

Stochastic Computing on Quantum Gates

Yoshito Kanamori

Abstract— The concept of Stochastic Computing is applied to Quantum Computing. A qubit in a superposition state is used to represent a probability as an input for Stochastic Computation, instead of a random bit stream. Measuring the output qubit from the quantum circuit produces zero or one with the probability of the computation result. This process is repeated N times to generate the N -bit stochastic number, where N is determined by the required accuracy.

PROBLEM AND MOTIVATION

Error in the quantum circuit is a serious obstacle especially for the development of the large-scale quantum computers. This paper proposes a probability calculation method with quantum circuits by utilizing the concept of stochastic computing. Instead of correcting errors in the quantum circuit, our approach is to improve the accuracy of computation by increasing the number of bits in the output stochastic number. This proposed method can also relax the constraint of stochastic computing by reducing the effect of the inherent variance in generating the random bit streams and in estimating the values of the computation results.

BACKGROUND & RELATED LITERATURE

Quantum computing [1] is one of the most promising technologies. Many universities and research institutes have been competing for quantum computing research and development. D-Wave makes their Ising model based quantum computer commercially available [2]. IBM makes their quantum gate based 5-qubit and 20-qubit superconducting quantum computer available in public via their cloud service called “IBM Q Experience” [3][4]. It seems that the time has come for researchers who are not necessary physicists to use a quantum computer and to develop new algorithms and applications for the quantum computers.

Stochastic computing (SC)[5] is the unconventional method of calculations by processing random bit streams on the conventional Boolean logic gate. SC has drawn attention from the researchers in the field of image processing[6], [7] and deep neural network [8], which needs more computational speed over accuracy in general. SC also can reduce computation hardware area and power consumption. For example, Stochastic Low-density parity-check (LDPC) decoders have been proposed and continuously improved over the last decade. [9]–[11]. Those decoders utilize SC to reduce the additional space in the circuits and processing power to perform the LDPC decoding operations.

In SC, a stochastic number generator (SNG) converts binary numbers to random N bit-streams, called stochastic number, prior to the computation. Although there are several formats to interpret the bit streams [12], the unipolar format is used in this paper for simplicity. In the unipolar format where the number range is $[0,1]$, the stochastic number S is interpreted as the probability p determined by the frequency of 1’s in the N -bit stream.

For instance, a multiplication of probabilities: $p_c = p_A * p_B$ can be performed by a single AND gate with two bit-streams. In Fig.1, the stochastic numbers for the input bit-streams S_A and S_B represent the probabilities $p_A = 4/8$ and $p_B = 4/8$. The output bit stream S_C (i.e., 00001100) represents $p_c = 2/8$. Similarly, a scaled adder can be made with a multiplexer and the other arithmetic operations have been proposed [13].

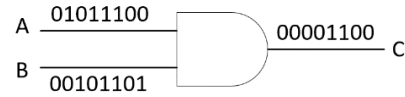


Fig. 1: AND gate as a stochastic multiplier

SC can also provide better fault tolerance than other classical computing techniques. For example, when a bit flip occurs near the most significant bit in a binary data, the result of the binary calculation is significantly changed by the error. However, a bit-flip in a stochastic number does not notably affect the computation result regardless of its position in the stochastic number because the stochastic number becomes $(n \pm 1)/N$ with a bit-flip error, which can be ignored when N is large enough. (n is the number of 1s in the N -bit stochastic number.)

Challenges in Stochastic Computing

One of the serious limitations of SC is that the result from a stochastic computation is the approximate value of the intended computation result. For example, if the stochastic number is $S_A = 01011010$ ($p_A = 4/8$) in Fig.1, the output bit stream becomes $S_C = 00001000$ ($p_c = 1/8$, instead of $2/8$). If S_A and S_B happened to be a same bit sequence (e.g., in the circuits with feedback and feed-back logics), the bit stream S_C would be always 00000000. These simple examples indicate that the stochastic computation intrinsically introduces errors in the form of random variance in the stochastic numbers and the computation results.

Also, a typical SNG, which converts a binary number to a random bit stream, utilizes a random source (e.g., LFSR). As a result, the stochastic number generated by the SNG is the estimated value $\hat{p}$ of the target value p over N samples [14]. For example, in Fig. 1, the bit stream S_A from a SNG for p_A may not have four 1’s in the 8-bit stream occasionally. Therefore, as the number of inputs and levels of logic gates in the circuit increases, the computation result becomes more inaccurate.

• The author is with Department of Information Systems and Decision Sciences, University of Alaska Anchorage, 3211 Providence Drive, Anchorage, AK 99508, E-mail: ykanamori@alaska.edu.

APPROACH & UNIQUENESS

The problem mentioned in the previous section occurs because of the randomness in the input bit streams used in the computation. This paper proposes the use of a quantum superposition state [1] instead of a random bit stream to represent a probability p . Those prepared qubits are placed into a quantum circuit as the inputs. The output qubit is measured to observe zero or one with the probability of the calculation result. This will be repeated N times to generate the N -bit stochastic number for the estimated value $\hat{p}_{out}$ of the intended computation result p_{out} .

Definitions

Most quantum circuits perform digital computations by using quantum bits (called qubits). A qubit has two possible states $|0\rangle = [1,0]^T$ and $|1\rangle = [0,1]^T$ corresponding to the state 0 and 1 for a classical bit and is represented as a unit vector in a two-dimensional complex vector space

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = [\alpha, \beta]^T,$$

where the number α and β are complex numbers and satisfy $|\alpha|^2 + |\beta|^2 = 1$. The orthonormal basis $|0\rangle$ and $|1\rangle$ may correspond to the spin states of an electron (i.e., spin-up and spin-down) and the polarizations of a photon (i.e., vertical and horizontal orientations). The qubit is measured to read out the information (i.e., $|0\rangle$ and $|1\rangle$) in the qubit. When a qubit is measured, the measurement changes the state of the qubit to one of the two basis states. The probability of observing the state $|0\rangle$ after the measurement is $|\alpha|^2$ while the probability of obtaining $|1\rangle$ is $|\beta|^2$. When the two basis states and a rotation operator $R(\gamma)$ are defined in the Bloch sphere [1], the state $|\psi\rangle = |0\rangle$ can be transformed to $|\psi\rangle = |1\rangle$ by rotating the state $|0\rangle$ by $\gamma = \pi$. These notations may be convenient to imagine the orientation of the spins in positive ($|\uparrow\rangle = |0\rangle$) or negative ($|\downarrow\rangle = |1\rangle$) z -direction in the Bloch sphere. When an arbitrary phase angle θ $\{\theta \in [0, \pi/2], \theta = \gamma/2\}$ is defined, the rotation matrix can be represented as

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$

which is the same as the Jones matrix in Optics [15]. This notation may be convenient to imagine the orientation of the photons in vertical ($|\uparrow\rangle = |0\rangle$) or horizontal ($|\leftrightarrow\rangle = |1\rangle$) direction. This paper uses $R(\theta)$ to simplify the expressions.

N qubits in the state $|0\rangle$ can be written as

$$\begin{aligned} |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_i\rangle \otimes \dots \otimes |\psi_N\rangle \\ = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes \dots \otimes |0\rangle \end{aligned}$$

where $\otimes$ indicates a tensor product and $i = 1, 2, 3, \dots, N$. After the initial state of a qubit $|\psi_i\rangle = |0\rangle$ is rotated by θ_i , the state is written as

$$|\psi_i\rangle = R(\theta_i)|0\rangle = \cos\theta_i|0\rangle + \sin\theta_i|1\rangle.$$

The probability of obtaining $|\psi_i\rangle = |1\rangle$ and $|\psi_i\rangle = |0\rangle$ after the measurement are

$$\begin{aligned} P(|\psi_i\rangle = |1\rangle) &= |\sin\theta_i|^2 = \sin^2\theta_i = p_i \\ P(|\psi_i\rangle = |0\rangle) &= |\cos\theta_i|^2 = \cos^2\theta_i = 1 - p_i \end{aligned}$$

Example:

This example shows a multiplication of probabilities: $p_c = p_A * p_B$ on a quantum circuit. Quantum AND gate can be implemented with a controlled-controlled-NOT (ccNOT) gate[1].

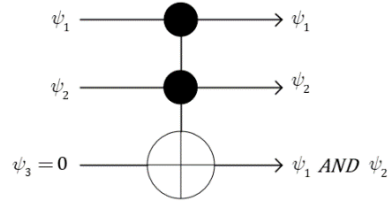


Fig. 2: AND gate in a quantum circuit

The ccNOT operator is represented as

$$\begin{aligned} U_{ccnot} = U_{AND} &= |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I \\ &+ |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes X \end{aligned}$$

θ_1 and θ_2 are chosen to satisfy $p_1 = |\sin\theta_1|^2$ and $p_2 = |\sin\theta_2|^2$ ($p_1 \in [0,1], p_2 \in [0,1]$), accordingly. Then, rotate $|\psi_1\rangle$ and $|\psi_2\rangle$ by θ_1 and θ_2 respectively, and place them into the AND gate as the inputs.

$$|\Psi_{in}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle = R(\theta_1)|0\rangle \otimes R(\theta_2)|0\rangle \otimes |0\rangle$$

$$|\Psi_{out}\rangle = U_{AND}|\Psi_{in}\rangle$$

$$\begin{aligned} &= [\cos\theta_1\cos\theta_2, 0, -\cos\theta_1\sin\theta_2, 0, -\sin\theta_1\cos\theta_2, 0, 0, \sin\theta_1\sin\theta_2]^T \\ &= \cos\theta_1\cos\theta_2|000\rangle - \cos\theta_1\sin\theta_2|010\rangle \\ &\quad - \sin\theta_1\cos\theta_2|100\rangle + \sin\theta_1\sin\theta_2|111\rangle \end{aligned}$$

When the $|\psi_3\rangle$ is measured after the ccNOT gate, $|\psi_3\rangle = |1\rangle$ can be observed with the probability

$$p_3 = |\sin\theta_1\sin\theta_2|^2 = p_1 \times p_2.$$

This process is repeated N times to get the stochastic number. The computation result $\hat{p}_3$ is obtained by counting the number of 1's in the N -bit measurement result.

RISK & CONTRIBUTION

With currently available technologies, each quantum gate and each rotation of qubit cause errors in quantum circuits. However, the proposed approach can make the size of the quantum circuit smaller to reduce the errors in the calculation for certain applications (e.g., for approximate computations [16].)

Unlike SC on classical circuits, the fun-out and feed-back logics in a circuit do not affect the result of the computation with the proposed method. Moreover, the number of inputs and levels of logic gates in the circuit does not increase the inaccuracy of the computation in theory. Also, an additional circuit for SNG is not necessary for the proposed method. When an application needs more accurate results, the accuracy of the result can be improved by increasing the number N of measurements on the output qubit.

Although this paper shows only one example due to the page limit, any classical logic gate can be replicated with quantum gates in theory. Therefore, any classical circuits proposed in SC can be implemented with the proposed method.

REFERENCES

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniv. Cambridge University Press, 2010.
- [2] E. Gibney, "D-Wave upgrade: How scientists are using the world's most controversial quantum computer," *Nature*, vol. 541, no. 7638, pp. 447–448, 2017.
- [3] IBM, "IBM Q Experience." [Online]. Available: <https://quantumexperience.ng.bluemix.net/qx/experience>. [Accessed: 13-May-2018].
- [4] D. Castelvecchi, "IBM's quantum cloud computer goes commercial," *Nature*, vol. 543, no. 7644, p. 159, Mar. 2017.
- [5] A. Alaghi and J. P. Hayes, "Survey of Stochastic Computing," *ACM Trans. Embed. Comput. Syst.*, vol. 12, no. 2s, pp. 1–19, May 2013.
- [6] P. Li, D. J. Lilja, W. Qian, K. Bazargan, and M. D. Riedel, "Computation on Stochastic Bit Streams Digital Image Processing Case Studies," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 22, no. 3, pp. 449–462, Mar. 2014.
- [7] B. Moons and M. Verhelst, "Energy-Efficiency and Accuracy of Stochastic Computing Circuits in Emerging Technologies," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, vol. 4, no. 4, pp. 475–486, Dec. 2014.
- [8] Y. Xie, S. Liao, B. Yuan, Y. Wang, and Z. Wang, "Fully-Parallel Area-Efficient Deep Neural Network Design Using Stochastic Computing," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 64, no. 12, pp. 1382–1386, Dec. 2017.
- [9] X.-R. Lee, C.-L. Chen, H.-C. Chang, and C.-Y. Lee, "A 7.92 Gb/s 437.2 mW Stochastic LDPC Decoder Chip for IEEE 802.15.3c Applications," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 62, no. 2, pp. 507–516, Feb. 2015.
- [10] D. Wu, Y. Chen, Q. Zhang, Y. Ueng, and X. Zeng, "Strategies for Reducing Decoding Cycles in Stochastic LDPC Decoders," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 63, no. 9, pp. 873–877, Sep. 2016.
- [11] Y.-L. Ueng, C.-Y. Wang, and M.-R. Li, "An Efficient Combined Bit-Flipping and Stochastic LDPC Decoder Using Improved Probability Tracers," *IEEE Trans. Signal Process.*, vol. 65, no. 20, pp. 5368–5380, Oct. 2017.
- [12] B. R. Gaines, "Stochastic Computing Systems," in *Advances in Information Systems Science*, Tou J.T., Ed. Boston, MA: Springer US, 1969, pp. 37–172.
- [13] B. D. Brown and H. C. Card, "Stochastic neural computation. I. Computational elements," *IEEE Trans. Comput.*, vol. 50, no. 9, pp. 891–905, 2001.
- [14] A. Alaghi, W. Qian, and J. P. Hayes, "The Promise and Challenge of Stochastic Computing," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, pp. 1–1, 2017.
- [15] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics*. John Wiley & Sons, Inc, 1991.
- [16] T. Moreau *et al.*, "A Taxonomy of General Purpose Approximate Computing Techniques," *IEEE Embed. Syst. Lett.*, vol. 10, no. 1, pp. 2–5, Mar. 2018.