

An unsolved problem since Gauss



Quadratic nonresidue problem (QNR):

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

Question: Is QNR in P?

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

QNR is in EQP_C

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

$[O(n)]$ 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.

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

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

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

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

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

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

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

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

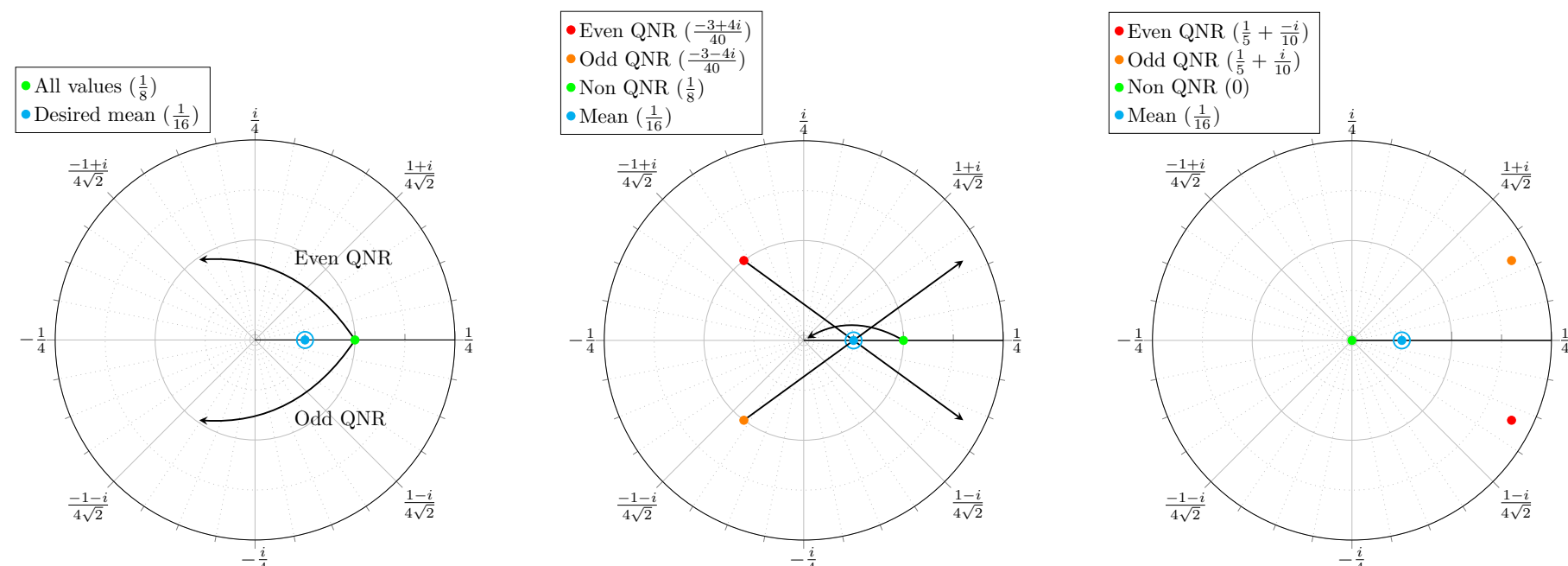
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i\theta f(x)(1-2x_0)} |x\rangle$$

$[O(n)]$ 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 success rate of the classical computer will always be less than 100%.

A NISQ test based on the QNR algorithm evaluates two properties:

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

Designing a QNR test circuit for $p = 17$

A highlighted block containing some math

A different kind of highlighted block.

$$\int_{-\infty}^{\infty} e^{-x^2} dx = \sqrt{\pi}$$

Interdum et malesuada fames $\{1, 4, 9, \dots\}$ ac ante ipsum primis in faucibus. Cras eleifend dolor eu nulla suscipit suscipit. Sed lobortis non felis id vulputate.

A heading inside a block

Praesent consectetur mi $x^2 + y^2$ metus, nec vestibulum justo viverra nec. Proin eget nulla pretium, egestas magna aliquam, mollis neque. Vivamus dictum **uTv** sagittis odio, vel porta erat congue sed. Maecenas ut dolor quis arcu auctor porttitor.

Another heading inside a block

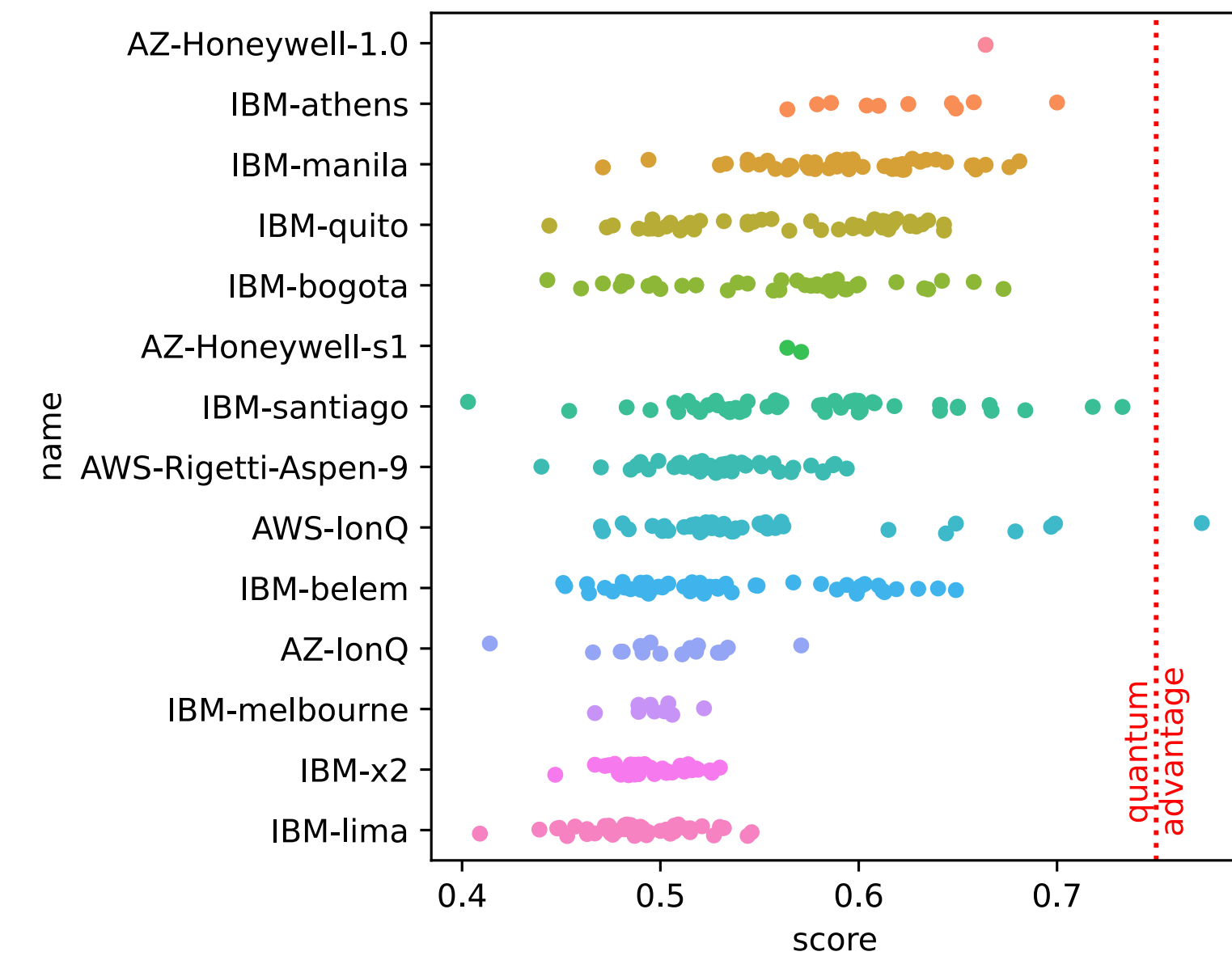
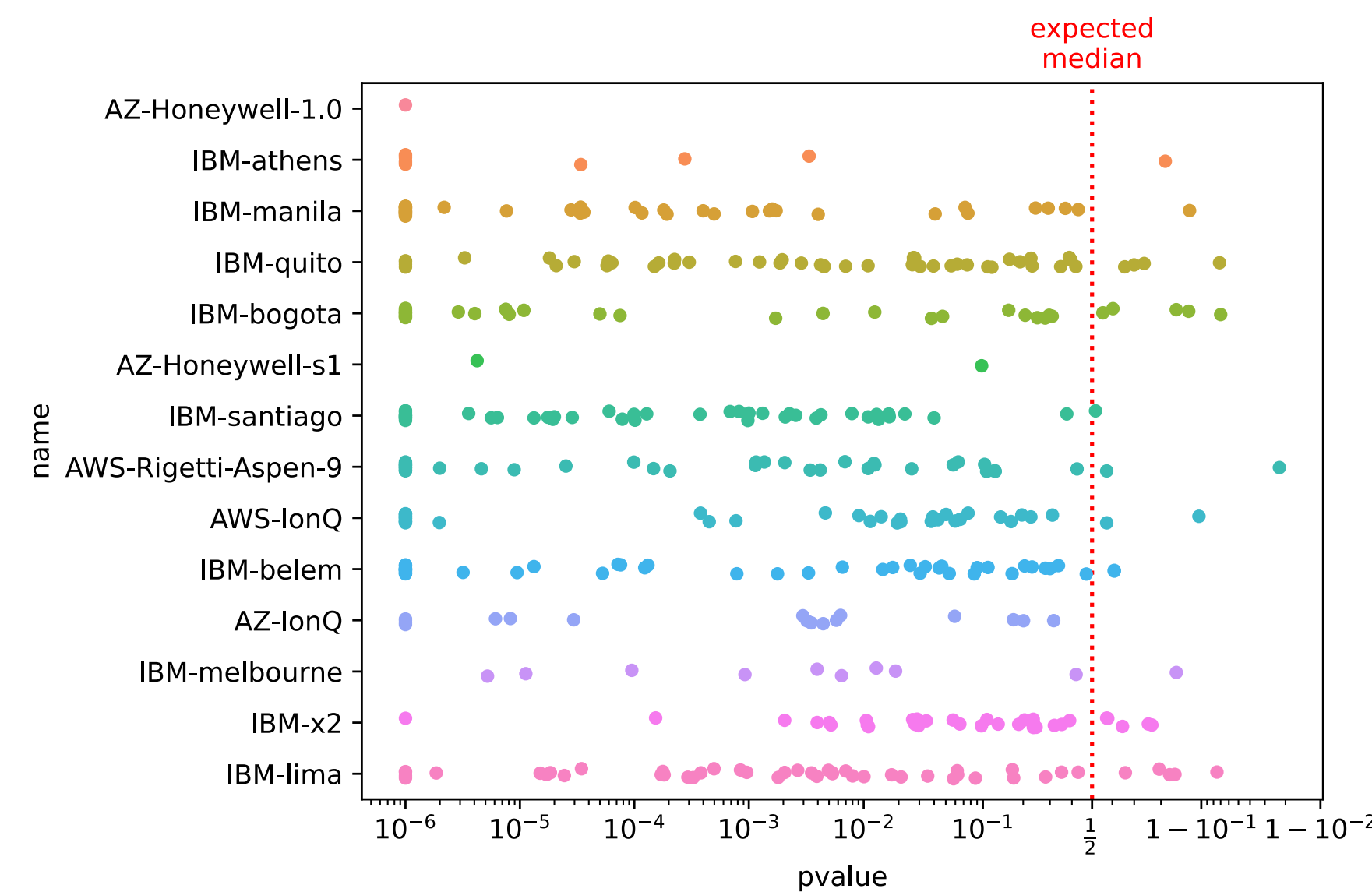
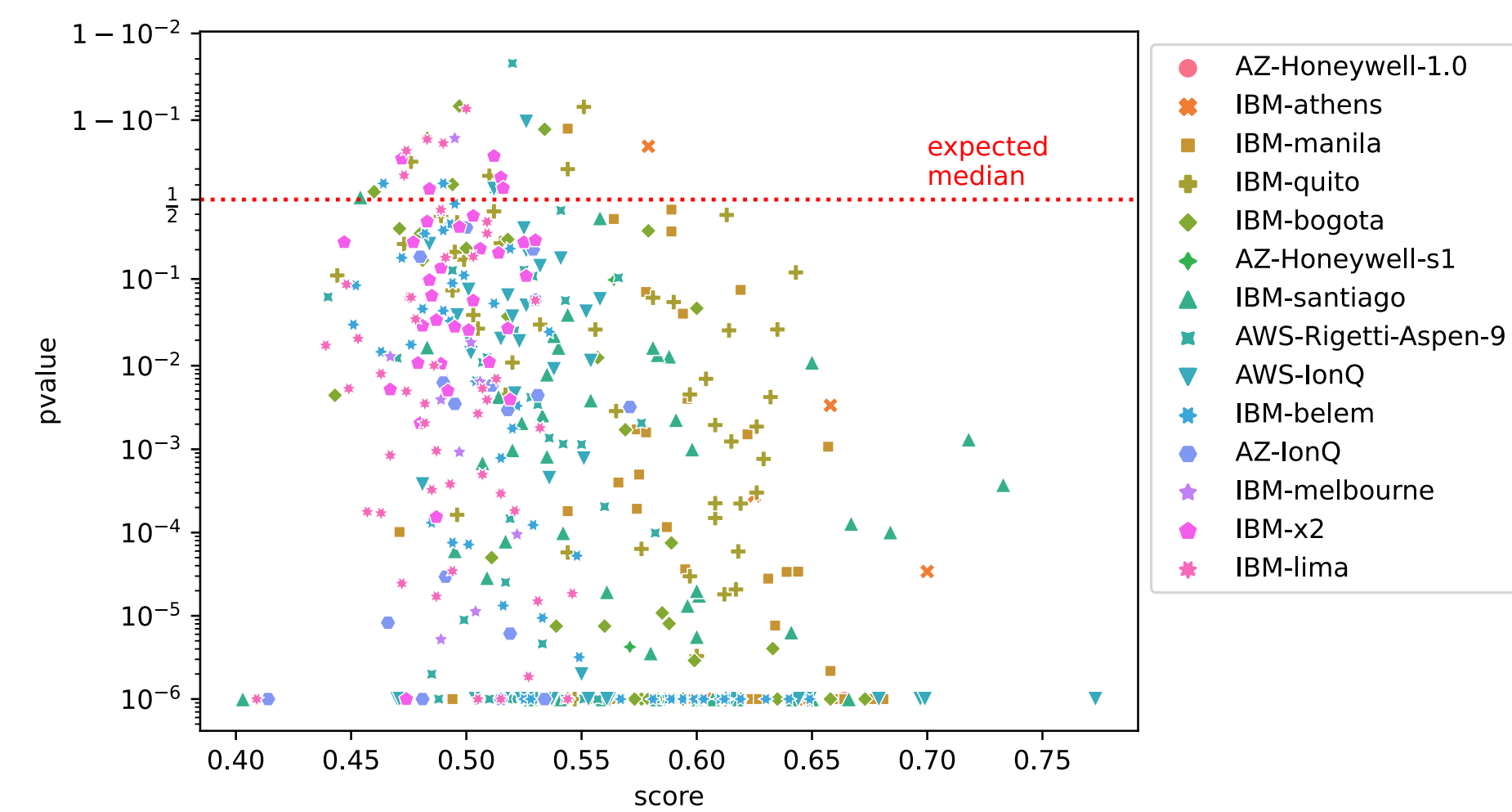
Sed augue erat, scelerisque a purus ultricies, placerat porttitor neque. Donec $P(y | x)$ fermentum consectetur $\nabla_x P(y | x)$ sapien sagittis egestas. Duis eget leo euismod nunc viverra imperdiet nec id justo.

References

- [1] Claude E. Shannon.
A mathematical theory of communication.
Bell System Technical Journal, 27(3):379–423, 1948.

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

Success rates of 1000 shot runs

 p -values of 1000 shot runsSuccess rate vs. p -value

References

Circuit

