Limitation on Effective Degree of Quantum Parallelism

Masataka Ohta

Email: mohta@necom830.hpcl.titech.ac.jp

Department of Computer Science, School of Information Science and Engineering

Tokyo Institute of Technology

2-12-1-W8-54, O-okayama, Meguro, Tokyo 1528552, JAPAN

Feb. 14, 2018

Abstract: Consider a binary quantum channel with binary states $|0\rangle$ and $|1\rangle$ as an output channel of some quantum computation device and assume that, if the channel is used as a classical binary channel where $|0\rangle$ and $|1\rangle$ represent bit values of 0 and 1, respectively, the channel has small error probability of p. Then, $|0\rangle$ transmitted over the channel will typically be $\sqrt{1-p}|0\rangle + e^{i\theta}\sqrt{p}|1\rangle$ $(0 \leq \theta < 2\pi)$. That is, error of the channel makes $|0\rangle$ and $\sqrt{1-p}|0\rangle + e^{i\theta}\sqrt{p}|1\rangle$ indistinguishable, which means different results of parallel execution of the device can't be represented by $|0\rangle$ and $\sqrt{1-p}|0\rangle + e^{i\theta}\sqrt{p}|1\rangle$. As representing N parallel binary results needs 2^N distinguishable states, effective degree of quantum parallelism of the device, which is defined as degree of parallelism of binary results with arbitrary small error probability by ideal encoding and ideal error correction, is limited by $\log_2(\pi/2\sqrt{p} + 1)$. That is, in practice, quantum computers are only as powerful as classical ones. Then, a brief introduction on modern communication technology over photons is provided to show that capacity of a binary quantum channel is almost twice better than quantum physicists had thought, that a classical state representing an entangled state exists and that "qubit" is a bad idea. Finally, it is shown that, without error caused by noise, ideal classical computers can be arbitrary fast.

I. INTRODUCION

In theory, quantum computers are believed to be more powerful than classical ones. For example, factorization of an integer is solved in polynomial (w.r.t. the number of digits of the integer) time by quantum computers [1], though, by practical classical computers, the best known algorism requires exponential time. It is essential that [1] use quantum parallelism. That is, a single computation step of a quantum device has quantum parallelism that exponentially many entangled terms are computed in parallel.

In practice, however, quantum devices suffer from error. Just as error of a classical channel limits capacity of the channel [2], error of a quantum device should limit effective degree of quantum parallelism by quantum superposition.

Consider a binary quantum channel with binary states $|0\rangle$ and $|1\rangle$ as an output channel of some quantum computation device and assume that, if the channel is used as a classical binary channel where $|0\rangle$ and $|1\rangle$ represent a bit value of 0 and 1 respectively, the channel has small error probability of p. Then, $|0\rangle$ transmitted over the channel will typically (those physicists not familiar with theory of Shannon can still understand "typical" as typical states of statistical mechanics) be $\sqrt{1-p}|0\rangle + e^{i\theta}\sqrt{p}|1\rangle$ $(0 \leq \theta < 2\pi)$. That is, error of the channel makes $|0\rangle$ and $\sqrt{1-p}|0\rangle + e^{i\theta}\sqrt{p}|1\rangle$ indistinguishable, which means different results of parallel execution of the device can't be represented by $|0\rangle$ and $\sqrt{1-p}|0\rangle + e^{i\theta}\sqrt{p}|1\rangle$, which is the essential part of Shannon Hartley theorem on capacity of analog channels. As entire quantum state is $\cos\varphi\,|0\rangle + e^{i\theta}\cos\varphi\,|1\rangle$ $(0 \leq \theta < 2\pi, 0 \leq \varphi < \pi)$, $\sin^{-1} p \sim p$, and as representing N parallel binary results needs 2^N distinguishable states, effective degree of quantum parallelism of the device, which is defined as degree of parallelism of binary results with arbitrary small error probability by ideal encoding and ideal error correction, is limited by $\log_2(\pi/2\sqrt{p}+1)$ (1 is added, because, even with large p, the entire state is distinguished as itself). , which is, not surprisingly, capacity of an analog channel with SNR of $\pi/2\sqrt{p}$. That is, in practice, quantum computers are only as powerful as classical ones.

While Quantum Threshold Theorem may reduce error doubly exponentially with exponential amount of hardware, because of exponential relationship between degree of parallelism and the number of distinguishable states, it only means exponential increase of degree of parallelism by exponential amount of hardware, which is no better than practical classical computers.

II. Brief Introduction on Modern Communication Technology over Photons

Radio waves as a solution of Maxwell's equations are transvers waves having two polarization modes, amplitude and phase of which can be controlled independently. Degree of freedom by quantum superposition of binary quantum states, in classical context, merely means relative amplitude and relative phase between two polarization modes.

However, as signals of two polarization modes are easily mixed during transmission, for example, by reflections, it was difficult to extract capacity of both modes, except for direct sight communications such as communications between a satellite and ground stations, where right and left circular polarization states can be separated by properly designed anntenas. Still, information has been encoded in absolute amplitude and phase as relative variation of amplitude and phase in time traditionally as analog AM (Amplitude Modulation) and PM (Phase Modulation) radio waves. With modern digital communication technology, short sequence of symbols with known amplitude and phase, which is called preamble or training sequence, is used as a delimiter between bytes or packets and reference amplitude and phase. Long term phase reference is maintained by LO (Local Oscillator) usually controlled by PLL (Phase

Locked Loop).

Thanks to Moore's law, which predicts semiconductor circuit size can be scaled down twice in every 18 months, and Denard's scaling law, which means speed of semiconductor circuit doubles if size and driving voltage is scaled down twice, it becomes practical to use DSPs (Digital Signal Processers) to restore original signals transmitted over multiple interfering channels using preambles as reference to estimate how signals in the channels interfere, which is called MIMO (Multiple Input and Multiple Output), special case of which is PDM (Polarization Division Multiplexing). MIMO is extensively used in 4G and Wifi.

With PDM, modern communication technology utilizes both relative and absolute amplitude and phase of a binary quantum state, which is twice more capacity than quantum superposition save capacity consumed by preambles.

As Moore's law further evolve, it is now possible to use PDM for optical signals over optical fibers, which is practically used in some 100G Ethernet implementations. As infrared photons over optical fibers has more energy than radio wave photons and power saving is of important concern, the number of photons consisting a symbol to achieve certain raw (that is, before error correction) error rate is minimized by taking into consideration quantum fluctuations as quantum noise such as shot noise.

Then, consider two binary quantum states. Can entanglement introduce new degree of freedom not available to classical channels? Disappointingly, it is merely that degree of freedom by entanglement of two binary states is freedom of absolute amplitude and phase of the second state as relative amplitude and phase relative to those of the first state. As such, an entangled state can be represented as a classical state of two classical channels. By representing $|0\rangle$ and $|1\rangle$ as classical states of vertical and horizontal polarization, $|00\rangle$ and $|11\rangle$ corresponds to classical state of both channels vertically polarized and horizontally polarized, respectively. Thus, $|00\rangle+|11\rangle$ corresponds to classical state of both channels diagonally polarized, which is classical superposition of horizontal and vertical polarization with same phase. Interestingly, $|01\rangle+|10\rangle$ is represented by the same classical state, implications of which is discussed in a separate paper [ENT].

Now, as a binary quantum state can carry information by four real numbers of absolute and relative amplitude and phase, it is obviously improper to call it "qubit". Moreover, even if we use only two states of $|0\rangle$ and $|1\rangle$, it is still inappropriate to call it "qubit", as we may use a symbol with $\{|00\rangle, |10\rangle, |11\rangle\}$ excluding $|01\rangle$, in which case, while $\log_2 3$ bits may be encoded in the symbol, we can't count the number of bits encoded by each "qubit". Information is represented by symbols, not by partial states consisting the symbols.

III. Classical Computers can be Arbitrary Fast

As ideal noiseless classical computers are not annoyed by quantum effects such as size of atoms, which limits machining accuracy, or a unit of electric charge, which limits minimum current through shot noise, there is no limitation to apply Moore's law and Denard's scaling law, which means ideal noiseless classical computers can be arbitrary fast.

IV. CONCLUSIONS

As noise of practical quantum devices limits effective degree of quantum parallelism of the device, it is practically impossible to make quantum computers more powerful than classical ones.

Computer scientists, including the Author, must concentrate on making classical computers faster, less power consuming with wider von Neumann bottlenecks.

But, first of all, let's celebrate 100th birthday of Shannon, if it is not too late [100th]

REFERENCES

[1] P. W. Shor, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994, p. 124.

[2] C. E. Shannon, in Proceedings of IRE, 37 (1), 1949, p. 10–21.

[3] S. Lloyd, Phys. Rev. A55 (1997) 1613, arXiv:quant-ph/9604015.

[4] D. Aharonov, M. Ben-Or, arXiv:quant-ph/9906129.

[MOORE]

[DENARD]

[ENT] M. Ohta, To Appear

[100th] https://www.ieeefoundation.org/ClaudeShannon