

# Quantum Threshold Is Powerful

Daniel Grier 

University of California, San Diego, La Jolla, CA, USA

Jackson Morris 

University of California, San Diego, La Jolla, CA, USA

---

## Abstract

In 2005, Høyer and Špalek showed that constant-depth quantum circuits augmented with multi-qubit Fanout gates are quite powerful, able to compute a wide variety of Boolean functions as well as the quantum Fourier transform. They also asked what other multi-qubit gates could rival Fanout in terms of computational power, and suggested that the quantum Threshold gate might be one such candidate. Threshold is the gate that indicates if the Hamming weight of a classical basis state input is greater than some target value.

We prove that Threshold is indeed powerful – there are polynomial-size constant-depth quantum circuits with Threshold gates that compute Fanout to high fidelity. Our proof is a generalization of a proof by Rosenthal that exponential-size constant-depth circuits with generalized Toffoli gates can compute Fanout. Our construction reveals that other quantum gates able to “weakly approximate” Parity can also be used as substitutes for Fanout.

**2012 ACM Subject Classification** Theory of computation → Quantum complexity theory; Theory of computation → Circuit complexity

**Keywords and phrases** Shallow Quantum Circuits, Circuit Complexity, Threshold Circuits

**Digital Object Identifier** 10.4230/LIPIcs.CCC.2025.3

**Related Version** *Previous Version:* <https://arxiv.org/abs/2411.04953>

**Funding** Part of this research was performed while the authors were visiting the Institute for Mathematical and Statistical Innovation (IMSI), which is supported by the National Science Foundation (Grant No. DMS-1929348).

**Acknowledgements** JM thanks Farzan Byramji for helpful discussions about threshold circuits. We also thank anonymous reviewers for many useful comments. Part of this research was performed while the authors were visiting the Institute for Mathematical and Statistical Innovation (IMSI), which is supported by the National Science Foundation (Grant No. DMS-1929348).

## 1 Introduction

To what extent are large multi-qubit gates useful for quantum computation? On the one hand, it is well-known that every multi-qubit gate can be decomposed into a circuit of simpler 1- and 2-qubit gates. On the other hand, this decomposition may introduce large overheads both in terms of gate count and circuit depth. Given that some multi-qubit gates might be experimentally feasible [22, 14, 16], it’s natural to ask what kinds of computational powers they unlock.

Specifically, we focus on the power of these large multi-qubit gates in constant depth. Such shallow circuits are experimentally appealing due to the possibility for less decoherence. Moreover, even shallow quantum circuits with 1- and 2-qubit gates are known to be surprisingly powerful, exhibiting quantum advantage in a variety of settings [4, 9, 25, 11]. Given the inherent complexity of simulating such circuits, there is the exciting possibility that augmenting these circuit models with large multi-qubit gates might lead to constant-depth implementations of practical quantum algorithms.



© Daniel Grier and Jackson Morris;  
licensed under Creative Commons License CC-BY 4.0

40th Computational Complexity Conference (CCC 2025).

Editor: Srikanth Srinivasan; Article No. 3; pp. 3:1–3:23

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



Much of the excitement about such circuit models is driven by a single gate – the multi-qubit Fanout gate – which is the quantum operation that copies *classical* information:

$$F_n |b, x_1, \dots, x_n\rangle := |b, x_1 \oplus b, \dots, x_n \oplus b\rangle$$

for all  $b, x_1, \dots, x_n \in \{0, 1\}$ .

This seemingly innocuous gate (the classical analogue of which is included for free in almost every classical circuit model) turns out to be quite powerful. For starters, it is locally equivalent via conjugation by Hadamard gates to the quantum Parity gate [17],

$$P_n |b, x_1, \dots, x_n\rangle := |b \oplus (x_1 \oplus \dots \oplus x_n), x_1, \dots, x_n\rangle,$$

which is a duality that has no classical counterpart [1]. Moreover, there are constant-depth quantum circuits with Fanout (and arbitrary single-qubit gates) for a wide variety of other symmetric Boolean operations such as And/Or and Majority [13, 24]. Perhaps most impressively, constant-depth quantum circuits with Fanout gates can factor integers with polynomial-time classical post-processing [13].

Given the centrality of Fanout to the story of low-depth circuits with multi-qubit gates, there has been significant work in trying to understand if other multi-qubit gates are similarly powerful. Most notably, it is widely believed that the multi-qubit generalization of the Toffoli gate is fundamentally less powerful than the Fanout gate in constant depth, and there is long line of work giving evidence that these generalized Toffoli gates cannot compute Fanout [3, 6, 21, 19, 18, 2]. In some sense, all of these results are grappling with a fundamental tension in the study of these low-depth circuit models – the high entanglement in the states produced by these circuits is an obstacle to proving lower bounds, but it is simultaneously unclear how one could leverage this complexity to implement a useful quantum algorithm.

There is a surprising dearth of low-depth circuit models with multi-qubit gates that are as powerful as Fanout. One natural<sup>1</sup> candidate for a gate that could be as powerful as Fanout is the quantum Threshold gate, a multi-qubit gate parameterized by some value  $k \in \mathbb{N}$ :

$$Th_{n,k} |b, x_1, \dots, x_n\rangle := |b \oplus \mathbb{I}_{|x| \geq k}, x_1, \dots, x_n\rangle$$

where  $\mathbb{I}_{|x| \geq k}$  indicates if the Hamming weight of the input bit string  $x = x_1 \dots x_n \in \{0, 1\}^n$  is at least the target value  $k$ . In fact, Høyer and Špalek asked almost 20 years ago about the power of Threshold in constant depth [13]: “Can we simulate unbounded fan-out in constant depth using unbounded fan-in gates, e.g.  $\text{threshold}[t]$  or  $\text{exact}[t]$ ?” This question was reiterated more pointedly by Takahashi and Tani in 2011 [24]: “Does there exist a fundamental gate that is as powerful as an unbounded fan-out gate?”

We directly answer both of these questions in the affirmative by giving explicit constructions for Fanout using quantum Threshold gates:

► **Theorem 1.** *There are poly-size constant-depth quantum circuits consisting of Threshold gates and arbitrary single-qubit gates that compute Fanout with high fidelity. Formally,  $BQTC^0 = BQNC_{wf}^0$ .*

The construction from this theorem actually reveals a number of other gates that are as fundamentally powerful as the Fanout gate. As it turns out, the salient feature of Threshold for our purposes is that it can be used to construct a sort of “weak” Parity gate – a gate that only acts non-trivially on inputs of the same parity.

---

<sup>1</sup> This candidate looks considerably more natural after considering the analogous landscape of *classical* circuits, which we discuss in Section 1.1.

Based on this idea, we introduce a class of multi-qubit phase gates that exhibit a generalization of this behavior. Formally, these gates are defined with respect to a set  $S \subset \{0, 1\}^n$  in the following way:

$$U_S |x_1, \dots, x_n\rangle := (-1)^{\mathbb{I}_{x \in S}} |x_1, \dots, x_n\rangle.$$

Crucially, we restrict our attention to “parity-restricted” sets  $S$ , that is, sets where all elements have the same parity (i.e.,  $x, y \in S \implies |x| \equiv |y| \pmod{2}$ ). We show that these weak parity gates can be bootstrapped in constant depth into true Parity gates (which, recall, are locally-equivalent to Fanout) albeit with the help of a few generalized Toffoli gates:

► **Theorem 2.** *Let  $\{S_n\}_n$  be a family of parity-restricted sets with size  $|S_n| = \Theta(2^n/\text{poly}(n))$ . There are poly-size constant-depth quantum circuits consisting of  $U_{S_n}$  gates, generalized Toffoli gates, and arbitrary single-qubit gates that compute Fanout with high fidelity.*

Since it is widely believed that multi-qubit Toffoli gates are not themselves sufficient to implement Fanout, the power of this construction likely derives from the weak parity gates. In fact, the reason these Toffoli gates were not required for Theorem 1 is due to the fact that Threshold can directly simulate Toffoli. In that vein, we also give conditions under which the  $U_{S_n}$  gates alone suffice to simulate Parity; namely, when  $|S_n| \geq 2^{n-O(1)}$  or  $|S_n| \leq 2^{(1-\epsilon)n}$ . Though, the latter condition will result in circuits of super-polynomial size.

While it has long been thought that Fanout/Parity gates were morally equivalent to other quantum modular arithmetic gates, those constructions seem to *also* require these generalized Toffoli gates [8]. By a careful inspection of the original construction presented in [8] we find that generalized Toffoli gates are in fact not necessary. Formally, the quantum Mod- $p$  gates are defined as

$$\text{MOD}_{n,p} |b, x_1, \dots, x_n\rangle := |b \oplus \text{Mod}_{n,p}(x), x_1, \dots, x_n\rangle,$$

where  $\text{Mod}_{n,p}(x)$  is 1 when  $p$  divides the Hamming weight of  $x = x_1, \dots, x_n \in \{0, 1\}^n$ . For example, the Mod-2 gate is essentially the Parity gate (up to a single-qubit  $X$  gate). It is implicit in [8] that Fanout can be computed by a circuit consisting of Mod- $p$  gates and one- and two-qubit gates, yielding  $\text{QNC}_{wf}^0 = \text{QNC}^0[2] \subseteq \text{QNC}^0[q]$  for all  $q \geq 2$ , but not necessarily that  $\text{QNC}^0[p] = \text{QNC}^0[q]$  for distinct  $p$  and  $q$ . The result they make explicit is that when Toffoli gates are allowed, any Mod- $q$  gate can be obtained using any other Mod- $p$  gate (by first implementing Fanout with Mod- $q$  gates and then computing Mod- $p$  with Fanout and generalized Toffoli gates). Concretely;  $\text{QAC}^0[p] = \text{QAC}^0[q]$  for  $p, q \geq 2$ . Only later was it shown that generalized Toffoli gates can be implemented using Fanout and single- and two-qubit gates, i.e., that  $\text{QNC}_{wf}^0 = \text{QAC}_{wf}^0$  [13, 24]. In light of these results we observe the following:

► **Theorem 3.** *For all  $p, q \geq 2$ , there are poly-size constant-depth quantum circuits consisting of Mod- $p$  gates and single-qubit gates that compute the Mod- $q$  operation. Formally,  $\text{QNC}^0[p] = \text{QNC}^0[q]$ .*

## 1.1 Comparison to the classical setting

Our focus on shallow circuits draws considerable inspiration from the analogous study of classical constant-depth circuit classes with large fan-in gates, which has been hugely influential in classical complexity theory. For instance, initial work in Boolean circuits saw the development of techniques for proving unconditional lower bounds such as random restrictions [1, 7, 27, 12], Fourier analytic methods [15], and polynomial methods [20, 23].

So how do we compare the quantum and classical settings? And what does this comparison tell us about the power of quantum circuits in constant depth? To start, classical circuit classes (e.g.,  $\text{NC}^0$ ,  $\text{AC}^0$ ,  $\text{TC}^0$ , ...) typically assume that the output of any gate can be used as input for any number of other gates (i.e., a gate’s output can be “fanned out” to other gates). Of course, this is exactly the kind of fanout that immediately becomes so powerful when given to a constant-depth quantum circuit.

In fact, because of this fanout, the classical Threshold gate reigns supreme amongst similar classical circuit complexity classes. This is due to the fact that constant-depth classical circuits with Fanout and Threshold can compute any Boolean function where the output depends only on the Hamming weight of the input.<sup>2</sup> Formally, the complexity class  $\text{TC}^0$ , which contains all languages computed by constant-depth classical circuits with Threshold, contains all other similarly defined classical circuit classes with other large fan-in gates:  $\text{NC}^0[p]$ ,  $\text{AC}^0$ ,  $\text{AC}^0[p]$ , and  $\text{ACC}$ .<sup>3</sup> In many cases, Threshold is provably more powerful, e.g.,  $\text{AC}^0 \subsetneq \text{TC}^0$  [1, 7] and  $\text{AC}^0[p] \subsetneq \text{TC}^0$  [20, 23].

This is why the Threshold gate was a tantalizing target for quantum exploration. Prior to our work, it was *not* known whether the quantum version of  $\text{TC}^0$  – i.e.,  $\text{BQTC}^0$  – was as powerful as the quantum versions of the other classical complexity classes. In fact, given the surprising power of Fanout in the quantum world, the exact opposite was known:  $\text{BQNC}_{wf}^0 \supseteq \text{BQTC}^0$  [13]. That is, constant-depth quantum circuits with Fanout could simulate constant-depth circuits with Threshold. Our work restores order to the usually classical hierarchy, placing Threshold alongside Fanout as one of the most powerful quantum gates in constant depth:  $\text{BQTC}^0 = \text{BQNC}_{wf}^0$ .

## 1.2 Proof techniques and overview

The constructions in Theorem 1 and Theorem 2 follow a general outline pioneered by Rosenthal [21]. There, it is shown that constant-depth quantum circuits can compute Fanout using generalized Toffoli gates *provided exponential-sized circuits are allowed*. While not phrased in this language, Rosenthal’s construction shows a proof-of-principle technique for taking a very “weak” Parity gate (indeed, Toffoli non-trivially computes Parity for exactly one input!) and boosting it to a full Parity gate. We show that when we start with a gate (like Threshold) which is closer to Parity, this construction can be altered to yield circuits of polynomial size.

The proof goes in two steps. First, define a certain cat-like state called a “nekomata” [21]:

$$\frac{|0^n\rangle \otimes |\psi_0\rangle + |1^n\rangle \otimes |\psi_1\rangle}{\sqrt{2}}$$

where  $|\psi_0\rangle$  and  $|\psi_1\rangle$  are arbitrary states. Following a similar idea to that of Green et al. [8], such states can be used to compute Parity in constant depth using the relative phase between the  $|0^n\rangle$  and  $|1^n\rangle$  part of the state.

Second, show there is an explicit constant-depth construction for a nekomata state. Here, we show the key ingredient is the ability to create a “noisy” version of a usual cat state, where the all-zeroes and all-ones outcomes have noticeably larger amplitudes than those on

<sup>2</sup> To see this, first notice that for any  $k$ , there is a constant-depth circuit with two Threshold gates that computes whether or not the input has Hamming weight exactly  $k$ . Since any symmetric Boolean function can be expressed as a disjunction over these “exact- $k$ ” clauses, the claim immediately follows due to the fact that a threshold of 1 is equivalent to the Or function.

<sup>3</sup> See Section 2.2 for precise definitions.

the other outcomes. Threshold gates are significantly better at this task than the Toffoli gates in Rosenthal's original construction. Finally, these states can be combined together (using Toffoli or Threshold gates) to form a high-fidelity nekomata state, completing the construction.

### 1.3 Related work

Our work shares some similarity to that of [10], where the authors explore quantum advantage with constant-depth quantum circuits. They also make a similar claim suggesting that  $\text{QTC}^0 = \text{QNC}_{wf}^0$ , but crucially, their results hold in a circuit model with intermediate measurements and classical fanout. The classical fanout in their circuit model allows them to bootstrap the poor man's cat state construction of Bene Watts et al. [26] to construct an actual cat state, an idea that was also explored in [5]. To be clear, our circuit model and definition of  $\text{BQTC}^0$  follows in a traditional line of work (e.g, [17, 8, 13, 24, 19, 21, 18]), where no such intermediate measurements or classical fanout is allowed. Therefore, we must use entirely different techniques.

### 1.4 Future directions

One immediate question left open by our work is whether the approximation error inherent in the construction used to prove Theorem 1 can be eliminated without incurring a size or depth blow-up. More generally, we ask which other conditions on a family of multi-qubit gates lead to powerful shallow circuits. One explicit approach would be to ask what properties of the sets  $S$  parameterizing our phase gates  $U_S$  are sufficient to compute Fanout. Is there a sufficient condition beyond being parity restricted?

Another interesting question concerns the circuit complexity of restricted families of threshold functions. Specifically, consider the Exact- $k$  gate, which indicates if the Hamming weight of the input is exactly  $k$ . Notice that Exact- $k$  can be constructed from two Threshold gates. Moreover, for  $k \approx n/2$ , Exact- $k$  can be used to compute Threshold. This latter statement is not obvious and follows from the fact that our proof of Theorem 1 actually uses Exact gates rather than Threshold gates. Indeed, for any constant  $\alpha > 0$  and any  $k \in [n^\alpha, n - n^\alpha]$  the gates  $\text{EX}_{k/2}$ ,  $\text{Th}_k$  and  $\text{P}_n$  are all equivalent under  $\text{QAC}^0$  reductions (see Theorem 22). However, it is unclear if this remains true for  $k$  which is sub-polynomial in  $n$ , say  $k = \log n$ .

## 2 Preliminaries

We will now introduce the different types of entangling gates considered in this work, the types of circuits constructed from them, and the complexity classes to which they roughly correspond.

### 2.1 Multi-qubit Gates

A simple multi-qubit gate is the CNOT gate which acts on two qubits, flipping the target conditioned on the control, i.e.,

$$\text{CNOT} |x_1, x_2\rangle = |x_1, x_1 \oplus x_2\rangle$$

Any two-qubit gate can be constructed from constantly many single-qubit gates and CNOT gates. A circuit consisting entirely of arbitrary single- and two-qubit gates is said to be a QNC circuit.

Another multi-qubit gate of interest is the Toffoli gate, which acts on three qubits by flipping the last qubit controlled on the first two, i.e.,

$$\text{Tof} |x, y, z\rangle = |x, y, (x \wedge y) \oplus z\rangle$$

This gate can be seen as a CNOT gate with an additional control qubit. In fact, we call the analogous unitary on  $n > 1$  qubits a *generalized* Toffoli gate:

► **Definition 4.** *The generalized Toffoli gate  $\wedge_n$  acts on  $n + 1$  qubits by computing the AND of the first  $n$  bits in superposition. For all  $x_1, x_2, \dots, x_n, b \in \{0, 1\}$  the  $\wedge_n$ -gate acts as*

$$\wedge_n |x_1, x_2, \dots, x_n, b\rangle = |x_1, x_2, \dots, x_n, (x_1 \wedge \dots \wedge x_n) \oplus b\rangle$$

Circuits composed of arbitrary single-qubit gates and generalized Toffoli gates are referred to as QAC circuits.

► **Definition 5.** *For  $k \in \{0, 1 \dots n\}$  and  $x_1, x_2, \dots, x_n, b \in \{0, 1\}$  the unitary  $\text{Th}_{n,k}$  acts as*

$$\text{Th}_{n,k} |b\rangle |x\rangle = |b \oplus \mathbb{I}_{|x| \geq k}\rangle |x\rangle$$

Circuits composed of arbitrary single-qubit gates and threshold gates<sup>4</sup> are said to be QTC circuits. Note that by taking  $k = n$  we recover the generalized Toffoli gate, and in this sense the generalized Toffoli gate *is* a Threshold gate, so including this gate in the allowed gate-set for QTC circuits would be redundant.

Note that in the above definition we allow for the use of any threshold gate in QTC circuits, but this is actually not necessary, even in constant depth. As we will later show, it suffices to have a usual threshold,  $\text{Th}_{n,k}$ , or exact,  $\text{EX}_{n,k}$ , gate with  $k = \text{poly}(n)$  to recover the full computational power of QTC as is defined above. In other words, any sufficiently powerful  $\text{EX}_{n,k}$  or  $\text{Th}_{n,k}$  gate can be leveraged to recover *all other* threshold and exact gates in constant-depth and polynomial-size. This reduction is non-trivial and combines our main result with the constant-depth constructions given in [13] for computing arbitrary threshold gates with fanout. A full explanation is given in Theorem 22.

Let  $U_f$  be the unitary which computes some boolean function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  in superposition, i.e., for all  $x \in \{0, 1\}^n$  and  $b \in \{0, 1\}$   $U_f |x, b\rangle = |x, b \oplus f(x)\rangle$ . Note that all multi-qubit gates discussed thus far fall into this category. Now, observe that when the target qubit is replaced with  $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ , we can “compute  $f$  in the phase”:

$$U_f |-\rangle |x\rangle = (-1)^{f(x)} |-\rangle |x\rangle$$

So, given  $U_f$  we can with a single ancilla implement  $V_f$  which acts as  $V_f |x\rangle = (-1)^{f(x)} |x\rangle$ . While going from  $U_f$  to  $V_f$  is not a difficult task the converse could in general be quite non-trivial.<sup>5</sup>

As mentioned, the *quantum Fanout gate* gives us some way of “copying” a given qubit and XOR-ing it onto an unbounded number of qubits.

<sup>4</sup> Recall that a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  is said to be a *threshold function* if it can be written as

$$f(x) = \begin{cases} 1 & \sum_{i=1}^n w_i x_i \geq b \\ 0 & \text{otherwise} \end{cases}$$

for some  $w_1, \dots, w_n, b \in \mathbb{R}$ . For our purposes it suffices to only consider threshold functions in which  $w_i = 1$  for all  $i \in [n]$ .

<sup>5</sup> For instance, take  $Z^{\otimes n}$ ; this gate computes parity in the phase as  $Z^{\otimes n} |x\rangle = (-1)^{|x|} |x\rangle$ , but it is unclear if there is a simple way to recover the usual parity gate:  $P_n$ .

► **Definition 6.** For all  $x_1, x_2, \dots, x_n, b \in \{0, 1\}$  the Fanout unitary,  $F_n$ , acts as

$$F_n |b\rangle |x_1, x_2, \dots, x_n\rangle = |b \oplus x_1, b \oplus x_2, \dots, b \oplus x_n\rangle$$

We will refer to circuits constructed from one- and two-qubit and Fanout gates as  $\text{QNC}_{wf}$  circuits.

Another important class of gates are so-called MOD gates:

► **Definition 7.** For a given  $m \in \mathbb{N}$  and all  $x_1, x_2, \dots, x_n, b \in \{0, 1\}$  the  $\text{MOD}_{n,m}$  gate acts as

$$\text{MOD}_{n,m} |x_1, x_2, \dots, x_n\rangle |b\rangle = |x_1, x_2, \dots, x_n\rangle |\text{Mod}_{n,m}(x) \oplus b\rangle$$

Where  $\text{Mod}_{n,m}(x) = 1$  iff  $|x|$  is divisible by  $m$ . Further, for  $\ell \in \{0, 1, \dots, m-1\}$  we use  $\text{Mod}_{n,m,\ell}(x)$  to denote the function which is 1 iff  $|x| \equiv \ell \pmod{m}$  and the corresponding quantum gate accordingly:

$$\text{MOD}_{n,m,\ell} |b\rangle |x_1, x_2, \dots, x_n\rangle = |\text{Mod}_{n,m,\ell}(x) \oplus b\rangle |x_1, x_2, \dots, x_n\rangle.$$

Note that when  $m = 2$  the  $\text{MOD}_{n,2,1}$  gate is equivalent to the parity gate  $P_n$ . When a circuit consists of one- and two-qubit gates and  $\text{MOD}_{n,m}$  gates for a fixed  $m$  it is called a  $\text{QNC}[m]$  circuit and when the circuit also contains generalized Toffoli gates it is referred to as a  $\text{QAC}[m]$  circuit.

The final class of gates we will define are what we call “parity-restricted” gates which have not previously appeared in the literature. A set of bit strings  $S \subseteq \{0, 1\}^n$  is said to be *parity restricted* if  $|s_1| \equiv |s_2| \pmod{2}$  for all  $s_1, s_2 \in S$ .

► **Definition 8.** For a given set  $S \subset \{0, 1\}^*$  we define the  $n$ -qubit gate  $U_{S,n}$  as

$$U_{S,n} |x\rangle = (-1)^{\mathbb{I}_S(x)} |x\rangle$$

Further, we call  $U_{S,n}$  a *parity-restricted gate* if  $|x| \equiv |y| \pmod{2}$  for all  $x, y \in S$ .

We will often drop the  $n$  subscript from  $U_{S,n}$  when discussing sets  $S$  which only consist of strings of the same length, i.e.  $S \subset \{0, 1\}^n$  for some  $n$ .

For a given parity-restricted set  $S$ , a circuit consisting of arbitrary one- and two-qubit gates and  $U_{S,n}$  gates for  $n \in \mathbb{N}$  is said to be a  $\text{QNC}_S$  circuit. Similarly, if the circuit also consists of generalized Toffoli gates the circuit is said to be a  $\text{QAC}_S$  circuit. Indeed, the parity-restricted condition can be dropped, but in this work we will only consider  $S$  which are parity-restricted sets.

Finally, we will define the primary complexity measures for quantum circuits.

► **Definition 9.** A quantum circuit  $C$  is said to have depth  $d$  if  $C$  can be decomposed as a sequence  $M_d S_d \dots M_2 S_2 M_1 S_1$  where each  $S_i$  consists entirely of single-qubit gates and  $M_i$  consists of non-overlapping multi-qubit gates (i.e., every pair of gates in  $M_i$  operate on disjoint sets of qubits).

► **Definition 10.** A quantum circuit  $C$  has size  $s$  if  $C$  has exactly  $s$  multi-qubit gates.

## 2.2 Quantum Circuit Complexity Classes

In this section we will define the relevant quantum circuit classes, but before doing that we must introduce the notion of a circuit family and what it means for a circuit family to compute a Boolean function.



► **Definition 11.** A family of quantum circuits is a collection  $\mathcal{C} = \{C_n\}_{n \geq 1}$  where  $C_n$  acts on  $n + a(n)$  qubits where  $a(n)$  is some computable function.

This definition of a circuit family is analogous to the classical notion of a *non-uniform* circuit family since there need not be any relation between circuits for different sizes (e.g., it is not necessary for there to exist a Turing machine which outputs a description of  $C_n$  on input  $1^n$ . Such a requirement is only for *uniform* circuit families). It should be noted that all constructions presented in this work correspond to uniform circuit families nonetheless.

► **Definition 12.** For a given language  $L \subseteq \{0, 1\}^*$  we say that a family of quantum circuits  $\{C_n\}_{n \geq 1}$  each acting on  $n + a(n)$  qubits exactly computes  $L$  if for all  $n \geq 1$  and  $x \in \{0, 1\}^n$  measuring the last qubit of  $C_n |x\rangle |0^{a(n)}\rangle$  in the computational basis yields

- $|1\rangle$  with certainty if  $x \in L$
- $|0\rangle$  with certainty if  $x \notin L$

Now, for the complexity classes of interest:

- $\text{QNC}^i$  is the class of problems decidable by QNC circuits which act on polynomially-many qubits (i.e.  $n + a(n)$  is bounded by some polynomial in  $n$ ), have polynomial size and depth  $O(\log^i(n))$ .
- $\text{QAC}^i$  is the class of problems decidable by QAC circuits which act on polynomially-many qubits, have polynomial size and depth  $O(\log^i(n))$ .
- $\text{QTC}^i$  is the class of problems decidable by QTC circuits which act on polynomially-many qubits, have polynomial size and depth  $O(\log^i(n))$ .
- $\text{QNC}_{wf}^i$  is the class of problems decidable by  $\text{QNC}_{wf}$  circuits which act on polynomially-many qubits, have polynomial size and depth  $O(\log^i(n))$ .

The primary focus of this work will be constant depth circuits, which correspond to  $i = 0$  in the above definitions, i.e., the classes  $\text{QNC}^0$ ,  $\text{QAC}^0$ ,  $\text{QTC}^0$ , and  $\text{QNC}_{wf}^0$ .

Finally, we introduce two new complexity classes parameterized by sets  $S \subset \{0, 1\}^*$ :

- For a given set  $S$ ,  $\text{QNC}_S^i$  is the class of problems decidable by  $\text{QNC}_S$  circuits which act on polynomially-many qubits, have polynomial size and depth  $O(\log^i n)$ .
- For a given set  $S$ ,  $\text{QAC}_S^i$  is the class of problems decidable by  $\text{QAC}_S$  circuits which act on polynomially-many qubits, have polynomial size and depth  $O(\log^i n)$ .

► **Proposition 13** (Proposition 3.1 of [8]). The following tasks are equivalent for constant-depth circuits consisting of  $\wedge_n$ -gates and single-qubit gates:

1. Preparing the state  $\frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$  from  $|0^n\rangle$  and performing the inverse transformation.
2. Applying Fanout  $F_n$ .
3. Applying Parity  $P_n$ .

In other words, these tasks are equivalent under  $\text{QAC}^0$  reductions.

Critical to our construction is the fact that (1) in the above proposition can be relaxed to a more general state preparation task. To see how, we must define a class of a “cat-like” states, first introduced by Rosenthal [21] which he calls *nekomata*:

► **Definition 14.** A state  $|\phi\rangle$  on  $n + m$  qubits is said to be an  $n$ -nekomata if there exists some ordering of the qubits such that

$$|\phi\rangle = \frac{|0^n\rangle \otimes |\psi_0\rangle + |1^n\rangle \otimes |\psi_1\rangle}{\sqrt{2}}$$

where  $|\psi_0\rangle$  and  $|\psi_1\rangle$  are arbitrary  $m$ -qubit states. The first  $n$  qubits of this state are referred to as the target qubits.



As mentioned, Proposition 13 is still true when the cat state in task 1 is replaced with any  $n$ -nekomata (see Section A for more details). This fact is quite powerful since we only need to design a circuit which produces a state on which some subsystem is “cat-like” in order to compute parity. This makes the prospect of designing a circuit to compute parity far less daunting.

### 2.3 Approximate Quantum Circuits

Proposition 13 shows that exactly preparing a cat state is in fact computationally equivalent to exactly computing parity, up to some  $\text{QAC}^0$  computations and this can further be generalized by relaxing the task of preparing a nekomata state. Further, it is established in [21] that preparing an approximate nekomata state is sufficient to *approximately* compute parity or fanout. This notion is made precise below.

► **Definition 15.** For  $\epsilon \in [0, 1]$  a state  $|\phi\rangle$  on  $n + m$  qubits is said to be an  $\epsilon$ -approximate nekomata if there exists some nekomata  $|\nu\rangle$  such that  $|\langle\nu|\phi\rangle|^2 \geq 1 - \epsilon$ .

When we refer to a quantum circuit as approximately computing some function or approximating a given unitary we mean that the circuit,  $C$ , and the ideal unitary  $U$  have small distance. Explicitly, for  $\epsilon \in (0, 1)$  we say that  $C$  is an  $\epsilon$ -approximate implementation of  $U$  or that  $C$  computes  $U$  with approximation error  $\epsilon$  if  $\|U - C\|_{\text{op}} \leq \epsilon$  where  $\|\cdot\|_{\text{op}}$  denotes the operator norm.

A statement analogous to Proposition 13 holds for the approximate version of each task:

► **Lemma 16** (Theorem 3.1 of [21]). For any  $\epsilon \in (0, 1)$  the following tasks are equivalent under  $\text{QAC}^0$  reductions:

- Preparation of  $O(\epsilon)$ -approximate nekomata from the all zeros state and the inverse transformation
- Approximately computing Parity with error  $O(\epsilon)$
- Approximately computing Fanout with error  $O(\epsilon)$

This lemma is again quite useful for us as circuit designers; now any circuit producing a state which has some subsystem that is *approximately* cat-like suffices to approximately implement fanout or parity.

Finally, we define the bounded-error analogues of the quantum circuit complexity classes introduced thus far:

► **Definition 17** ( $\text{BQNC}^i$ ). A decision problem  $L \subseteq \{0, 1\}^*$  is in  $\text{BQNC}^i$  if there exists a family of  $\text{QNC}^i$  circuits  $\{C_n\}_{n \in \mathbb{N}}$  acting on  $n + a(n) = \text{poly}(n)$  qubits and a constant  $c > 0$  such that for all  $n \in \mathbb{N}$  and  $x \in \{0, 1\}^n$  measuring the last qubit of  $C_n |x\rangle |0^{a(n)}\rangle$  in the computational basis yields

- $|1\rangle$  with probability at least  $2/3$  if  $x \in L$
- $|1\rangle$  with probability at most  $1/3$  if  $x \notin L$

$\text{BQAC}^i$ ,  $\text{BQTC}^i$ ,  $\text{BQNC}_{wf}^0$ ,  $\text{BQNC}_S^i$ , and  $\text{BQAC}_S^i$  are defined similarly for their respective circuit classes.

## 3 Bootstrapping weak parity gates

In this section we will show that for any non-empty parity restricted set  $S \subseteq \{0, 1\}^n$  the unitary  $U_S |x\rangle = (-1)^{\mathbb{I}_{x \in S}} |x\rangle$  can be bootstrapped in constant depth to approximately compute Parity. This construction generalizes the constant-depth exponential-size  $\text{QAC}$  circuit family given in [21]. As a corollary, we find that for any polynomial  $p$ , there exist poly-size  $\text{QTC}^0$  circuits which have fidelity  $1 - 1/p(n)$  with Parity.

### 3.1 Grid Construction

Rather than directly computing Parity, the circuits described in this section will prepare approximate nekomata, which via Lemma 16 can be used to compute Parity and Fanout with high essentially the same approximation error, up to constant factors.

We will make use of the following lemma:

► **Lemma 18** (Lemma 4.3 of [21]). *Let  $|\varphi\rangle$  be a state with  $n$  “target” qubits that measure to all-zeros with probability at least  $1/2 - \epsilon$  and all-ones with probability at least  $1/2 - \epsilon$ . Then there exists an  $n$ -nekomata  $|\nu\rangle$  such that  $|\langle\nu|\varphi\rangle|^2 \geq 1 - 2\epsilon$ .*

**Proof.** Suppose that the first  $n$  qubits of  $|\varphi\rangle$  are the targets. Then, the state

$$|\nu\rangle = \frac{1}{\sqrt{2}} \sum_{b \in \{0,1\}} \frac{|b^n\rangle\langle b^n| \otimes \mathbb{I} |\varphi\rangle}{\| |b^n\rangle\langle b^n| \otimes \mathbb{I} |\varphi\rangle \|}$$

is an  $n$ -nekomata and

$$|\langle\varphi|\nu\rangle|^2 = \left( \frac{1}{\sqrt{2}} \sum_{b \in \{0,1\}} \| |b^n\rangle\langle b^n| \otimes \mathbb{I} |\varphi\rangle \| \right)^2 \geq \frac{1}{2} \left( \sqrt{1/2 - \epsilon} + \sqrt{1/2 - \epsilon} \right)^2 = 1 - 2\epsilon \quad \blacktriangleleft$$

As mentioned, a parity-restricted gate can be thought of as a “weak” parity gate in the sense that it correctly computes parity on some  $\frac{1+\epsilon}{2}$ -fraction of the inputs. The idea behind our construction is to use these “weak” parity gates to prepare many bad, but not horrible approximate cat states in parallel. These bad, but not horrible cat states are of the form

$$|\phi\rangle = \sqrt{p_0} |0^n\rangle + \sqrt{p_1} |1^n\rangle + \sqrt{\epsilon} |\omega\rangle$$

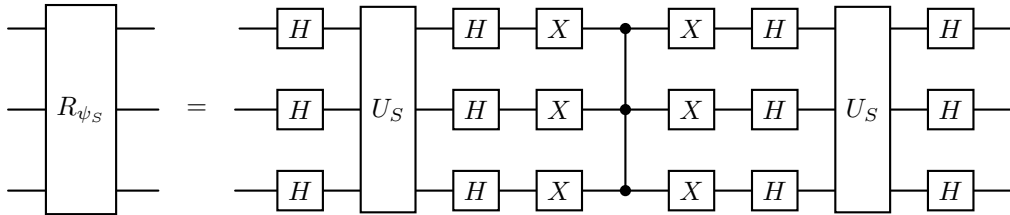
where  $|\omega\rangle$  is orthogonal to  $|b^n\rangle$  for  $b \in \{0,1\}$ . These initial states are bad approximate cat states in the sense that they may have little overlap with the cat state, but aren’t horrible because the distributions corresponding to their measurement outcomes are peaked only at  $|0^n\rangle$  and  $|1^n\rangle$ . In the final stage of our construction we accrue the distributions on each of these bad cat states into some  $n$  target qubits using Toffoli gates. We then show that for the right choice of parameters this accruing step effectively amplifies the original bad, but not horrible, distribution given by each of the weak parity gates in parallel. The final result is a good approximate nekomata.

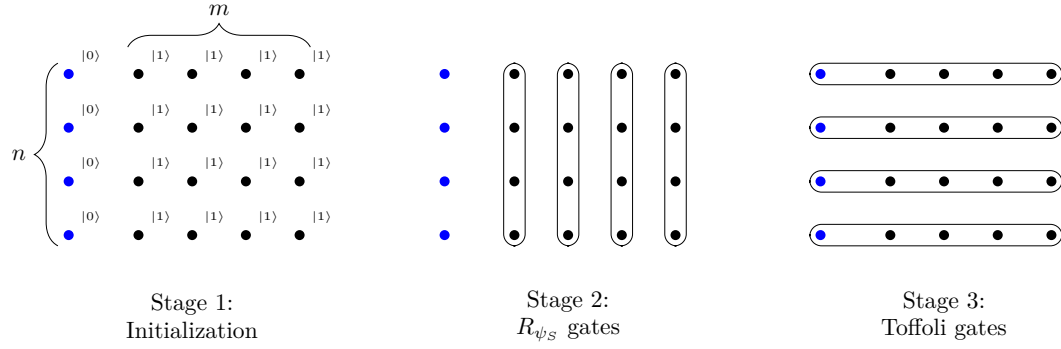
► **Theorem 19.** *For any parity-restricted  $S \subseteq \{0,1\}^n$  with  $|S| \leq 2^{n-4}$  there exists a depth-4,  $O(n + \frac{2^{2n}}{|S|^2})$ -size  $\text{QAC}_S$  circuit that constructs an  $O(|S|^2 2^{-2n})$ -approximate nekomata.*

**Proof.** The  $\text{QAC}_S$  circuit will act on  $n(m+1)$  qubits arranged in a grid of width  $m+1$  and height  $n$ . The first column will be designated as the “target” qubits, initialized to  $|0^n\rangle$  and all other columns initialized to  $|1^n\rangle$  (say, with a layer of  $X$  gates). To each non-target column apply an  $R_{\psi_S} = \mathbb{I} - 2|\psi_S\rangle\langle\psi_S|$  gate, where  $|\psi_S\rangle = H^{\otimes n} U_S H^{\otimes n} |0^n\rangle$ . Note that this can be implemented in depth-3 as

$$\mathbb{I} - 2|\psi_S\rangle\langle\psi_S| = H^{\otimes n} U_S H^{\otimes n} (\mathbb{I} - 2|0^n\rangle\langle 0^n|) H^{\otimes n} U_S H^{\otimes n}$$

which looks like the following quantum circuit:





■ **Figure 1** Constructing a nekomata from  $U_S$  and Toffoli gates. Target qubits are shown in blue. Here  $R_{\psi_S}$  is a rotation about the state  $|\psi_S\rangle = \frac{1}{|S|} \sum_{x \in S} |x\rangle$  discussed further below.

Finally, apply a Toffoli gate along each row with the output qubit being the corresponding target qubit (i.e. the qubit in the first column). We will now show that the probability that the target column is measured (in the computational basis) as  $|b^n\rangle$  is at least  $\frac{1}{2} - \frac{|S|}{2^{n-2}}$  for  $b \in \{0, 1\}$ .

To start, let

$$\begin{aligned} \gamma_0 &:= \langle 0^n | \psi_S \rangle^2 = \langle 0^n | H^{\otimes n} U_S H^{\otimes n} | 0^n \rangle^2 \\ &= \left[ \langle 0^n | \left( |0^n\rangle - \frac{1}{2^{n-1}} \sum_{s \in S} \sum_{x \in \{0,1\}^n} (-1)^{\langle x, s \rangle} |x\rangle \right) \right]^2 \\ &= \left( 1 - \frac{|S|}{2^{n-1}} \right)^2 \end{aligned}$$

and

$$\begin{aligned} \gamma_1 &:= \langle 1^n | \psi_S \rangle^2 = \langle 1^n | H^{\otimes n} U_S H^{\otimes n} | 0^n \rangle^2 \\ &= \left[ \langle 1^n | \left( |0^n\rangle - \frac{2}{2^n} \sum_{s \in S} \sum_{x \in \{0,1\}^n} (-1)^{\langle x, s \rangle} |x\rangle \right) \right]^2 \\ &= \left( \frac{1}{2^{n-1}} \sum_{s \in S} (-1)^{|s|} \right)^2 \\ &= \frac{|S|^2}{2^{2n-2}} \end{aligned}$$

where the last line follows from the fact that  $S$  is parity-restricted. For  $b \in \{0, 1\}$ , let  $p_b$  be the probability that a given non-target column yields  $|b^n\rangle$  after measuring in the computational basis. We have

$$\begin{aligned} p_0 &= \langle 0^n | (\mathbb{I} - 2 |\psi_S\rangle \langle \psi_S|) | 1^n \rangle^2 = 4\gamma_0\gamma_1 \\ p_1 &= \langle 1^n | (\mathbb{I} - 2 |\psi_S\rangle \langle \psi_S|) | 1^n \rangle^2 = (1 - 2\gamma_1)^2 \end{aligned}$$

Notice that, in fact,  $\gamma_1$  is maximized when  $S$  is parity-restricted (at least among sets of the same size as  $S$ ). This, in turn, minimizes the probability that any given column is measured as  $|1^n\rangle$  (though this will still be the most likely outcome since  $|S| \leq 2^{n-4}$ ). Though, one may perform a similar analysis for sets  $S$  which are only approximately parity-restricted.

### 3:12 Quantum Threshold Is Powerful

Recall that after we've created these states along the column, we apply Toffoli gates along the rows. Let's now compute the probability that we measure all zeroes or all ones on the first column. Note that computational basis measurements commute with Toffoli gates of any size, so in order for the targets to be measured as  $|1^n\rangle$  all other columns must also be measured as  $|1^n\rangle$ . Let  $m = \lfloor \frac{-\ln(2)}{2\ln(1-2\gamma_1)} \rfloor$ , then

$$\begin{aligned} \mathbb{P}[\text{Targets measure } |1^n\rangle] &= (1 - 2\gamma_1)^{2m} \\ &> (1 - 2\gamma_1)^{\frac{-\ln(2)}{\ln(1-2\gamma_1)} + 1} \\ &= \frac{1}{2}(1 - 2\gamma_1) \\ &= \frac{1}{2} - \frac{|S|^2}{2^{2n-2}} \end{aligned}$$

Now, call a non-target column “bad” if it is measured as anything other than  $|0^n\rangle$  or  $|1^n\rangle$ . Via a union bound,

$$\begin{aligned} \mathbb{P}[\text{Some column is bad}] &\leq m(1 - p_0 - p_1) = m(1 - 4\gamma_0\gamma_1 - (1 - 2\gamma_1)^2) \\ &= 4m\gamma_1(1 - \gamma_0 - \gamma_1) \end{aligned}$$

Observe that

$$\frac{1}{2}(1 - 2\gamma_1) = (1 - 2\gamma_1)^{\frac{-\ln(2)}{\ln(1-2\gamma_1)} + 1} \leq (1 - 2\gamma_1)^{2m} \leq \exp(-4m\gamma_1),$$

so  $4m\gamma_1 \leq -\ln(\frac{1}{2} - \gamma_1) < 1$  as  $\gamma_1 \leq \frac{1}{16}$ . So,

$$\begin{aligned} 4m\gamma_1(1 - \gamma_0 - \gamma_1) &< 1 - \gamma_0 - \gamma_1 \\ &\leq \frac{|S|}{2^{n-2}} \end{aligned}$$

Thus, every column is good with probability at least  $1 - \frac{|S|}{2^{n-2}}$  and the targets are measured as  $|0^n\rangle$  with probability at least  $1 - \frac{|S|}{2^{n-2}} - (\frac{1}{2} - \frac{|S|^2}{2^{2n-2}}) \geq \frac{1}{2} - \frac{|S|}{2^{n-2}}$ . By Lemma 18, the state produced is an  $\frac{|S|}{2^{n-3}}$ -approximate nekomata. Also, note that  $m = \Theta(1/\gamma_1)$ , hence the circuit has size  $O(n + m) = O(n + \frac{2^{2n}}{|S|^2})$ . ◀

Note that  $|S|$  affects our construction in two *distinct* ways. First, the bound we obtain on the probability that some non-target column is bad is proportional to the size of  $S$ , i.e.,  $\frac{|S|}{2^{n-2}}$ . This exactly corresponds to the approximation guarantee on the final approximate nekomata state. In particular, this means that for very large parity-restricted sets the approximation guarantee becomes quite poor. On the other hand, we choose  $m = \Theta(\frac{2^{2n-2}}{|S|^2})$  so that the entire grid is measured as  $|1^n\rangle^{\otimes m}$  with probability very close to  $\frac{1}{2}$ . This means that the number of columns in the grid shrinks as  $|S|$  grows. The main takeaway is that this construction results in a tradeoff between the quality of the approximate nekomata state and circuit size depending on  $|S|$ .

It may seem peculiar that we require  $S$  to not be too large in Theorem 19, but this is indeed necessary. Intuition suggests that  $U_S$  should approximate the parity gate better when  $|S|$  approaches  $2^{n-1}$ . In some sense, this is true: if  $|S| = 2^{n-1}$ , then  $U_S$  exactly computes parity (or its negation) in the phase. In this extreme setting, unfortunately,  $U_S$  ceases to be a useful multi-qubit gate, as it is simply  $\pm Z^{\otimes n}$ . Roughly, as  $|S|$  grows too large,  $U_S$  no longer becomes useful for preparing column-states with the peaked measurement distributions

exploited in the grid construction as a result of how weakly entangling the  $U_S$  gate becomes. However, if you weakly approximate parity as a classical reversible gate (instead of in the phase) there is another set of techniques which allow for very large parity-restricted gates to be bootstrapped to approximately compute parity. This is further discussed in Section 3.2.

It should also be noted that by applying  $Z^{\otimes n}$  to  $U_S$  yields  $U_T$  where  $T$  is a parity restricted set of size  $2^{n-1} - |S|$ , which can be used to achieve a similar grid construction with different size and accuracy parameters.

Finally, let's compare our construction to that of Rosenthal [21], which only requires generalized Toffoli gates. If one takes  $S$  to be a singleton set then  $U_S$  is locally-equivalent to a generalized Toffoli gate and the resulting constructions have similar guarantees. However, one critical difference is the fact that the present construction has depth-4 while Rosenthal's is only depth-2 since it uses column states  $H^{\otimes n} U_S H^{\otimes n} |1^n\rangle$ . Let us analyze roughly what goes wrong in the present construction if we were to use the same state. First, let  $d_S := \frac{|S|}{2^{n-1}}$  be the density of  $S$ . We have  $d_S$  and  $1 - d_S$  are the amplitudes on the states  $|0^n\rangle$  and  $|1^n\rangle$ , respectively. Following the previous analysis, we find that all columns measure  $|1^n\rangle$  with probability  $(1 - d_S)^{2^m}$  and the probability that some column measures  $|0^n\rangle$  is  $1 - (1 - d_S^2)^m$ . This means that if  $(1 - d_S)^{2^m} \approx \frac{1}{2}$  then  $m = \Theta(1/d_S)$ , but  $(1 - d_S^2)^m$  tends to 1 when  $m = \Theta(1/d_S)$ , so it seems that a depth-2 construction just using Hadamard and  $U_S$  gates may not be possible (at least with these techniques). However, it may be possible to obtain a depth-2 construction here by using some single-qubit gate other than the Hadamard (as Rosenthal does), but this will lead to a slightly more complicated analysis.

► **Corollary 20.** *If  $S \subset \{0,1\}^*$  is a parity-restricted set satisfying  $\frac{2^n}{|S \cap \{0,1\}^n|} = O(n^a)$  and  $\frac{2^n}{|S \cap \{0,1\}^n|} = \Omega(n^b)$  for some constants  $a, b > 0$  then  $\text{BQAC}_S^0 \supseteq \text{BQNC}_{wf}^0$ .*

**Proof.** Observe that the construction in Theorem 19 yields a constant-depth  $\text{QAC}_S$  circuit of size  $O(n + \frac{2^{2n}}{|S \cap \{0,1\}^n|^2}) = O(n + n^{2a}) = \text{poly}(n)$  which prepares an  $O(n^{-b})$ -approximate nekomata on  $n$  qubits. Via Lemma 16 this circuit can be leveraged to compute  $F_n$  with approximation error  $O(n^{-b})$ . Note that we can make the error an arbitrarily small polynomial by making the circuit polynomially larger. That is, suppose we want to construct an  $O(n^{-c})$ -approximate  $n$ -nekomata for some  $c > b$ . Simply use the construction above for an  $n^{c/b}$ -nekomata, but only use  $n$  of the targets (i.e., any  $n^{c/b}$ -nekomata is an  $n$ -nekomata for  $c > b$ ). The circuit will have size  $O(n^{ac/b})$  and error at most  $O(n^{-c})$ . Therefore, by Lemma 16, there are poly-size  $\text{QAC}_S^0$  circuits to compute Fanout to arbitrary polynomial precision, so  $\text{BQAC}_S^0 \supseteq \text{BQNC}_{wf}^0$ . ◀

Next, we argue that Threshold gates can be used to hit the “sweet spot” of Theorem 19. Namely, they correspond to parity-restricted sets of the right size to make the size and accuracy of the above construction polynomial.

► **Corollary 21.**  $\text{BQTC}^0 = \text{BQNC}_{wf}^0$

**Proof.** Without a loss of generality assume  $n$  is even, otherwise this can be rectified with a single ancilla qubit. Let  $S = \{x \in \{0,1\}^n : |x| = \frac{n}{2}\}$ , i.e.,  $S$  is the Hamming slice of weight  $\frac{n}{2}$ . Note that  $|x| = \frac{n}{2}$  if and only if  $\text{Maj}(x_1, \dots, x_n) = 1$  and  $\text{Maj}(x_1, \dots, x_n, 0) = 0$ , thus the  $U_S$  gate can be implemented in depth 2 by applying  $\text{Maj}_n$  once to  $|\psi\rangle$ , tacking on an ancilla qubit set to  $|0\rangle$  then applying another  $\text{Maj}_n$  gate to  $|\psi\rangle |0\rangle$ . In this case the circuit from Theorem 19 has size  $s = O(n + \frac{2^{2n}}{|S|^2})$  and produces an  $\epsilon = \frac{|S|}{2^{n-3}}$ -approximate nekomata. Since

$$\binom{n}{n/2} \in \left[ \frac{2^n}{\sqrt{2n}}, \frac{2^n}{\sqrt{n\pi/2}} \right]$$

via Stirling's formula, it follows that  $s = O(n)$  and  $\epsilon = O(\frac{1}{\sqrt{n}})$ . Via Corollary 20,  $\text{BQTC}^0 = \text{BQNC}_{wf}^0$ . ◀

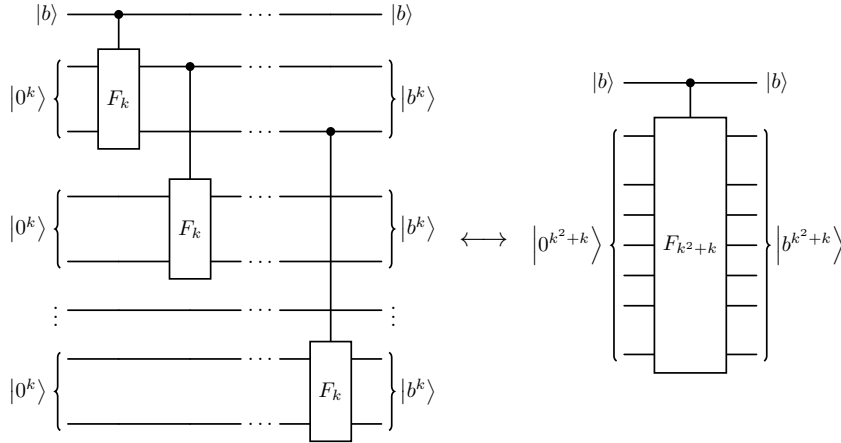
► **Theorem 22.** *The following tasks are equivalent under  $\text{QAC}^0$  reductions:*

1. *Preparation of  $\frac{1}{\text{poly}(n)}$ -approximate nekomata from the all zeros state and the inverse transformation for some polynomial  $p$*
2. *Approximately computing  $\text{Th}_{n,k}$  to error  $\frac{1}{\text{poly}(n)}$  for any  $k = \text{poly}(n)$*
3. *Approximately computing  $\text{EX}_{2k-2,k-1}$  to error  $\frac{1}{\text{poly}(n)}$  for any  $k = \text{poly}(n)$*

**Proof.** Observe that for  $x \in \{0, 1\}^{2k-2}$   $\text{EX}_{2k-2,k-1}(x) = \text{Th}_{2k-2,k-1}(x) \wedge \overline{\text{Th}_{2k-2,k}(x)}$  and we can implement this directly by first applying  $U$  to  $|x\rangle |10^{n-(2k-2)-1}\rangle$  and then to  $|x\rangle |0^{n-(2k-2)}\rangle$  for any  $U$  which computes  $\text{Th}_{n,k}$  to inverse-polynomial precision. Thus, (2)  $\implies$  (3).

Via Theorem 19 a unitary  $V$  approximately computes  $\text{EX}_{2k-2,k-1}$  to inverse-polynomial error can be leveraged in constant-depth to prepare an  $\frac{1}{\text{poly}(k)}$ -approximate nekomata on  $k$  qubits. In fact, this construction will yield an approximate nekomata on  $2k - 2$  qubits, but as mentioned in the proof of Corollary 20, an approximate nekomata on  $2k - 2$  is also an approximate nekomata on  $k$  qubits. This circuit (and the inverse transformation) can be used to compute  $F_k$  to the same precision, up to constants (Lemma 16). Observe that iteratively applying  $F_k$  in a tree-like fashion allows us to apply fanout to a number of qubits that is exponential in the depth. In particular, using  $F_k$  gates we can construct  $F_{k^d}$  in depth  $d$  by stacking  $F_k$  gates on the qubits which we have fanned-out onto in the previous layer (see Figure 2). This means that as long as  $k = n^\alpha$  for some  $\alpha = \Omega(1)$  we can take  $d = O(1/\alpha) = O(1)$  and approximately compute  $F_n$  to the same precision. Hence, (3)  $\implies$  (1).

Finally, (1)  $\implies$  (2) can be seen by applying the construction of [13] which allows us to approximately compute any threshold gate on  $\text{poly}(n)$  qubits via a  $\text{QNC}_{wf}^0$  circuit. ◀



■ **Figure 2** Iteratively applying  $F_k$  in a tree-like fashion. In the above, we achieve fanout  $k^2 + k$  in depth-2 using  $F_k$  gates.

## 3.2 Removing the Toffoli gates

The construction presented in Theorem 19 for generic  $S$  requires large Toffoli gates, however we will show that for some regimes of  $|S|$ , these gates are unnecessary, i.e.,  $\text{QNC}_S^0$  circuits can exactly compute Toffoli on polynomially many qubits. We will show that this is indeed

the case when  $|S| \geq 2^{n-O(1)}$  and  $|S| \leq 2^{(1-\epsilon)n}$  for a fixed constant  $\epsilon < 1$ . Though for this result we require the use of  $U_{f_S}$  gates, i.e., those gates which check membership in  $S$  as  $U_{f_S}|x\rangle|b\rangle = |x\rangle|f(x) \oplus b\rangle$  where  $f(x) = 1$  iff  $x \in S$ .

► **Lemma 23.** *Let  $c$  be constant, and let  $S$  be a parity restricted set with size  $|S| \geq 2^{n-c}$  and strings of parity  $b \in \{0, 1\}$ . Then, there exist some  $c-1$  bit-strings  $t_1, t_2, \dots, t_{c-1} \in \{0, 1\}^n$  such that  $|x| \equiv b \pmod{2}$  iff*

$$\bigvee_{y \in \text{Span}(t_1, \dots, t_{c-1})} \{x \oplus y \in S\}$$

is satisfied.

**Proof.** Suppose that  $b = 0$ . Let  $\mathcal{E} \subset \mathbb{F}_2^n$  be the subspace of dimension  $n-1$  consisting of vectors of even Hamming weight. Observe that  $S \subseteq \mathcal{E}$ , and moreover that  $S$  contains at least  $n-c$  linearly independent elements of  $\mathcal{E}$ . Therefore, there exist some  $t_1, \dots, t_{c-1} \in \mathcal{E}$  such that  $S \cup \{t_1, \dots, t_{c-1}\}$  span  $\mathcal{E}$ . Hence, every element of  $\mathcal{E}$  can be written as  $s \oplus y$  for some  $s \in S$  and  $y \in \text{span}\{t_1, \dots, t_{c-1}\}$ . Thus,  $|x| \equiv 0$  iff the disjunction is satisfied.

If  $b = 1$  then the set  $S'$  obtained by flipping the first bit of every element of  $S$  contains vectors of even Hamming weight - further,  $S'$  contains at least  $n-c$  linearly independent vectors. So, take  $\{t_1, \dots, t_{c-1}\}$  as before such that  $S' \cup \{t_1, \dots, t_{c-1}\}$  spans  $\mathcal{E}$ . Any vector of even Hamming weight,  $y \in \mathbb{F}_2^n$ , can be expressed as  $y = s' + t'$  for some  $s' \in S'$  and  $t' \in \text{Span}(t_1, \dots, t_{c-1})$ . Now, observe that if  $x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$  has odd Hamming weight then  $(x_1 \oplus 1, \dots, x_n)$  can be expressed as  $s' + t'$  for some  $s' \in S'$  and  $t' \in \text{Span}(t_1, \dots, t_{c-1})$ . Since  $s' = (s_1 \oplus 1, s_2, \dots, s_n)$  for some  $s = (s_1, s_2, \dots, s_n) \in S$ , it follows that  $x$  has odd Hamming weight iff the disjunction is satisfied. ◀

As shown above, if  $|S| \geq 2^{n-c}$  for some constant  $c$  then we can extend  $S$  linearly to “cover” all strings of a fixed Hamming weight. To implement a parity gate in this way, one can encode every linear combination  $t' \in \text{Span}(t_1, \dots, t_c)$  in the ancilla and then apply a  $U_{f_S}$  gate to  $|x \oplus t'\rangle$  for every  $t'$  - this can be done in constant depth using only  $U_{f_S}$  and CNOT gates since  $|\text{Span}(t_1, \dots, t_c)| = 2^c = O(1)$ . If any of these  $U_{f_S}$  gates evaluate to 1 then  $x$  must have Hamming weight consistent with that of the strings in  $S$ , in effect computing the parity of  $x$ . We will now see how generalized Toffoli can be computed with just  $U_{f_S}$  and CNOT gates when  $|S|$  is sufficiently small.

► **Lemma 24.** *For any  $S \subseteq \{0, 1\}^n$  there exists some  $s \in S$  and some subset of indices  $\{i_1, i_2, \dots, i_k\}$  such that  $s$  is the unique  $x \in S$  which satisfies  $x_{i_j} = s_{i_j}$  for all  $j \in [k]$ . Further,  $k \leq \log |S|$ .*

**Proof.** Note that unless  $|S| = 1$  there exists some index on which elements of  $S$  take different values. If  $|S| = 1$  we are done and can take this single element to be  $s$ . Otherwise, let  $i_1$  be the first index on which elements of  $S$  take different values. We will now partition  $S$  into two sets  $S_0^1$  and  $S_1^1$  where  $S_b^1 = \{s \in S \mid s_{i_1} = b\}$ . Take  $T_1$  to be the set with fewer elements and repeat this procedure, defining  $T_j$  similarly for  $j > 1$ . Since  $|T_{j+1}| \leq \frac{|T_j|}{2}$  for  $j \geq 1$ , it follows that for some  $k > 1$ ,  $|T_k| = 1$  and it follows that  $k \leq \log |S|$ . ◀

Now, when  $|S|$  is sufficiently small, there is always some way to fix a small number ( $\log |S|$ ) of bits so that the unfixed bits have a unique assignment consistent with  $S$ . In particular, if  $|S| \leq 2^{(1-\epsilon)n}$  for some constant  $\epsilon \in (0, 1)$  then there exists some partial assignment of at most  $(1-\epsilon)n$  bits such that for the remaining  $\epsilon n$  bits there is a unique assignment such that



the resulting string is a member of  $S$ . For simplicity, suppose that the partial assignment is on the first  $(1 - \epsilon)n$  as  $y \in \{0, 1\}^{(1-\epsilon)n}$  and that the unique assignment for the remaining bits which is consistent with  $S$  is  $z \in \{0, 1\}^{\epsilon n}$ . Now, for  $x \in \{0, 1\}^{\epsilon n}$  we can see that

$$U_{f_S} |y\rangle |x\rangle |0\rangle = |y\rangle |x\rangle |\mathbb{I}_z(x)\rangle$$

In this way, after fixing the first  $(1 - \epsilon)n$  bits to  $y$  forces  $U_{f_S}$  to act like a  $U_{f_{\{z\}}}$  gate on the remaining qubits. This gate is locally equivalent to a Toffoli gate; we can just apply  $X$  gates to the wires on which  $z_i = 0$ . Since  $\epsilon$  is a constant, we can repeat this procedure  $1/\epsilon$  times to implement the Toffoli gate on  $n$  qubits in constant depth. In this way, we can directly implement generalized Toffoli gates in the grid construction of Theorem 19 using the  $U_{f_{S_n}}$  gates when  $|S|$  is sufficiently small.

► **Corollary 25.** *For any parity restricted set  $S$  which satisfies  $|S| \geq \Omega(2^n)$  or  $|S| \leq 2^{(1-\epsilon)n}$  for some fixed  $\epsilon \in (0, 1)$  there exist constant-depth  $\text{QNC}_S$  circuits of size  $O(n + \frac{2^{2n}}{|S|^2})$  which prepare  $O(\frac{|S|^2}{2^{2n}})$ -approximate nekomata. In particular, for  $S \subset \{0, 1\}^*$  which are parity restricted and satisfy  $\frac{2^n}{|S \cap \{0, 1\}^n|} = \text{poly}(n)$ ,  $\text{BQNC}_S^0 \supseteq \text{BQNC}_{wf}^0$ .*

#### 4 Quantum MOD gates are powerful even on their own

In this section we show a strengthening of a result of [8]. In particular they show that for any fixed  $q > 1$   $\text{MOD}_{n,q}$  gates,  $\wedge_n$  gates, single- and two-qubit gates can be leveraged to implement Fanout in constant depth and polynomial size:

► **Theorem 26** (Theorem 4.6 of [8]). *For  $p \geq 2$ ,  $\text{QAC}^0[p] = \text{QAC}_{wf}^0$ .*

However, the family of  $\text{QAC}^0[p]$  circuits they construct does not actually require  $\wedge_n$  gates, i.e., the family of circuits they construct to compute  $F_n$  is actually a  $\text{QNC}^0[p]$  family. This immediately yields the collapse of all  $\text{QNC}^0[p]$ :

► **Theorem 27.**  $\text{QNC}^0[p] = \text{QNC}_{wf}^0$  for all primes  $p$ .

Combined with the results of [13] and [24] we have an even larger collapse of constant-depth circuit classes:

$$\text{QNC}^0[p] = \text{QNC}_{wf}^0 = \text{QAC}_{wf}^0 = \text{QAC}^0[q] = \text{QTC}_{wf}^0$$

for all  $p, q \geq 2$ . Before showing and analyzing the construction we will introduce some preliminaries.

##### 4.1 Simulating qudit arithmetic in $\text{QNC}^0[p]$

By a proposition of Moore, in order to implement  $F_n$  it actually suffices to construct a circuit which behaves like  $F_n$  when all but the one qubit to be fanned-out are set to  $|0\rangle$ :

► **Proposition 28** (Proposition 1 of [17]). *In any class of quantum circuits which includes Hadamard and CNOT-gates, the follow are equivalent in constant depth:*

1. *It is possible to map  $(\alpha|0\rangle + \beta|1\rangle)|0^{n-1}\rangle$  to  $\alpha|0^n\rangle + \beta|1^n\rangle$  and from  $\alpha|0^n\rangle + \beta|1^n\rangle$  to  $(\alpha|0\rangle + \beta|1\rangle)|0^{n-1}\rangle$  for all  $|\alpha|^2 + |\beta|^2 = 1$*
2.  *$F_n$  can be implemented with at most  $n - 1$  ancilla qubits*
3.  *$P_n$  can be implemented with at most  $n - 1$  ancilla qubits*

Hence, constructing a unitary  $U$  which satisfies  $U(\alpha|0\rangle + \beta|1\rangle) \otimes |0^{n-1+a(n)}\rangle = (\alpha|0^n\rangle + \beta|1^n\rangle) |0^{a(n)}\rangle$  for any single-qubit state  $\alpha|0\rangle + \beta|1\rangle$  will result in the ability to compute Fanout; this is exactly what the construction does.

First, for a fixed prime  $p$  consider the qudit generalizations of the Parity and Fanout gates for local dimension  $p$ :

$$\begin{aligned} M_{n,p} |b\rangle |x_1 x_2 \cdots x_n\rangle &= |b - |x| \pmod{p}\rangle |x_1 x_2 \cdots x_n\rangle \\ F_{n,p} |b\rangle |x_1 x_2 \cdots x_n\rangle &= |b\rangle |(x_1 + b \pmod{p}), (x_2 + b \pmod{p}), \dots, (x_n + b \pmod{p})\rangle \end{aligned}$$

where  $x_1, \dots, x_n, b \in \{0, \dots, p-1\}$ .

Additionally, consider the following single-qudit gate:

$$Q_p |b\rangle = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \omega^{jb} |j\rangle$$

where  $\omega = e^{2i\pi/p}$ . For example, when  $p = 2$ ,  $Q_p = H$ , and  $F_{n,p}$  and  $M_{n,p}$  are the usual Fanout and Parity gates for qubits, respectively.

► **Lemma 29** (Proposition 4.2 of [8]).  $M_{n,p} = (Q_p^\dagger)^{\otimes(n+1)} F_{n,p} Q_p^{\otimes(n+1)}$

Recall our goal: we want to use Mod- $p$  gate to simulate Fanout over qubits. While this seems somewhat challenging for qubits, it is trivial over qudits of local dimension  $p$  by Lemma 29. Therefore, our plan will be to pretend that we are in that setting by encoding a qudit using several qubits. Once we have set an encoding, we need encoded versions of the  $M_{n,p}$  and  $Q_p$  gates in Lemma 29. Encoding the  $Q_p$  gate is easy – it's a gate of constant-size and each one of our encoded qudits will be of constant size, so any brute force encoding of  $Q_p$  will do. The challenging step is to show that an encoded  $M_{n,p}$  gate is possible using (qubit) MOD $_{n,p}$  gates. One of the key observations is that after we've applied the encoded Fanout, we will have accomplished Task 1 of Proposition 28, and therefore, we can construct general Fanout over qubits.

**Proof of Theorem 27.** To start, define a linear encoding map  $E: \mathbb{C}^p \rightarrow (\mathbb{C}^2)^{\otimes p}$  which maps from qudits of local dimension  $p$  to a tensor product of  $p$  qubits:

$$E |j\rangle = \bigotimes_{k=0}^{p-1} |\delta_{k,j}\rangle$$

for all  $j \in \{0, \dots, p-1\}$  and where  $\delta_{k,j}$  denotes the Kronecker delta function. Note that  $E$  is a linear map of full rank from the  $p$ -dimensional space spanned by  $\{|j\rangle\}_{j=0}^{p-1}$  to the  $p$ -dimensional

subspace of  $(\mathbb{C}^2)^{\otimes n}$  spanned by  $\left\{ \bigotimes_{k=0}^{p-1} |\delta_{k,j}\rangle \right\}_{j=0}^{p-1}$ . Throughout this construction we will

only be working over qubits and not actually implementing  $E$ . Instead, we will be exploiting the equivalence of Lemma 29 by simulating qudit arithmetic with qubits. We introduce  $E$  for the sake of describing this simulation method succinctly.

Now, applying  $Q_p$  to an encoded state on qubits amounts to implementing any  $\tilde{Q}_p$  which satisfies:

$$\tilde{Q}_p |\delta_{0,j}\rangle |\delta_{1,j}\rangle \cdots |\delta_{p-1,j}\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \omega^{jk} |\delta_{0,k}\rangle |\delta_{1,k}\rangle \cdots |\delta_{p-1,k}\rangle$$

i.e., any unitary  $\tilde{Q}_p$  on  $(\mathbb{C}^2)^{\otimes p}$  which respects the homomorphism induced by  $E$ . Since  $p$  is fixed, any such  $\tilde{Q}_p$  operates on constantly many qubits and can be implemented in constant depth and size.

### 3:18 Quantum Threshold Is Powerful

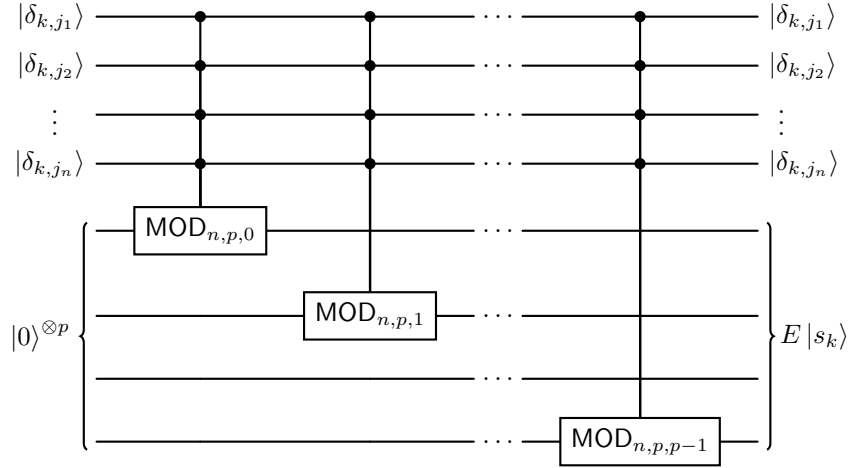
Now, we must implement  $M_{n,p}$  on the encoded subspace using just  $\text{MOD}_{n,p}$  (and one- and two-qubit gates). Note that for any  $j_1, \dots, j_n \in \mathbb{F}_p$  their sum modulo  $p$  can be decomposed

$$\begin{aligned} j_1 + \dots + j_n &\equiv 0(\delta_{0,j_1} + \dots + \delta_{0,j_n}) + 1(\delta_{1,j_1} + \dots + \delta_{1,j_n}) + \dots + (p-1)(\delta_{p-1,j_1} + \dots + \delta_{p-1,j_n}) \\ &\equiv \sum_{k=0}^{p-1} k \left( \sum_{i=1}^n \delta_{k,j_i} \right) \pmod{p} \end{aligned}$$

Let  $s_k := \sum_{i=1}^n \delta_{k,j_i} \pmod{p}$  be the number of  $j_i$  terms equal to  $k$  modulo  $p$ . Let's also define a family of generalized Mod- $p$  gates over qubits. For  $\ell \in \{0, \dots, p-1\}$ , recall  $\text{MOD}_{n,p,\ell}$  acts as

$$\text{MOD}_{n,p,\ell} |b\rangle |x_1, \dots, x_n\rangle = |b \oplus \text{Mod}_{n,p,\ell}(x)\rangle |x_1, \dots, x_n\rangle$$

Notice that  $\text{MOD}_{n,p,\ell}$  can be implemented over qubits with an  $\text{MOD}_{n,p,0}$  gate (the standard  $\text{MOD}_{n,p}$  gate on qubits) and  $p-1$  additional ancilla qubits,  $p-\ell$  of which are set to 1. We can use these gates to compute  $s_k$  for a given  $k \in \{0, 1, \dots, p-1\}$ :



For  $k \in \{0, \dots, p-1\}$  the above circuit, can be applied in parallel to the appropriate qubits in the encoding; namely those of the form  $|\delta_{k,j}\rangle$  for fixed  $k$ . This leaves us with the state  $E |s_0\rangle \otimes \dots \otimes E |s_{p-1}\rangle$ . Recall that the sum over  $\mathbb{F}_p$  we wish to compute is  $\sum_{i=1}^n j_i = \sum_{k=0}^{p-1} k s_k$ ; so, if we can compute each of  $k s_k$  and sum over all  $k$ , we will be left with the desired sum. However, the product  $k s_k$  is over elements of  $\mathbb{F}_p$  and  $p$  is fixed, so it is clear that this can be computed in  $\text{QNC}^0$  ( $\text{NC}^0$  even). Further,  $\sum_{k=0}^{p-1} k s_k$  is a sum of constantly many integers each described by  $p = O(1)$  bits, which is of course computable by a  $\text{QNC}^0$  ( $\text{NC}^0$  even) circuit.

For the sake of completeness, we will describe a circuit composed of permutations on  $p$  qubits which computes  $\sum_{k=0}^{p-1} k s_k$  in our encoded subspace. First let  $U_\sigma$  be the permutation unitary which satisfies  $U_\sigma E |j\rangle = E |j-1 \pmod{p}\rangle$ . For any  $k \in \{0, 1, \dots, p-1\}$ ,  $U_\sigma^k$  can be implemented in constant depth via a sequence of at most  $p^2$  swap gates. Since  $U_\sigma^a E |j\rangle = E |j-a\rangle$  for all  $a, j \in \mathbb{F}_p$ , we can in series apply  $U_\sigma^{k s_k}$  to  $E |b\rangle$  to finally achieve

$$\begin{aligned}
\left( \prod_{k=0}^{p-1} U_{\sigma}^{ks_k} \right) E |b\rangle &= U_{\sigma}^{\sum_{k=0}^{p-1} ks_k} E |b\rangle \\
&= U_{\sigma}^{\sum_{i=1}^n j_i} |b\rangle \\
&= E \left| b - \sum_{i=1}^n j_i \pmod{p} \right\rangle
\end{aligned}$$

Hence, this gives a circuit of depth  $p^3 = O(1)$  and linear size for simulating  $M_{p,n}$  on the encoded qudits. After conjugating by  $\tilde{Q}_p$  gates on the appropriate groups of qubits the equivalence of Lemma 29 shows that the entire circuit exactly implements fanout on the encoded qudits.

Let's now put all the pieces together to show that we can achieve Task 1 of Proposition 28. Starting with the state  $(\alpha |0\rangle + \beta |1\rangle) |0^{(p(n+1)-1)}\rangle$ , we want to get to an *encoding* of  $\alpha |0\rangle + \beta |1\rangle$  and the ancillary qubits. First, apply a CNOT gate from the first to second qubit, followed by an  $X$  gate on the first to obtain the state

$$(\alpha |10^{p-1}\rangle + \beta |010^{p-2}\rangle) \otimes |0^{pn}\rangle.$$

Now apply an  $X$  gate to the  $(pj+1)$ st qubit for  $j \in \{0, 1, \dots, n-1\}$  yielding the encoded state:  $E(\alpha |0\rangle + \beta |1\rangle) \otimes E|0^n\rangle$ . Note that this is a state on  $n+1$  qudits encoded by  $p(n+1)$  qubits. After applying the previously described circuit which simulates  $F_{n,p}$  on the encoded states the result is (up to a known permutation of the qubits)

$$(\alpha |0\rangle^{\otimes 2(n+1)} + \beta |1\rangle^{\otimes 2(n+1)}) \otimes |0^{(p-2)(n+1)}\rangle$$

Now, via Proposition 28 any such circuit is sufficient to compute Fanout (on qubits), thus  $\text{QNC}_{wf}^0 \subseteq \text{QNC}^0[p]$ . It is shown in [13] and [24] that the reverse inclusion holds and it can be concluded that  $\text{QNC}_{wf}^0 = \text{QNC}^0[p]$ . ◀

► **Corollary 30.**  $\text{QNC}^0[a] = \text{QNC}_{wf}^0$  for all  $a > 1$ .

**Proof.** This follows from the previous construction by taking  $p$  to be any prime factor of  $a$  and setting ancilla qubits appropriately or concatenating the input  $a/p$  times so that any  $\text{MOD}_a$  gate instead computes  $\text{MOD}_p$ . ◀

## References

- 1 Miklós Ajtai.  $\Sigma_1$ -formulae on finite structures. *Annals of pure and applied logic*, 24(1):1–48, 1983.
- 2 Anurag Anshu, Yangjing Dong, Fengning Ou, and Penghui Yao. On the computational power of  $\text{QAC}^0$  with barely superlinear ancillae. *arXiv preprint*, 2024. [arXiv:2410.06499](#).
- 3 Debajyoti Bera. A lower bound method for quantum circuits. *Information processing letters*, 111(15):723–726, 2011. doi:10.1016/J.IPL.2011.05.002.
- 4 Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.
- 5 Harry Buhrman, Marten Folkertsma, Bruno Loff, and Niels MP Neumann. State preparation by shallow circuits using feed forward. *arXiv preprint*, 2023. [arXiv:2307.14840](#).
- 6 Maosen Fang, Stephen Fenner, Frederic Green, Steven Homer, and Yong Zhang. Quantum lower bounds for fanout. *Quantum Information and Computation*, 6(1):046–057, 2006. doi:10.26421/QIC6.1–3.
- 7 Merrick Furst, James B Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical systems theory*, 17(1):13–27, 1984. doi:10.1007/BF01744431.

- 8 Frederic Green, Steven Homer, Cristopher Moore, and Christopher Pollett. Counting, fanout, and the complexity of quantum ACC. *arXiv preprint*, 2001. [arXiv:quant-ph/0106017](#).
- 9 Daniel Grier and Luke Schaeffer. Interactive shallow clifford circuits: quantum advantage against  $nc^1$  and beyond. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 875–888, 2020. doi:10.1145/3357713.3384332.
- 10 Alex Bredariol Grilo, Elham Kashefi, Damian Markham, and Michael de Oliveira. The power of shallow-depth Toffoli and qudit quantum circuits. *arXiv preprint*, 2024. doi:10.48550/arXiv.2404.18104.
- 11 Jonas Haferkamp, Dominik Hangleiter, Adam Bouland, Bill Fefferman, Jens Eisert, and Juani Bermejo-Vega. Closing gaps of a quantum advantage with short-time hamiltonian dynamics. *Physical Review Letters*, 125(25):250501, 2020.
- 12 Johan Håstad. *Computational limitations for small depth circuits*. PhD thesis, Massachusetts Institute of Technology, 1986.
- 13 Peter Høyer and Robert Špalek. Quantum fan-out is powerful. *Theory of computing*, 1(1):81–103, 2005. doi:10.4086/TOC.2005.V001A005.
- 14 Harry Levine, Alexander Keesling, Giulia Semeghini, Ahmed Omran, Tout T Wang, Sepehr Ebadi, Hannes Bernien, Markus Greiner, Vladan Vuletić, Hannes Pichler, et al. Parallel implementation of high-fidelity multiqubit gates with neutral atoms. *Physical review letters*, 123(17):170503, 2019.
- 15 Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, fourier transform, and learnability. *Journal of the ACM (JACM)*, 40(3):607–620, 1993. doi:10.1145/174130.174138.
- 16 Klaus Mølmer and Anders Sørensen. Multiparticle entanglement of hot trapped ions. *Physical Review Letters*, 82(9):1835, 1999.
- 17 Cristopher Moore. Quantum circuits: Fanout, parity, and counting. *arXiv preprint*, 1999. [arXiv:quant-ph/9903046](#).
- 18 Shivam Nadimpalli, Natalie Parham, Francisca Vasconcelos, and Henry Yuen. On the pauli spectrum of  $QAC^0$ . In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1498–1506, 2024.
- 19 Daniel Padé, Stephen Fenner, Daniel Grier, and Thomas Thierauf. Depth-2 QAC circuits cannot simulate quantum parity. *arXiv preprint*, 2020. [arXiv:2005.12169](#).
- 20 Alexander A Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mat. Zametki*, 41(4):598–607, 1987.
- 21 Gregory Rosenthal. Bounds on the  $QAC^0$  complexity of approximating parity. In *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*. Schloss Dagstuhl – Leibniz Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.ITCS.2021.32.
- 22 Mark Saffman and Klaus Mølmer. Efficient multiparticle entanglement via asymmetric Rydberg blockade. *Physical review letters*, 102(24):240502, 2009.
- 23 Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 77–82, 1987. doi:10.1145/28395.28404.
- 24 Yasuhiro Takahashi and Seiichiro Tani. Collapse of the hierarchy of constant-depth exact quantum circuits. *computational complexity*, 25:849–881, 2016. doi:10.1007/S00037-016-0140-0.
- 25 Barbara M Terhal and David P DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games. *arXiv preprint*, 2002. [arXiv:quant-ph/0205133](#).
- 26 Adam Bene Watts, Robin Kothari, Luke Schaeffer, and Avishay Tal. Exponential separation between shallow quantum circuits and unbounded fan-in shallow classical circuits. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 515–526, 2019. doi:10.1145/3313276.3316404.
- 27 Andrew Chi-Chih Yao. Separating the polynomial-time hierarchy by oracles. In *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*, pages 1–10. IEEE, 1985.

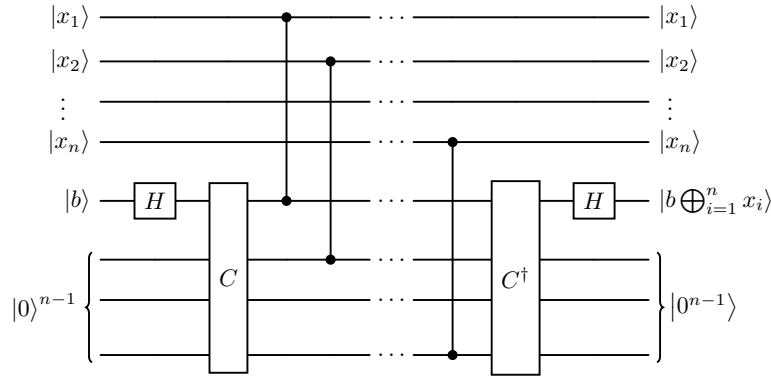
## A

 Deferred Proofs

**Proof of Proposition 28.** To see that (2)  $\iff$  (3) it suffices to conjugate either gate by Hadamard gates, i.e.,  $H^{\otimes(n+1)}F_nH^{\otimes(n+1)} = P_n$ . (2)  $\implies$  (1) because  $F_n$  satisfies the condition described in (1) exactly:

$$F_n(\alpha|0\rangle + \beta|1\rangle)|0^n\rangle = \alpha|0^{n+1}\rangle + \beta|1^{n+1}\rangle$$

and  $F_n$  is its own inverse. Let  $C$  be any unitary which satisfies (1). To see that (1)  $\implies$  (3) we construct a circuit using  $C$  and  $C^\dagger$  in essentially the same way that we did in the proof of Proposition 13:



To see that this circuit exactly computes parity note that after the first Hadamard gate is applied the ancilla bits are in the state  $\frac{|0\rangle + (-1)^b|1\rangle}{\sqrt{2}}|0^{n-1}\rangle$  and after applying  $C$  we have  $\frac{|0^n\rangle + (-1)^b|1^n\rangle}{\sqrt{2}}$ . After the CZ gates are applied we are left with the state  $\frac{|0^n\rangle + (-1)^{b+\sum_{i=1}^n x_i}|1^n\rangle}{\sqrt{2}}$ . After applying  $C^\dagger$  we are left with  $\frac{|0\rangle + (-1)^{b+\sum_{i=1}^n x_i}|1\rangle}{\sqrt{2}}|0^{n-1}\rangle$ , so the final Hadamard gate leaves the output qubit and the ancilla qubits in the state  $|b \oplus_{i=1}^n x_i\rangle|0^{n-1}\rangle$ . ◀

It should be noted that when our circuit  $C$  has property (1) it is in some sense stronger than the guarantee  $C|0^n\rangle = \frac{|0^n\rangle + |1^n\rangle}{2}$ . In the case of the latter it seems that an OR gate is required to compute parity with  $C$  and  $C^\dagger$ , which Proposition 28 shows is not necessary when  $C(\alpha|0\rangle + \beta|1\rangle)|0^{n-1}\rangle = \alpha|0^n\rangle + \beta|1^n\rangle$  for all one-qubit states  $\alpha|0\rangle + \beta|1\rangle$ .

To see that (2)  $\implies$  (1) note that

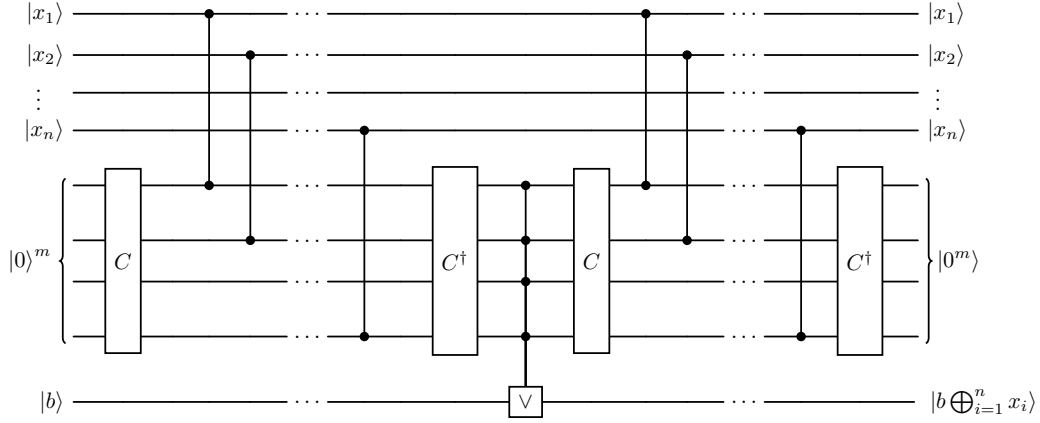
$$F_n|+\rangle|0^n\rangle = \frac{|0^{n+1}\rangle + |1^{n+1}\rangle}{\sqrt{2}}$$

Observe that if given access to some circuit  $C$  (and  $C^\dagger$ ) which satisfies the weaker condition of preparing an exact  $n$ -nekomata, i.e.,

$$C|0^m\rangle = \frac{|0^n\rangle|\psi_0\rangle + |1^n\rangle|\psi_1\rangle}{\sqrt{2}}$$

one can construct a constant-depth QAC circuit which exactly computes Parity:

Note that in the below circuit after the first layer of CZ gates are applied the state on the ancilla qubits is  $\frac{|0^n\rangle|\psi_0\rangle + (-1)^{|x|}|1^n\rangle|\psi_1\rangle}{\sqrt{2}}$ . When  $|x|$  is even, nothing has happened, so  $C^\dagger$  will return the state on these registers to  $|0^m\rangle$  and the  $\vee$ -gate will not change the final



■ **Figure 3** Computing  $P_n$  with a circuit  $C$  which prepares an exact  $n$ -nekomata and its inverse  $C^\dagger$ .

register. When  $|x|$  is odd  $\frac{|0^n\rangle|\psi_0\rangle + (-1)^{|x|}|1^n\rangle|\psi_1\rangle}{\sqrt{2}}$  is orthogonal to  $C|0^m\rangle$ , so after applying  $C^\dagger$  the resulting state is orthogonal to  $|0^m\rangle$  which will always trigger the  $V$ -gate. The second half of the circuit uncomputes returning the ancillary registers to  $|0^m\rangle$ . Thus, the final register is always left in the state  $|b \oplus_{i=1}^n x_i\rangle$  - thus, (up to an  $X$  gate) this circuit exactly computes parity.

Finally, we prove Lemma 16 and in particular that the below circuit approximates  $P_n$  when  $C$  is replaced with any  $U$  which produces an  $\epsilon$ -approximate  $n$ -nekomata when applied to the all zeros state.

**Proof of Lemma 16.** Let  $U$  be a unitary on  $m$  qubits such that  $U|0^m\rangle = |\psi\rangle$  is an  $\epsilon$ -approximate  $n$ -nekomata and let  $|\nu\rangle = \frac{|0^n\rangle|\psi_0\rangle + |1^n\rangle|\psi_1\rangle}{\sqrt{2}}$  be the  $n$ -nekomata on  $m$  qubits which maximizes  $|\langle\nu|\psi\rangle|^2$ . We can write  $|\psi\rangle = \sqrt{1-\epsilon}|\nu\rangle + \sqrt{\epsilon}|\nu^\perp\rangle$  for some  $|\nu^\perp\rangle$  which is orthogonal to  $|\nu\rangle$ . In the circuit shown in Figure 3 observe that after the first layer of CZ gates are applied the state on the ancilla registers is

$$|\psi_-\rangle = \sqrt{1-\epsilon} \frac{|0^n\rangle|\psi_0\rangle + (-1)^{|x|}|1^n\rangle|\psi_1\rangle}{\sqrt{2}} + \sqrt{\epsilon}|\nu^\perp\rangle$$

For some  $|\nu^\perp\rangle$ . Observe that when  $|x|$  is even then  $|\langle\psi_-|\psi\rangle|^2 \geq 1 - 2\epsilon$  and when  $|x|$  is odd then  $|\langle\psi_-|\psi\rangle|^2 = O(\epsilon)$ . In the former case  $C^\dagger|\psi_- \rangle$  will have fidelity at least  $1 - O(\epsilon)$  with  $|0^m\rangle$ , so after uncomputation we are left with  $|x, 0^m\rangle|\omega_b\rangle$  where  $|\langle b|\omega_b\rangle|^2 \geq 1 - O(\epsilon)$ . Similarly, when  $|x|$  is odd  $C^\dagger|\psi_- \rangle$  has fidelity at most  $O(\epsilon)$  with  $|0^m\rangle$  and after uncomputation we are left with  $|x, 0^m\rangle|\omega_b\rangle$  where  $|\langle b|\omega_b\rangle|^2 \leq O(\epsilon)$ . Thus, on any input  $|x, b\rangle$  the state produced by this circuit has fidelity at least  $1 - O(\epsilon)$  with  $F_n|x, b\rangle$  - equivalently, the  $\ell_2$ -distance is at most  $O(\epsilon)$  meaning that the unitary implemented by this circuit,  $V$ , satisfies  $\|V - P_n\|_{\text{op}} = O(\epsilon)$ . Thus, (1)  $\implies$  (3).

To see that (3)  $\implies$  (2) suppose that the unitary  $U$  satisfies  $\|U - P_n\|_{\text{op}} \leq \epsilon$ . Then,

$$\|H^{\otimes(n+1)}UH^{\otimes(n+1)} - F_n\|_{\text{op}} = \|H^{\otimes(n+1)}(U - P_n)H^{\otimes(n+1)}\|_{\text{op}} \leq \|U - P_n\|_{\text{op}} \leq \epsilon$$

For (2)  $\implies$  (1) let  $|\psi\rangle = F_n|+\rangle|0^n\rangle = \frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$  and  $|\phi\rangle = U|+\rangle|0^n\rangle$ . Note that if  $\|U - F_n\|_{\text{op}} \leq \epsilon$  then

$$\|\phi\rangle - |\psi\rangle\|_2 \leq \| |+\rangle|0^n\rangle \|_2 \|U - F_n\|_{\text{op}} \leq \epsilon$$



So,

$$\| |\phi\rangle - |\psi\rangle \|_2 = \sqrt{2 - \langle \psi | \phi \rangle - \langle \phi | \psi \rangle} \leq \epsilon \implies |\langle \psi | \phi \rangle|^2 \geq 1 - \epsilon^2 - \epsilon^4/4$$

Thus,  $|\phi\rangle$  is an  $O(\epsilon)$ -approximate nekomata. ◀

**Proof.** Proof of Lemma 29 This can be seen via a direct computation:

$$F_{n,p} Q^{\otimes n+1} |b\rangle |x\rangle = F_{n,p} \left( \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \omega^{bj} |j\rangle \right) \otimes \left( \frac{1}{\sqrt{p^n}} \sum_{y \in \mathbb{F}_p^n} \omega^{\langle x, y \rangle} |y\rangle \right)$$

Here  $\langle x, y \rangle$  denotes the inner product over vectors in  $\mathbb{F}_p^n$ :  $\langle x, y \rangle = \sum_{j=1}^p x_j y_j \pmod{p}$ . For  $y \in \mathbb{F}_p^n$  and  $j \in \mathbb{F}_p$  we will use  $y^{(j)}$  to denote the string obtained by adding  $j$  to every entry of  $y$ , i.e.,  $F_p |j\rangle |y\rangle = |j\rangle |y^{(j)}\rangle$ . Now we can see that

$$\left( \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \omega^{bj} |j\rangle \right) \otimes \left( \frac{1}{\sqrt{p^n}} \sum_{y \in \mathbb{F}_p^n} \omega^{\langle x, y \rangle} |y\rangle \right) = \frac{1}{\sqrt{p^{n+1}}} \sum_{y \in \mathbb{F}_p^n} \sum_{j=0}^{p-1} \omega^{bj + \langle x, y \rangle} |j\rangle |y\rangle$$

So,

$$F_{n,p} \frac{1}{\sqrt{p^{n+1}}} \sum_{y \in \mathbb{F}_p^n} \sum_{j=0}^{p-1} \omega^{bj + \langle x, y \rangle} |j\rangle |y\rangle = \frac{1}{\sqrt{p^{n+1}}} \sum_{y \in \mathbb{F}_p^n} \sum_{j=0}^{p-1} \omega^{bj + \langle x, y \rangle} |j\rangle |y^{(j)}\rangle$$

After rearranging we have

$$\begin{aligned} \frac{1}{\sqrt{p^{n+1}}} \sum_{y \in \mathbb{F}_p^n} \sum_{j=0}^{p-1} \omega^{bj + \langle x, y \rangle} |j\rangle |y^{(j)}\rangle &= \frac{1}{\sqrt{p^{n+1}}} \sum_{y \in \mathbb{F}_p^n} \sum_{j=0}^{p-1} \omega^{bj + \langle x, y^{(-j)} \rangle} |j\rangle |y\rangle \\ &= \frac{1}{\sqrt{p^{n+1}}} \sum_{y \in \mathbb{F}_p^n} \sum_{j=0}^{p-1} \omega^{bj + \langle x, y \rangle - j|x|} |j\rangle |y\rangle \\ &= \frac{1}{\sqrt{p^{n+1}}} \sum_{y \in \mathbb{F}_p^n} \sum_{j=0}^{p-1} \omega^{\langle x, y \rangle} \omega^{j(b-|x|)} |j\rangle |y\rangle \\ &= Q^{\otimes(n+1)} M_{n,p} |b\rangle |x\rangle \end{aligned}$$

Thus,  $M_{n,p} = (Q_p^\dagger)^{\otimes n+1} F_{n,p} Q_p^{\otimes n+1}$  as claimed. ◀