} (-)^{\mathbf{x}\cdot\mathbf{z}}|\mathbf{z}\rangle \right] |P(\mathbf{x})\rangle.$$

The last step applies by Eq. III.24 (p. 129). That is,

$$|\psi_2\rangle = \sum_{\mathbf{x}\in\mathbf{2}^n} \sum_{\mathbf{z}\in\mathbf{2}^n} \frac{1}{2^n}(-)^{\mathbf{x}\cdot\mathbf{z}}|\mathbf{z}\rangle|P(\mathbf{x})\rangle.$$

Separate out the state $\mathbf{z} = \mathbf{0}$ in order to see its amplitude:

$$\sum_{\mathbf{x}\in\mathbf{2}^n} \frac{1}{2^n}(-)^{\mathbf{x}\cdot\mathbf{0}}|\mathbf{0}\rangle|P(\mathbf{x})\rangle = \sum_{\mathbf{x}\in\mathbf{2}^n} \frac{1}{2^n}|\mathbf{0}\rangle|P(\mathbf{x})\rangle.$$

At least half of the 2^n vectors $\mathbf{x}$ must have the same value, $a = P(\mathbf{x})$ (since $P(\mathbf{x}) \in \mathbf{2}$). Therefore the amplitude of $|\mathbf{0}, a\rangle$ is at least $1/2$, and the probability of observing $|\mathbf{0}, a\rangle$ is at least $1/4$. We get a non-zero data register with probability $\leq 3/4$. (If we happen to observe $|\mathbf{x}_0, 1\rangle$, then of course we have our answer.)

In the case in which we get a zero data register, measurement of the data register yields the state:

$$|\psi_2\rangle \xrightarrow{\geq \frac{1}{4}} \mathcal{Z}^{-1}\left(\frac{s}{2^n}|\mathbf{0}\rangle|1\rangle + \frac{2^n - s}{2^n}|\mathbf{0}\rangle|0\rangle\right) = \mathcal{Z}^{-1}|\mathbf{0}\rangle\left(\frac{s}{2^n}|1\rangle + \frac{2^n - s}{2^n}|0\rangle\right),$$

where s is the number of solutions (the number of $\mathbf{x}$ such that $P(\mathbf{x}) = 1$) and $\mathcal{Z}^{-1}$ renormalizes after the state collapse.

The information we want is in the result qubit, but if s is small (as expected), then measurement will almost always yield $|0\rangle$. Recall what we did in Grover's algorithm. For $s \ll 2^n$, the vector $\mathcal{Z}^{-1}|\mathbf{0}\rangle\left(\frac{s}{2^n}|1\rangle + \frac{2^n-s}{2^n}|0\rangle\right)$ is very close to the vector $|\mathbf{0}, 0\rangle$. Therefore, we would like to drive them apart.

Step 4: Applying the nonlinear operator $\mathfrak{N}$ repeatedly will separate the vectors at an exponential rate. "[E]ventually, at a time determined by a polynomial function of the number of qubits n, the number of solutions s, and the rate of spreading (Lyapunov exponent) λ, the two cases will become

macroscopically distinguishable."

Step 5 (measure result register): Measure the result qubit. If the vectors have been sufficiently separated, there will be a significant probability of observing $|1\rangle$ in the $s \neq 0$ case.
□

If η is the angular extent of the nonlinear region, it might take $\mathcal{O}((\pi/\eta)^2)$ trials to get $|1\rangle$ with high probability. For large η, just one iteration might be sufficient.

E.3 Discussion of further results

The preceding algorithm depends on exponential precision, but Abrams and Lloyd present another algorithm that is robust against small errors. Each iteration doubles the number of components that have $|1\rangle$ in the result qubit, and after n iterations it yields a result with probability 1, and so the algorithm is linear.

Scott Aaronson has expressed doubts that the required nonlinear OR gate can be implemented. Abrams and Lloyd summarize: "We have demonstrated that nonlinear time evolution can in fact be exploited to allow a quantum computer to solve NP-complete and #P problems in polynomial time." (#P or "number-P" asks how many accepting paths in a NTM running in polynomial time. #P problems are at least as hard as corresponding NP problems.) Nevertheless, they continue, "we believe that quantum mechanics is in all likelihood exactly linear, and that the above conclusions might be viewed most profitably as further evidence that this is indeed the case."