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$_{\mathbb{C}}$

We prove a new result showing a quantum computer can solve QNR in quantum P.

Given $p \equiv 1 \bmod 8$, choose the smallest n such that $p < 2^n = N$. 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.

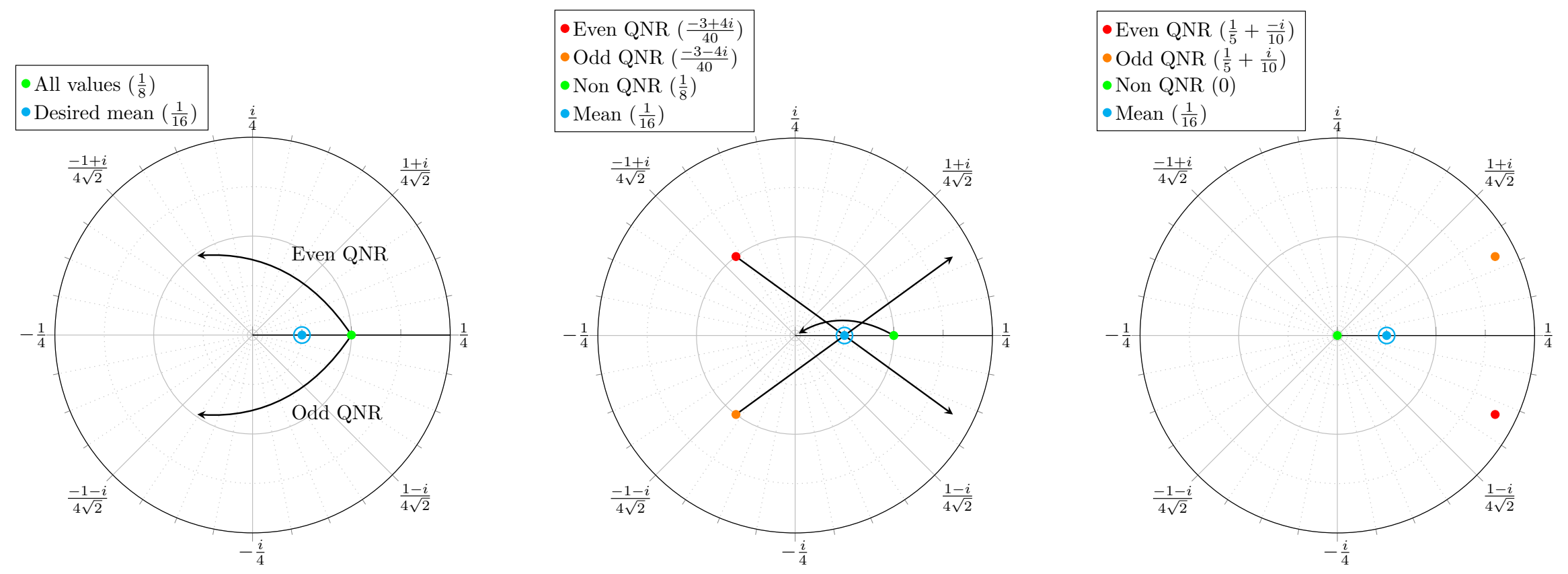
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i\theta f(x)(1-2x_0)} |x\rangle$$

$[O(n)]$ 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



Quadratic nonresidue amplitude progression for $p = 41$

Creating a NISQ test from the QNR algorithm

A quantum computer can create a probability distribution exclusively over quadratic nonresidues in polynomial time.

A classical algorithm capable of the same would be a mathematical breakthrough.

Using a single Jacobi symbol calculation, a quantum computer can find a QNR 100% of the time, whereas the classical computer success rate is bounded away from 1.

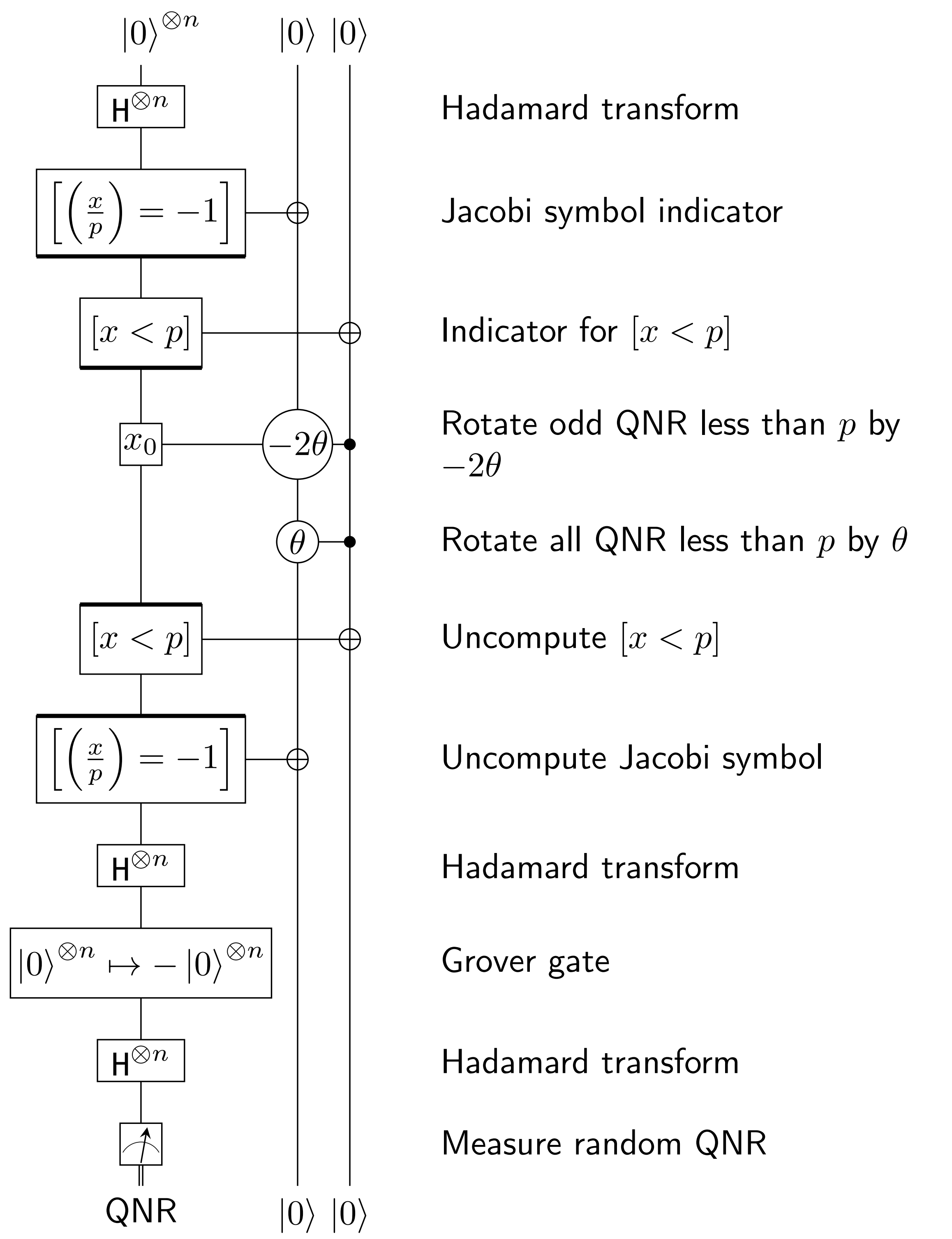
The QNR algorithm evaluates two NISQ properties:

- The rate of success
- The uniformity of the observations

QNR Test Advantages:

- Math inspired and implementation agnostic
- Infinite tests with $O(n \log^2 n)$ runtime
- Smallest tests are usable now
- Scores algorithmic success instead of a physical property

General QNR algorithm



Hadamard transform

Jacobi symbol indicator

Indicator for $[x < p]$

Rotate odd QNR less than p by -2θ

Rotate all QNR less than p by θ

Uncompute $[x < p]$

Uncompute Jacobi symbol

Hadamard transform

Grover gate

Hadamard transform

Measure random QNR

Note than when $p = 2^n + 1$, the inequality indicator $[x < p]$ can be left out since there are exactly 2^n nonzero residues. Additionally, since exactly half of the values less than 2^n will be nonresidues, a permutation of $0, 1, \ldots, 2^n - 1$ will exist where one of the output wires is the parity bit, and another is the indicator function for the Jacobi symbol. This only happens for Fermat primes where $p = 2^{2^m} + 1$.

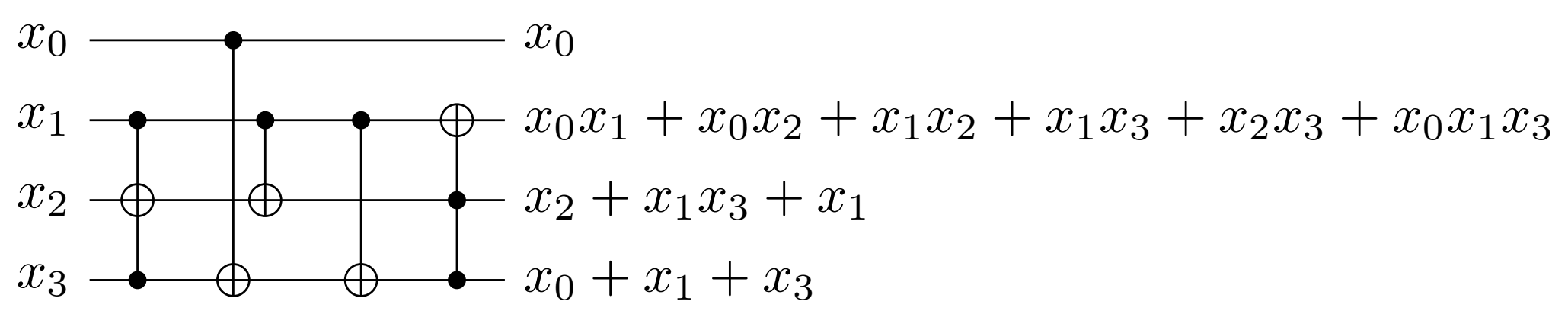
What can we test now?

Design a QNR test circuit for $p = 17$

Since $p = 17$ is a Fermat prime, the Jacobi symbol indicator is balanced.

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

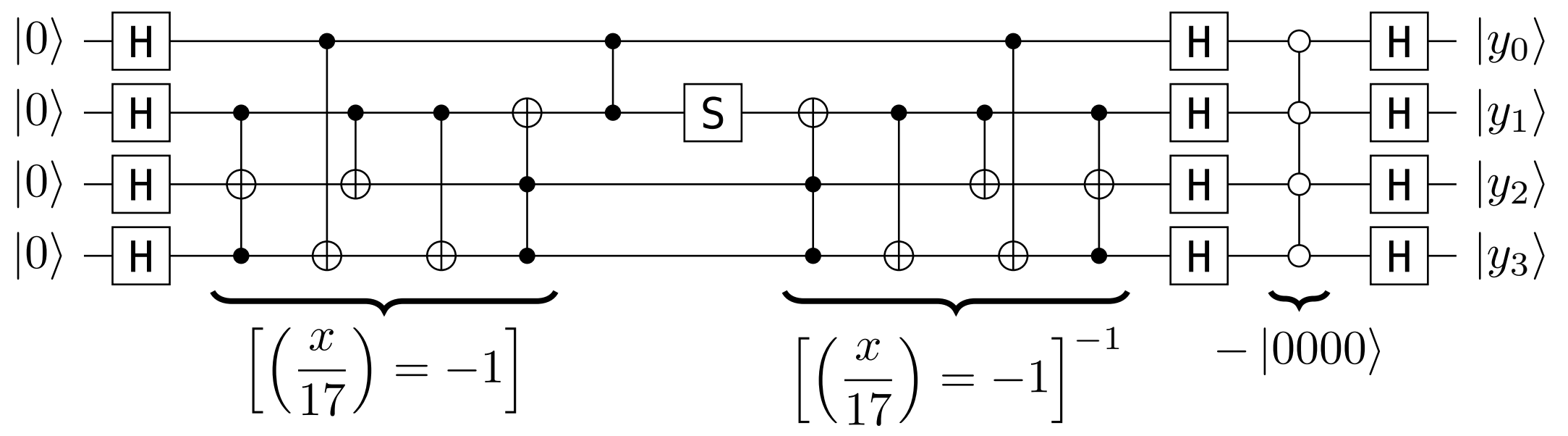
Jacobi symbol indicator permutation for $p = 17$



Ideally, the Jacobi symbol circuit should be produced by an algorithm, and not by computer search. We accept this shortcoming in the near term, since current NISQ devices fail to escape the noise floor using the full algorithm for $p = 17$.

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

Basic QNR circuit for $p = 17$



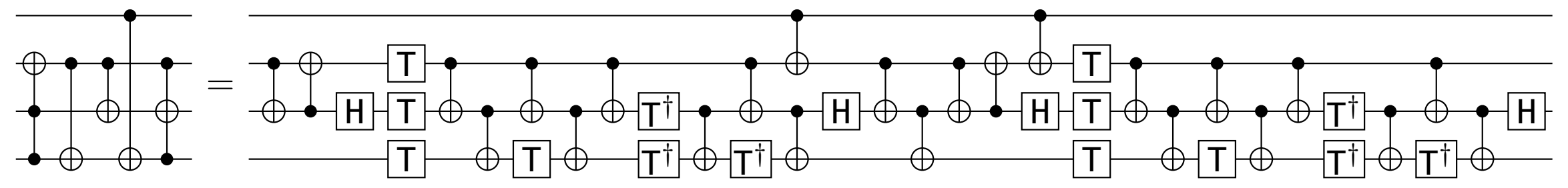
Running the QNR17 circuit on current NISQ devices

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

- Only single qubit gates and CNOTs.
- All CNOTs must be linear nearest neighbor.

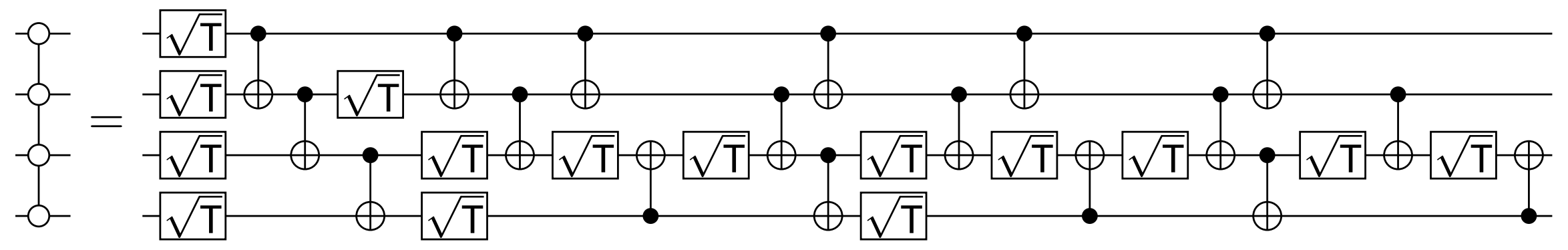
Inverse indicator permutation decomposition

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 [6].



Grover gate decomposition

We discovered a new circuit to flip the $|0000\rangle$ state without using an extra qubit.



The **QNR17 test** (far right), produces an equal superposition of the quadratic nonresidues for $p = 17$, namely $3, 5, 6, 7, 10, 11, 12, 14$.

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.

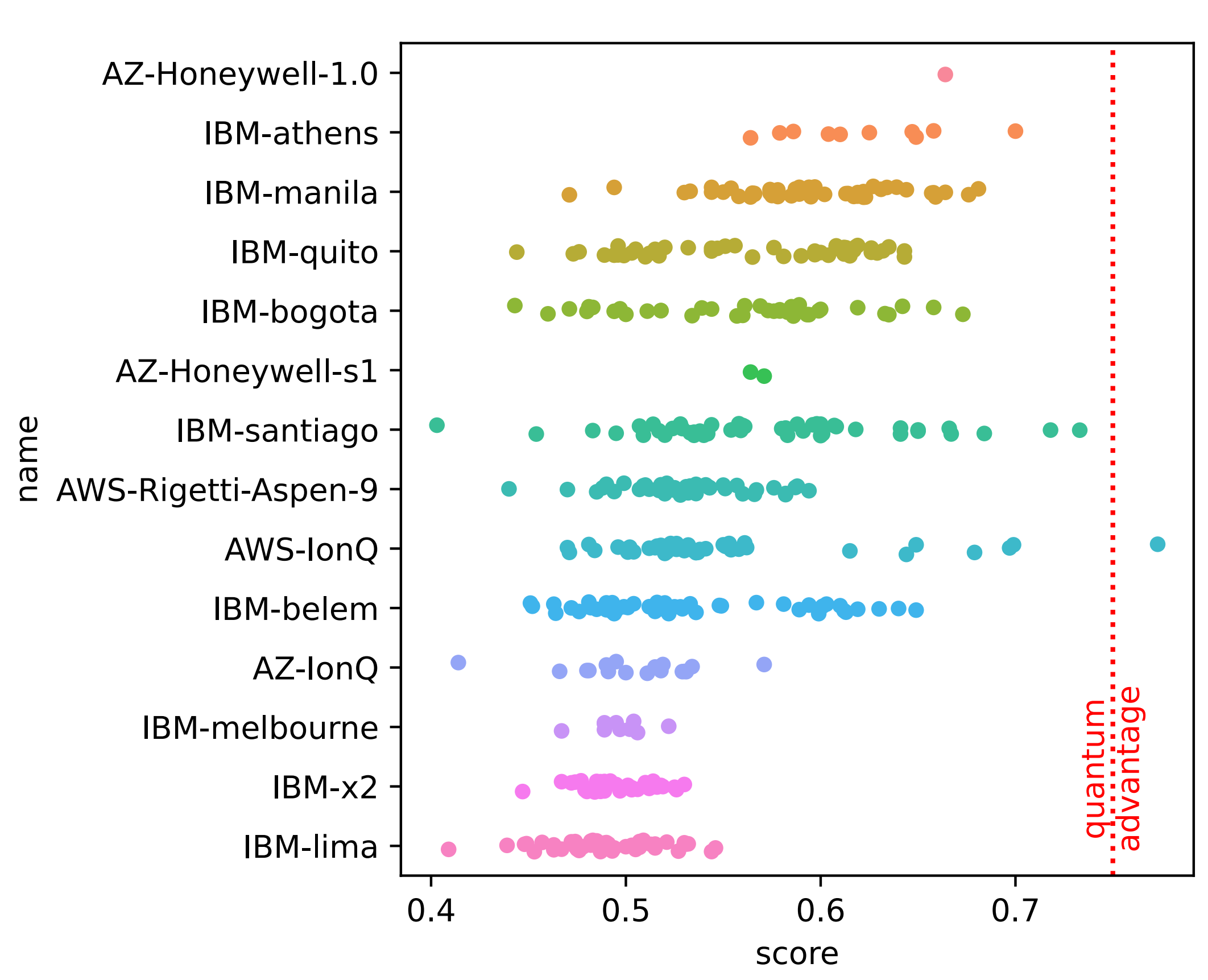
[4] R. P. Brent and P. Zimmerman, *An $O(M(n) \log n)$ algorithm for the Jacobi symbol*, CoRR, 2010.

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

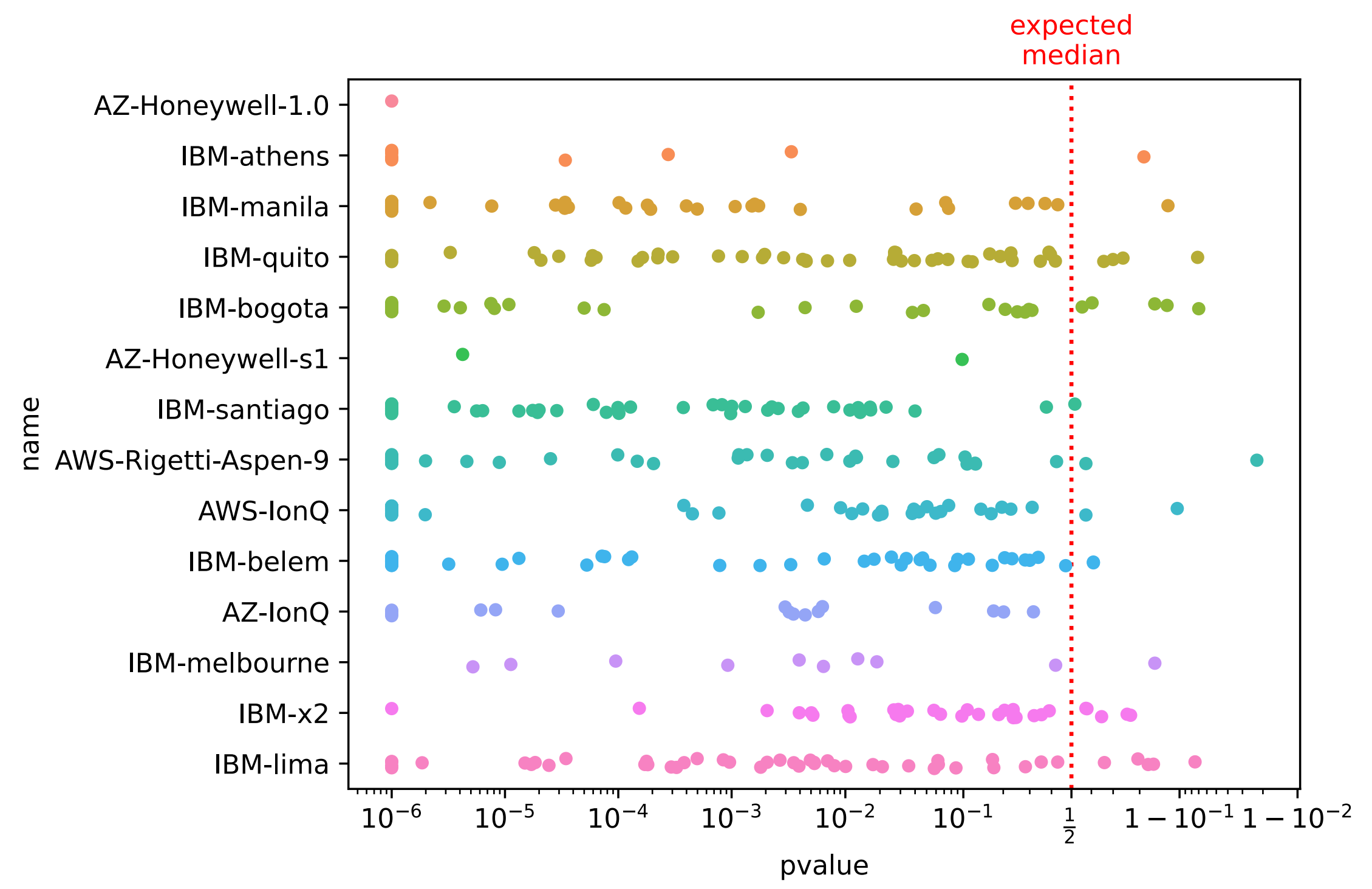
[6] C. Gidney, *Minimum number of CNOTs for Toffoli with non-adjacent controls (answer:3964)*, https://quantumcomputing.stackexchange.com, 2018.

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

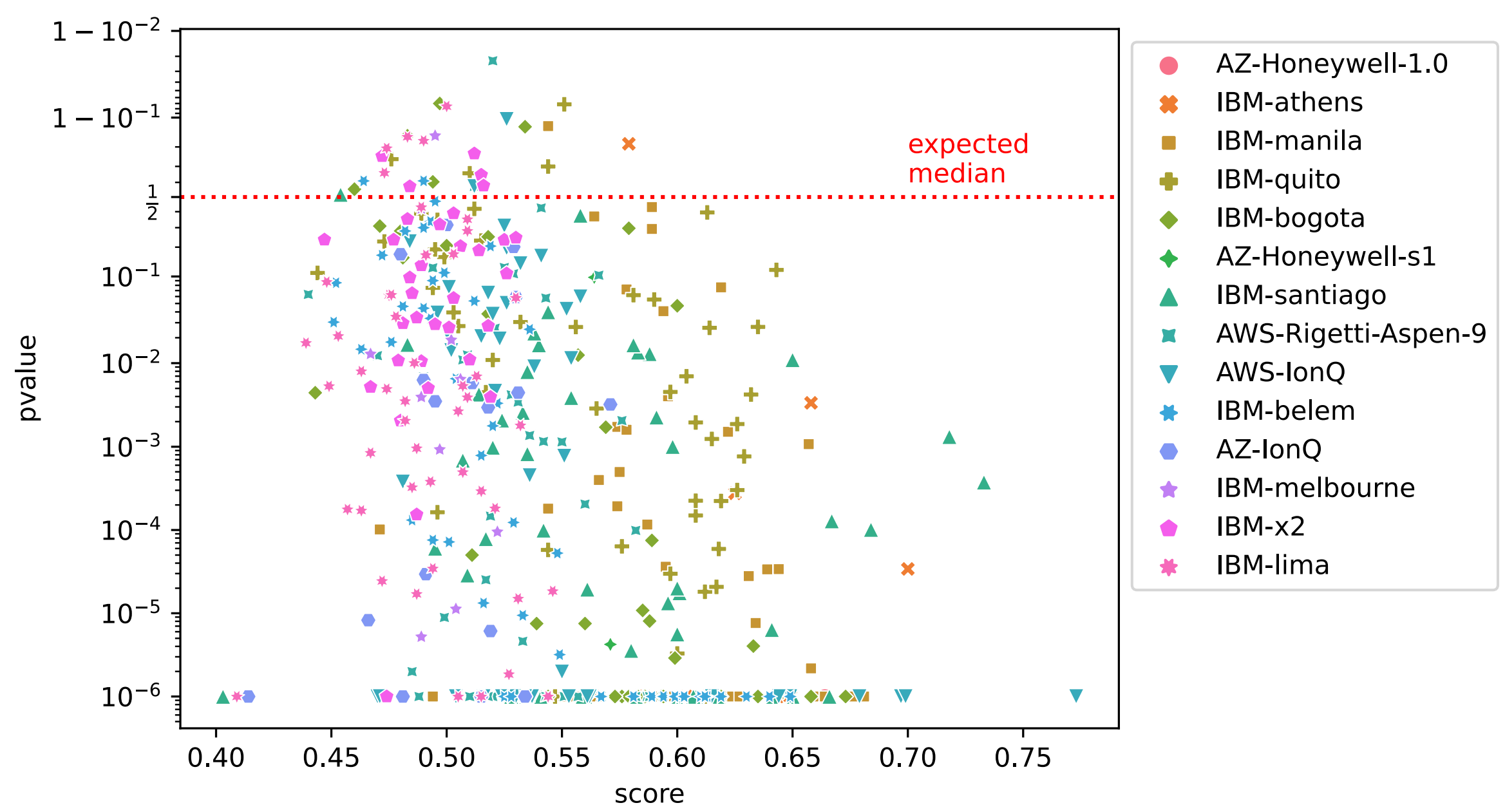
Success rate of 1000 shot runs



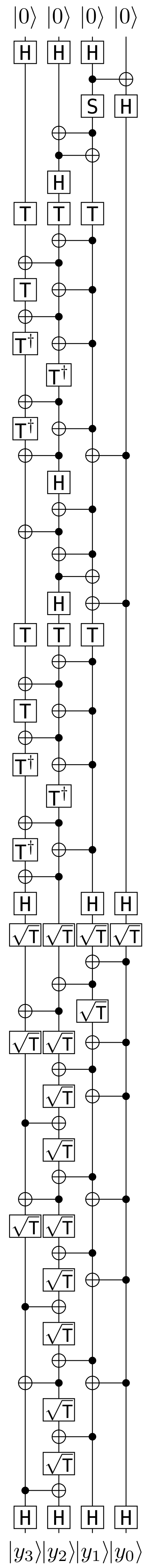
p-value of uniformity test for 1000 shot runs



Success rate vs. p-value



QNR17 test


$|0\rangle$ $|0\rangle$ $|0\rangle$ $|0\rangle$
H
S
T
T†
$\sqrt{T}$
$|y_3\rangle|y_2\rangle|y_1\rangle|y_0\rangle$

tinyurl.com/yckbk69n