An experimental quantum Bernoulli factory

Raj B. Patel[1], Terry Rudolph[2], and Geoff J. Pryde[1]

1. Centre for Quantum Computation and Communication Technology (Australian Research Council), Centre for Quantum Dynamics, Griffith University, Brisbane, QLD 4111, Australia
2. Department of Physics, Imperial College London, Prince Consort Road, London SW7 2AZ, UK.
Author e-mail address: r.patel@griffith.edu.au

In the current absence of full-scale quantum technologies, there has been a concerted effort to prove that a quantum advantage exists across a range information protocols from precision measurement, computation and simulation to secure communications. Recently an area in which a quantum advantage has been revealed is randomness processing which is exemplified in the Bernoulli factory[1].

The Bernoulli factory is an algorithm which takes, as an input, a finite sequence of independent and identically distributed Bernoulli random variables, or coin flips, with an unknown bias *p* and then outputs a new function given by coin with success probability *f(p)*. An early example, attributed to von Neumann[2], is the generation of a fair coin $f(p)=0.5$ from biased coins for $0<p<1$. The coin is flipped twice, if both outcomes are different output the result of the second coin, otherwise repeat. Another example is the case where $f(p)=2p(1-p)^2$ for which a heads outcome can be simulated when three *p* coins are tossed and either tails/tails/heads or tails/heads/tails are the outcomes, otherwise tails is outputted by the factory. The types of functions simulable by a Bernoulli factory using classical coins of unknown bias *p* was first defined by Keane and O'Brien[1]. A function that cannot be simulated classically with finite resources, but which is of great interest as it may lead to the construction of other Bernoulli factories[3], is $f_{\wedge}(p)=2p$.

Recent developments to the theory by Dale *et al.*[4] showed that replacing classical coins with quantum coins or 'quoins' of the form $|p\rangle=\sqrt{p}|0\rangle+\sqrt{1-p}|1\rangle$ not only relaxes the conditions on which functions can be simulated, but also provides a reduction in the number of resources required. Here we report an experimental demonstration of the quantum Bernoulli factory by simulating the function $f_{\wedge}(p)=2p$ under two scenarios, one which utilises single qubit measurements in the X and Z basis[5] and the other which utilises non-classical correlations by performing joint measurements of two qubits in the Bell basis[4]. Qubits given by $|p\rangle=\sqrt{p}|0\rangle+\sqrt{1-p}|1\rangle$ are encoded in the polarisation of single-photons generated from spontaneous parametric downconversion. The exact sequence of measurement outcomes is recorded by time-tagging individual detection events. Sampling from the measurement outcomes, along with classical post-processing, allows $f_{\wedge}(p)$ to be constructed. For both approaches, we are able to achieve $f_{\wedge}(0.5)=0.935$ where we attribute the slight deviation from unity to experimental imperfections. Our experiments reveal that for the single-qubit case, $f_{\wedge}(p)=2p$ requires on average 51.6 quoins to construct compared to 11.3 quoins in the two-qubit case, demonstrating that non-classical correlations offer almost a five-fold reduction in resources over single-qubit measurements alone. Fitting the data with a sum of Bernstein polynomials[6] allows us to estimate that ~50000 classical coins would be required to reproduce our data, which shows that the quantum Bernoulli factory, with a resource reduction of three orders of magnitude, shows a clear quantum advantage over the best known classical algorithm.

[1] Keane, M. S. & O'Brien., G. L., "A Bernoulli factory". ACM Trans. Model. Comput. Simul. 4, 213–219 (1994).

[2] Von Neumann, J., "Various techniques used in connection with random digits". Appl. Math Ser. 12, 36–38 (1951).

[3] Nacu, S. & Peres, Y., "Fast simulation of new coins from old". Ann. Appl. Probab. 15, 93–115 (2005).

[4] Dale, H. et al. Provable, "Quantum Advantage in Randomness Processing". Nat. Commun. 6:8203 doi: 10.1038/ncomms9203 (2015).

[5] X. Yuan, "Experimental Quantum Randomness Processing Using Superconducting Qubits". Phys. Rev. Letts. 117, 010502 (2016)

[6] M. Huber, "Nearly Optimal Bernoulli Factories for Linear Functions". Combinatorics, Probability and Computing. 25, 577–591, (2016)