Evaluating NISQ Devices with Quadratic Nonresidues

Thomas G. Draper

Center for Communications Research at La Jolla

An unsolved problem since Gauss

Quadratic nonresidue problem (QNR):

Given a prime $p \equiv 1 \bmod 8$, find a y such that $x^2 \equiv y \bmod p$ has no solution.

Question: Is QNR in P?

Gauss [1] proved the first nontrivial upper bound for the least quadratic nonresidue showing that $y < 2\sqrt{p} + 1$. Current best analytic tools prove that $y < C \cdot p^{\alpha}$ for a non-zero α [2, p. 33].

QNR is in EQP$_{\mathbb{C}}$

Given $p \equiv 1 \bmod 8$, choose least n where $p < 2^n = N$. Let $\theta = \arccos\left(1 - \frac{2^n}{p-1}\right)$, and $f(x) = \left[\left(\frac{x}{p}\right) = -1 \text{ and } 0 \le x < p\right]$.

$[O(n)]$ Apply $H^{\otimes n}$ to $|0\rangle^{\otimes n}$ (Hadamard transform).

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

$[O(n \log^2 n)]$ Compute Jacobi symbol indicator [3, 4].

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \left| \left[\left(\frac{x}{p}\right) = -1\right] \right\rangle$$

$[O(n)]$ Compute $[x < p]$ indicator [5].

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \left| \left[\left(\frac{x}{p}\right) = -1\right] \right\rangle |[x < p]\rangle$$

$[O(1)]$ Rotate odd QNRs less than p by -2θ.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-i2\theta f(x) x_0} |x\rangle \left| \left[\left(\frac{x}{p}\right) = -1\right] \right\rangle |[x < p]\rangle$$

$[O(1)]$ Rotate all QNRs less than p by θ.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i\theta f(x)(1-2x_0)} |x\rangle \left| \left[\left(\frac{x}{p}\right) = -1\right] \right\rangle |[x < p]\rangle$$

$[O(n \log^2 n)]$ Uncompute indicator functions.

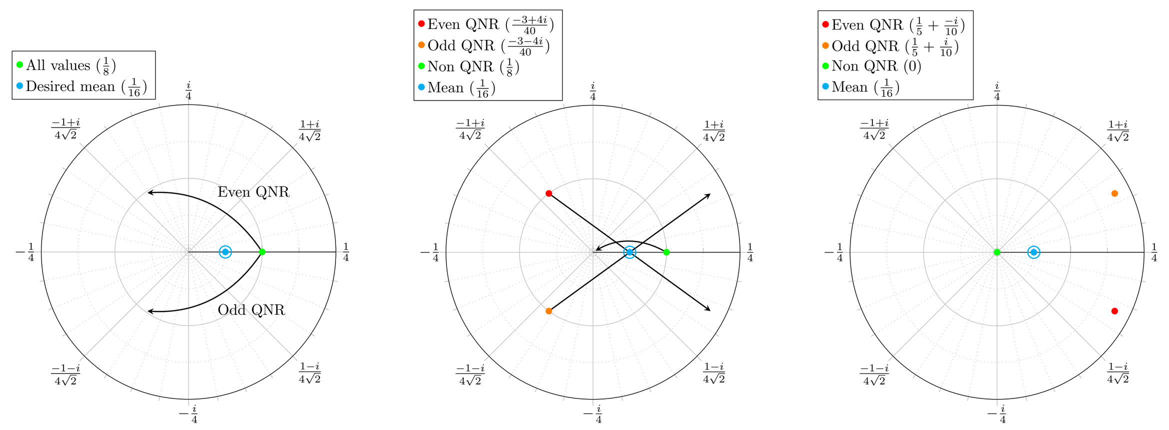
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i\theta f(x)(1-2x_0)} |x\rangle$$

$[O(n)]$ Use a Grover step to invert about the mean $\alpha = \frac{1}{2\sqrt{N}}$.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \left(1 - e^{i\theta f(x)(1-2x_0)}\right) |x\rangle$$

$[O(n)]$ Observe a quadratic nonresidue modulo p.

Phase inversion in the QNR algorithm



Amplitude values for Quadratic Nonresidues for $p = 41$

Creating a NISQ test from the QNR algorithm

Using a single Jacobi symbol calculation, a quantum computer can find a QNR 100% of the time, whereas a classical computer can only succeed 75% of the time.

Even if we want to argue for a different classical bound, without a mathematical breakthrough, the provable success rate of any algorithm in P will always be less than 100%.

The QNR algorithm evaluates two NISQ properties:

- The rate of success.
- The uniformity of the observations.

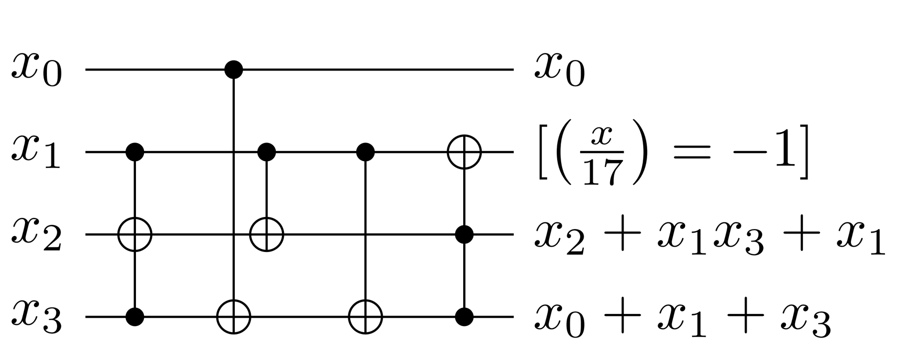
Jacobi symbol permutation for $p = 17$

For Fermat primes ($p = 2^{2^n} + 1$), the inequality indicator $[p < x]$, and be left out since there are only 2^{2^n} nonzero residues.

Additionally, a permutation of $0, 1, \ldots, 2^{2^n} - 1$ exists where one of the output wires is the parity bit, and another is the indicator function for the Jacobi symbol.

$$\left[\left(\frac{x}{17}\right) = -1\right] = x_0x_1 + x_0x_2 + x_1x_2 + x_1x_3 + x_2x_3 + x_0x_1x_3$$

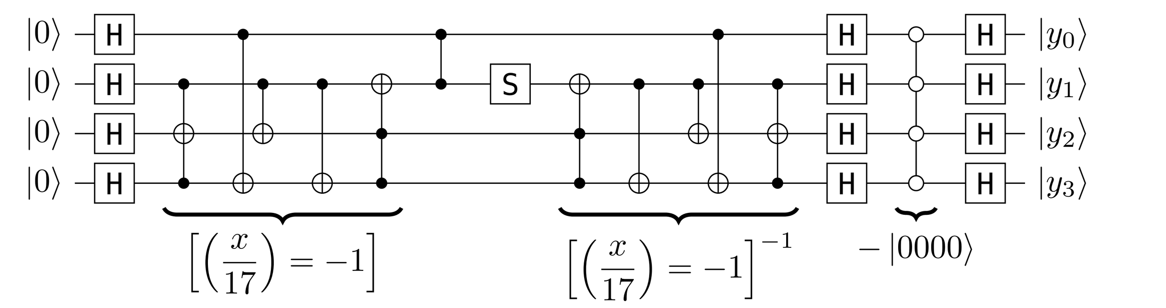
Indicator permutation for $p = 17$



Ideally, the Jacobi symbol circuit should be derived from an algorithm, and not by computer search. Given the current shortcomings of current NISQ devices, a full algorithm, even at the $p = 17$ level is hard to distinguish from random.

As NISQ devices improve, a full algorithmic test for $p = 17$ will be meaningful. The next tests of interest will likely be $p = 41$ and $p = 257$.

Basic QNR circuit for $p = 17$



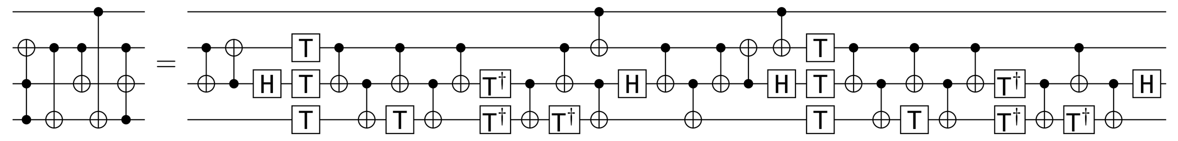
Transpiled subcircuits

Two properties are required circuit to run on all of the tested NISQ devices:

- Only single qubit gates and CNOTs.
- All CNOTs are nearest neighbor.

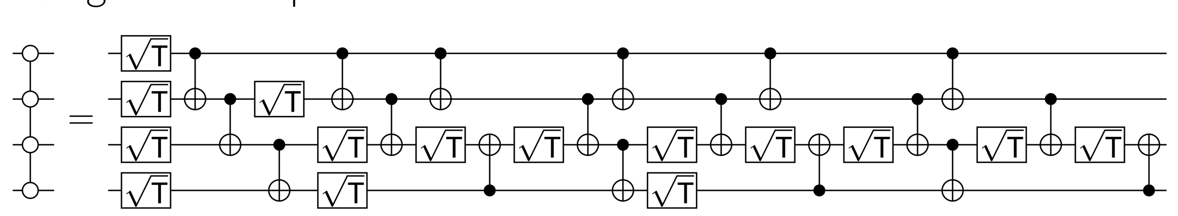
Inverse indicator permutation decomposition

Since a CNOT or CCNOT targeting a $|+\rangle$ does nothing, the entire forward pass of the indicator permutation can be removed. The backwards pass was constructed using ideas from Gidney [6].



Grover gate decomposition

A new method was discovered to flip the $|0000\rangle$ state without using an extra qubit.



QNR test advantages

- Implementation agnostic
- Infinite tests
- Ease of execution
- Better comparison

References

[1] Carl Friedrich Gauss, *Disquisitones arithmeticae*, 1801.

[2] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

[3] D. Harvey, J. Van Der Hoeven, *Integer multiplication in time $O(n \log n)$*, Annals of Mathematics, Princeton University, Department of Mathematics, 2020.

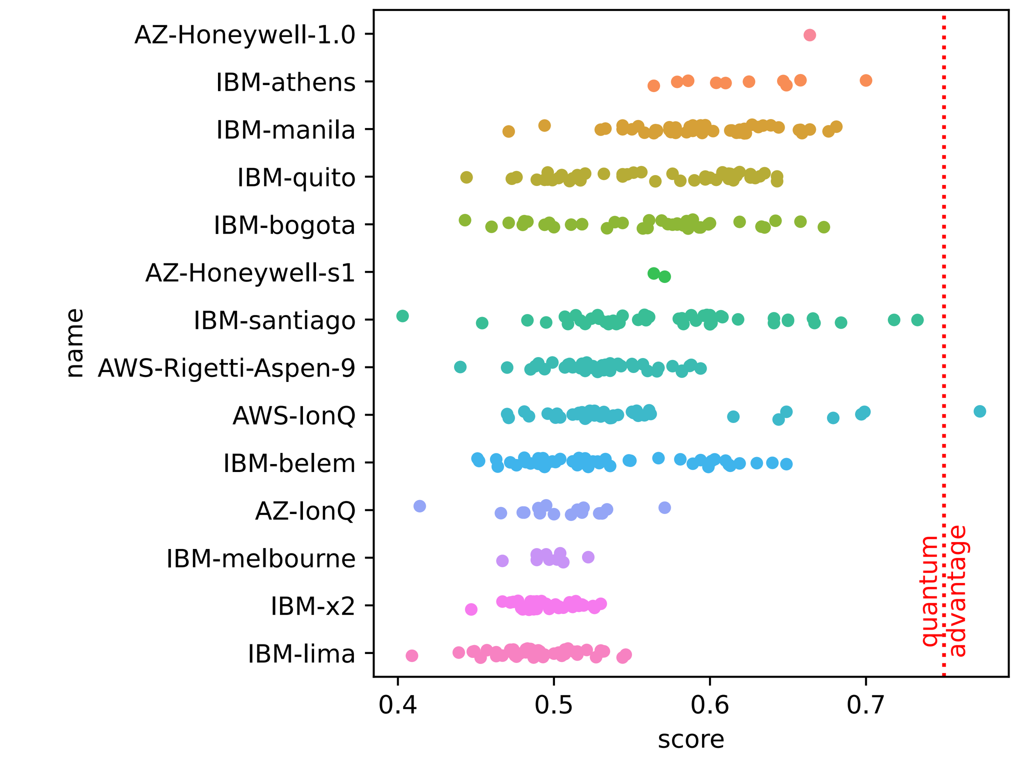
[4] R. P. Brent and P. Zimmerman, *An $O(M(n) \log n)$ algorithm for the Jacobi symbol*, CoRR, 2010.

[5] D. Oliveira, R. Ramos,*Quantum bit string comparator: Circuits and applications*, Quantum Computers and Computing, Vol.7, 2007.

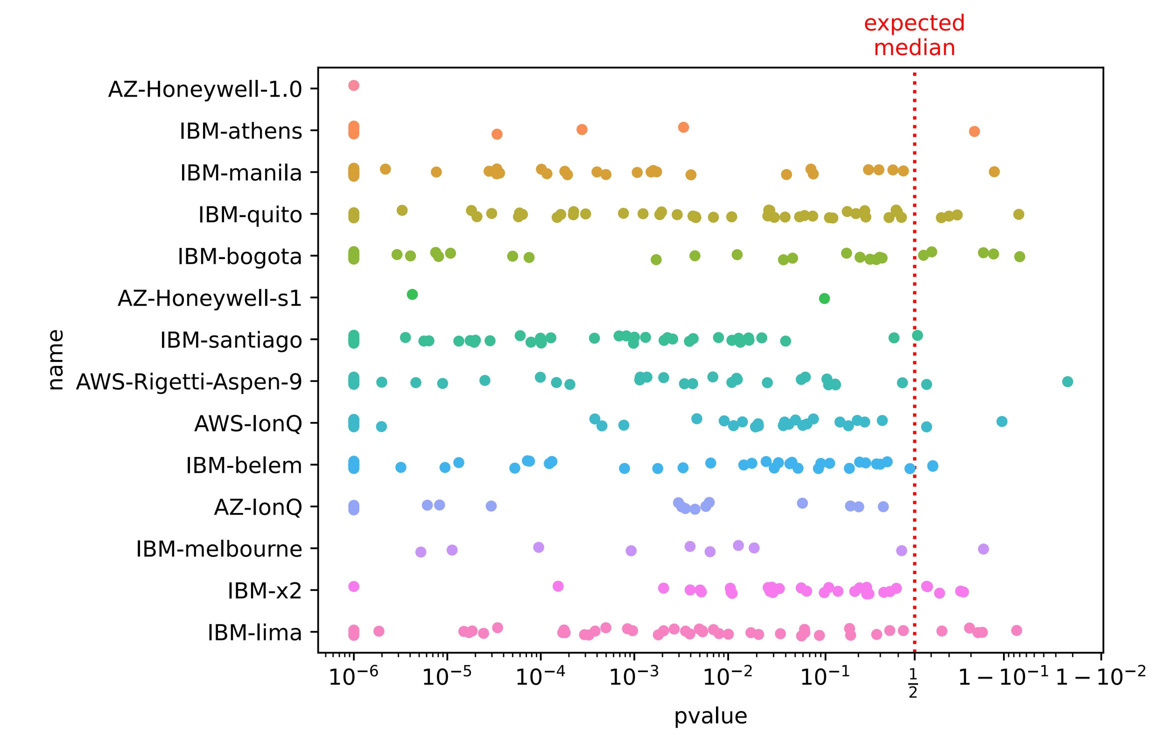
[6] C. Gidney, *Minimum number of CNOTs for Toffoli with non-adjacent controls (answer:3964)*, https://quantumcomputing.stackexchange.com, 2018.

Test results for $p = 17$ (Jun-Aug 2021)

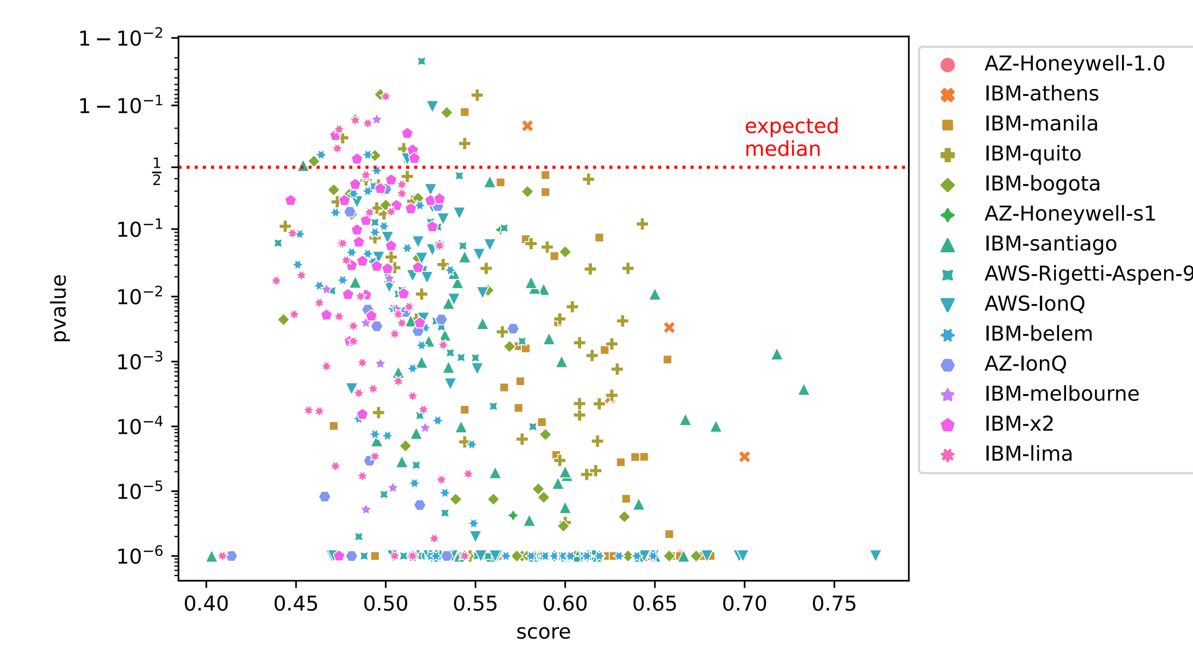
Success rates of 1000 shot runs



p-values of uniformity test for 1000 shot runs



Success rate vs. p-value



QNR17 Test