



# Quantum Circuits: Fanout, Parity, and Counting

Cristopher Moore<sup>1</sup>

Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, New Mexico 87501  
moore@santafe.edu

**Abstract.** We propose definitions of  $\mathbf{QAC}^0$ , the quantum analog of the classical class  $\mathbf{AC}^0$  of constant-depth circuits with AND and OR gates of arbitrary fan-in, and  $\mathbf{QACC}^0[q]$ , the analog of the class  $\mathbf{ACC}^0[q]$  where  $\text{Mod}_q$  gates are also allowed. We show that it is possible to make a ‘cat’ state on  $n$  qubits in constant depth if and only if we can construct a parity or  $\text{Mod}_2$  gate in constant depth; therefore, any circuit class that can fan out a qubit to  $n$  copies in constant depth also includes  $\mathbf{QACC}^0[2]$ . In addition, we prove the somewhat surprising result that parity or fanout allows us to construct  $\text{Mod}_q$  gates in constant depth for any  $q$ , so  $\mathbf{QACC}^0[2] = \mathbf{QACC}^0$ . Since  $\mathbf{ACC}^0[p] \neq \mathbf{ACC}^0[q]$  whenever  $p$  and  $q$  are distinct primes,  $\mathbf{QACC}^0[2]$  is strictly more powerful than its classical counterpart, as is  $\mathbf{QAC}^0$  when fanout is allowed.

## 1 Introduction

The theory of circuit complexity has become an important branch of theoretical computer science. Shallow circuits correspond to parallel algorithms that can be performed in small amounts of time on an massively parallel computer with constant communication delays, and so circuit complexity can be thought of as a study of how to solve problems in parallel. In addition, some low-lying circuit classes have beautiful algebraic characterizations, e.g. [3, 4, 11].

In [13, 14], Moore and Nilsson suggested a definition of  $\mathbf{QNC}$ , the quantum analog of the class  $\mathbf{NC}$  of problems solvable by circuits with polylogarithmic depth and polynomial size [15]. Here, we will study quantum versions of some additional circuit classes. Recall the following definitions:

1.  $\mathbf{NC}^k$  consists of problems solvable by families of circuits of AND, OR, and NOT gates with depth  $\mathcal{O}(\log^k n)$  and size polynomial in  $n$ , where  $n$  is the size of the input, and where the AND and OR gates have just two inputs each.
2.  $\mathbf{AC}^k$  is like  $\mathbf{NC}^k$ , but where we allow AND and OR gates with unbounded fan-in, i.e. arbitrary numbers of inputs, in each layer of the circuit.
3.  $\mathbf{ACC}^k[q]$  is like  $\mathbf{AC}^k$ , but where we also allow  $\text{Mod}_q$  gates with unbounded fan-in, where  $\text{Mod}_q(x_1, \dots, x_n)$  outputs 1 iff the sum of the inputs is not a multiple of  $q$ .
4.  $\mathbf{ACC}^k = \cup_q \mathbf{ACC}^k[q]$ .
5.  $\mathbf{NC} = \cup_k \mathbf{NC}^k = \cup_k \mathbf{AC}^k = \cup_k \mathbf{ACC}^k$ .

Then we have

$$\mathbf{AC}^0 \subset \mathbf{ACC}^0[2] \subset \mathbf{ACC}^0 \subseteq \mathbf{NC}^1 \subseteq \dots \subseteq \mathbf{NC}$$

In fact, these first two inclusions are known to be proper [1, 8, 16, 21]. Neither MAJORITY nor PARITY are in  $\mathbf{AC}^0$ , while the latter is trivially in  $\mathbf{ACC}^0[2]$ . In addition,  $\mathbf{ACC}^0[p]$  and  $\mathbf{ACC}^0[q]$  are known to be incomparable whenever  $p$  and  $q$  are distinct primes. Thus these classes give us some of the few strict inclusions known in computational complexity theory. However, for all anyone knows,  $\mathbf{ACC}^0[6]$  could contain  $\mathbf{P}$ ,  $\mathbf{NP}$ , and the entire polynomial hierarchy!

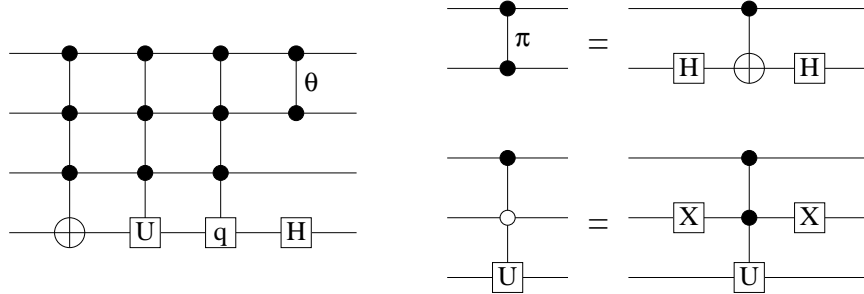
There is significant evidence that quantum complexity classes are often more powerful than their classical counterparts. The best-known is Shor's factoring algorithm [19], showing that integer factoring is in  $\mathbf{BQP}$ , the quantum analog of bounded-probability polynomial time. Other such results lower down on the computational hierarchy include the recognition of non-regular languages by two-way quantum finite automata with bounded probability [10] and quantum context-free languages that are not classically context-free [12].

In this paper, we prove a number of results about  $\mathbf{QAC}$  and  $\mathbf{QACC}$ , and address some definitional difficulties. We show that an ability to form a 'cat state' with  $n$  qubits, or fan out a qubit into  $n$  copies in constant depth, is equivalent to being able to constrict an  $n$ -ary parity gate in constant depth. Furthermore, we show the somewhat surprising result that either of these allows us to build  $\text{Mod}_q$  gates in constant depth for any  $q$ , so  $\mathbf{QACC}^0[2] = \mathbf{QACC}^0$ . This is markedly different from the classical situation mentioned above. Finally, we discuss how best to compare these circuit classes to classical ones, and conclude that  $\mathbf{QACC}^0[2]$ , and a form of  $\mathbf{QAC}^0$  we call  $\mathbf{QAC}_{\text{wf}}^0$ , are strictly more powerful than  $\mathbf{ACC}^0[2]$  and  $\mathbf{AC}^0$  respectively.

## 2 Definitions

We will use the notation in Figure 1 for our various gates. The  $n$ -ary Toffoli gate, or simply the AND gate, negates the target qubit if all the input qubits are true. The  $n$ -ary controlled- $U$  gate applies a unitary transformation  $U$  to the target if all the inputs are true, and the  $\text{Mod}_q$  gate negates the target if the number of true inputs is not a multiple of  $q$ . Note that all these are reversible. For three inputs, for instance, the Toffoli, controlled- $U$ , and  $\text{Mod}_2$  gates can be written as the matrices

$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & x \end{pmatrix}, \quad \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & U \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & & & & & & & \\ & x & & & & & & \\ & & x & & & & & \\ & & & 1 & & & & \\ & & & & x & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & x \end{pmatrix}$$



**Fig. 1.** Our notation for  $n$ -ary Toffoli, controlled- $U$ , and  $\text{Mod}_q$  gates, symmetric phase shift gates, and the Hadamard gate. On the top right, we show a useful identity between the controlled-not, the controlled  $\pi$ -shift, and the Hadamard gate. On the bottom right we show a controlled- $U$  gate with one of its inputs negated by conjugation with  $X$ .

where  $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  is the identity and  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  negates a qubit. We will also use the symmetric phase shift gate, shown here for two qubits  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$  which is a special case of the controlled- $U$  gate, and the one-qubit *Hadamard gate*  $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ . Note that the controlled  $\pi$ -shift is simply the controlled-not with the target qubit conjugated with  $H$ , and that  $H^2 = \mathbf{1}$ . Finally, we will also sometimes use controlled- $U$  gates with some inputs negated, which can be performed by conjugating that input with  $X$ . All of these are shown in Figure 1.

Then our definition of **QAC** and **QACC** is as follows:

**Definition.** A family of unitary operators on  $n$  qubits  $F_n \in U(2^n)$  is in **QAC** <sup>$k$</sup>  if  $F_n$  can be written as a product of  $\mathcal{O}(\log^k n)$  operators, each of which is a tensor product of one-qubit gates and Toffoli gates of arbitrary arity acting on disjoint sets of qubits. Each such tensor product is called a *layer*. The definition of **QACC** <sup>$k$</sup>  $[q]$  is similar, except that  $\text{Mod}_q$  gates are also allowed. Finally,  $\mathbf{QACC}^k = \cup_q \mathbf{QACC}^k[q]$ .

We also allow our circuits to use a polynomial number of *ancillae* or work qubits. However, for the final measurement to be correct, these ancillae have to be unentangled from the qubits of the final state that we care about. The easiest way to do this is to require that the ancillae start and end in a pure state  $|0\rangle$ , in which case our desired operator occurs as a diagonal block of the larger operator on this subspace [13]. This also allows us to re-use ancillae.

Note that  $n$ -ary controlled- $U$  gates with arbitrary  $U$  can be performed in constant depth with one ancilla, by writing them as a product of two Toffoli gates and a two-qubit controlled- $U$  gate with one input, which in turn can be written as a product of controlled-nots and one-qubit gates [2]. Thus our definition of **QAC** remains the same if we allow  $n$ -ary controlled- $U$  gates in each layer. Similarly, allowing  $\text{Mod}_q$  controlled- $U$  gates, which apply  $U$  to the target qubit if the

number of true inputs is not a multiple of  $q$ , does not change our definition of **QACC**.

It is, of course, tempting to pronounce these classes ‘quack.’

### 3 Fanout, Cat states and parity

To make a shallow parallel circuit, it is often important to *fan out* one of the inputs into multiple copies. One of the differences between classical circuits and quantum ones as we have defined them here is that in classical circuits, we usually assume that we get arbitrary fanout for free, simply by splitting a wire into as many copies as we like. This is difficult in quantum circuits, since making an unentangled copy requires non-unitary, and in fact non-linear, processes:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \alpha^2|00\rangle + \alpha\beta(|01\rangle + |10\rangle) + \beta^2|11\rangle$$

has coefficients quadratic in  $\alpha$  and  $\beta$ . This is the so-called ‘no cloning’ theorem.

However, the controlled-not gate can be used to copy a qubit onto an ancilla in the pure state  $|0\rangle$  by making a non-destructive measurement:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \rightarrow \alpha|00\rangle + \beta|11\rangle$$

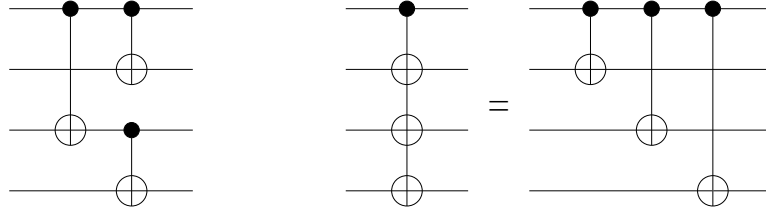
Note that the final state is not a tensor product of two independent qubits, since the two qubits are completely entangled. This means that whatever we do to one copy, we do to the other. Except when the states are purely Boolean, we have to treat this kind of ‘fanout’ more gingerly than we would in the classical case.

By making  $n$  copies of a qubit in this sense, we can make a ‘cat state’  $\alpha|000\dots 0\rangle + \beta|111\dots 1\rangle$ . Such states are useful in making quantum computation fault-tolerant (e.g. [7, 20]). We can do this in  $\log n$  depth with controlled-not gates, as shown on the left-hand side of Figure 2. When preceded by a Hadamard gate on the top qubit, this circuit will map an initial state  $|0000\rangle$  onto a cat state  $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ . However, we will also consider circuits which can do this in a single layer, with a ‘fanout gate’ that simultaneously copies a qubit onto  $n$  target qubits. This is simply the product of  $n$  controlled-not gates, as shown on the right-hand side of Figure 2.

We now show that in quantum circuits, we can do fanout in constant depth if and only if we can construct a parity gate in constant depth.

**Proposition 1.** *In any class of quantum circuits that includes Hadamard and controlled-not gates, the following are equivalent:*

1. *It is possible to map  $\alpha|0\rangle + \beta|1\rangle$  and  $n - 1$  ancillae in the state  $|0\rangle$  onto an  $n$ -qubit cat state  $\alpha|000\dots 0\rangle + \beta|111\dots 1\rangle$  in constant depth.*
2. *The  $n$ -ary fanout gate on the right-hand side of Figure 2 can be implemented in constant depth with at most  $n - 1$  additional ancillae.*
3. *An  $n$ -ary parity or  $\text{Mod}_2$  gate as defined above can be implemented in constant depth with at most  $n - 1$  additional ancillae.*



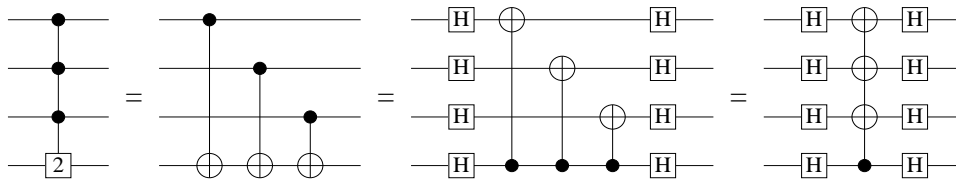
**Fig. 2.** Two ways to make a cat state on  $n$  qubits. The circuit on the left uses only two-qubit gates and has depth  $\log n$ . On the right, we define a ‘fanout gate’ that simultaneously performs  $n$  controlled-nots from one input qubit.

*Proof.* First, note that (1) is *a priori* weaker than (2), since (1) only requires that an operator map  $|100\dots 0\rangle$  to  $|111\dots 1\rangle$  and  $|000\dots 0\rangle$  to itself. In fact, the two circuits shown in Figure 2 both do this, even though they differ on other initial states.

To prove  $(2 \Leftrightarrow 3)$ , we simply need to notice that the parity gate is a fanout gate going the other way conjugated by a layer of Hadamard gates, since parity is simply a product of controlled-nots with the same target qubit, and conjugating with  $H$  reverses the direction of a controlled-not. This is shown in Figure 3. Clearly the number of ancillae used to perform either gate will be the same.

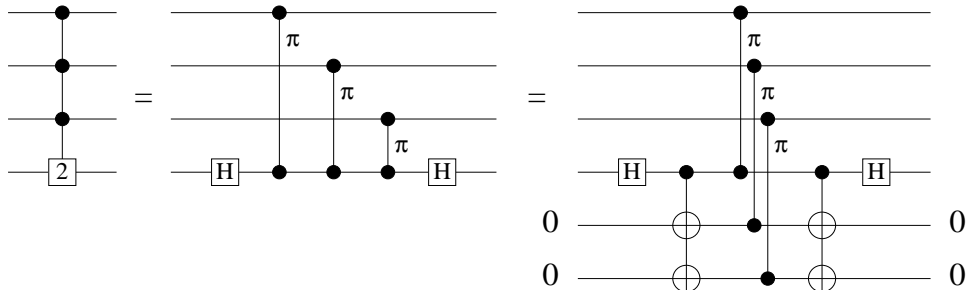
To prove  $(1 \Rightarrow 3)$ , we use a slightly more elaborate circuit shown in Figure 4. Here we use the identity shown in Figure 1 to convert the parity gate into a product of controlled  $\pi$ -shifts. Since these are diagonal, they can be parallelized as in [13] by copying the target qubit onto  $n - 1$  ancillae, and applying each one to a different copy. While we have drawn the circuit with two fanout gates, any gate that satisfies the conditions in (1), and its inverse after the  $\pi$ -shifts, will do.

Finally,  $(2 \Rightarrow 1)$  is obvious.  $\square$



**Fig. 3.** The parity and fanout gates are conjugates of each other by a layer of Hadamard gates.

This brings up an interesting issue. It is not clear that  $\mathbf{AC}^0 \subset \mathbf{QAC}^0$  as we have defined  $\mathbf{QAC}^0$  here, since we are not allowing arbitrary fanout in each layer. An alternate definition, which we might call  $\mathbf{QAC}$  with fanout or  $\mathbf{QAC}_{wf}$ , would allow us to perform controlled- $U$  gates or Toffoli gates in the same layer whenever they have different target qubits, even if their input qubits overlap.



**Fig. 4.** The parity gate can also be written as a product of controlled  $\pi$ -shifts, with the target qubit conjugated by  $H$ . Since these are diagonal, we can parallelize them using any gate that can make a cat state.

This seems reasonable, since these gates commute. Since we can fan out to  $n$  copies in  $\log n$  layers as in Figure 2, we have  $\mathbf{QAC}^k \subseteq \mathbf{QACC}_{\text{wf}}^k \subseteq \mathbf{QAC}^{k+1}$ . We can define  $\mathbf{QACC}_{\text{wf}}^k$  in the same way, and Proposition 1 implies that  $\mathbf{QAC}_{\text{wf}}^k = \mathbf{QACC}_{\text{wf}}^k[2] = \mathbf{QACC}^k[2]$ .

It is partly a matter of taste whether  $\mathbf{QAC}^0$  or  $\mathbf{QACC}_{\text{wf}}^0$  is a better analog of  $\mathbf{AC}^0$ . However, fanout does seem possible in several proposed technologies for quantum computing. In an ion trap computer [6], vibrational modes can couple with all the atoms simultaneously, so we could apply a controlled-not from one atom to the ‘bus qubit’ and then from the bus to the other  $n$  atoms. In bulk-spin NMR [9], we can activate the couplings from one atom to  $n$  others, and perform  $n$  controlled  $\pi$ -shifts simultaneously, which is equivalent to fanout with the target qubits conjugated with the Hadamard gate. Thus allowing fanout may in fact be the most reasonable model of constant-depth quantum circuits.

#### 4 Parity or fanout gives $\text{Mod}_q$ gates

As stated above, in the classical case  $\text{Mod}_p$  and  $\text{Mod}_q$  gates are not easy to build from each other whenever  $p$  and  $q$  are relatively prime. In fact, to do it in constant depth requires a circuit of exponential size [21]. In this section, we will show this is not true in the quantum case. Specifically, with  $n$ -ary parity gates we can build  $\text{Mod}_q$  gates in constant depth for any  $q$ .

**Proposition 2.** *In any circuit class containing  $n$ -ary parity gates and one-qubit gates, we can construct an  $n$ -ary  $\text{Mod}_q$  gate, with  $\mathcal{O}(n \log q)$  ancillae, in depth depending only on  $q$ .*

*Proof.* Let  $k = \lceil \log_2 q \rceil$ , and let  $M$  be a Boolean matrix on  $k$  qubits where the zero state has period  $q$ . For instance, if we write  $|x\rangle$  as shorthand for  $|x_{k-1} \cdots x_1 x_0\rangle$  where  $x_i$  is the  $2^i$  digit of  $x$ ’s binary expansion and  $0 \leq x < 2^k$ , we can define  $M$  so that it permutes the  $|x\rangle$  as follows:

$$M|x\rangle = \begin{cases} |(x+1) \bmod q\rangle & \text{if } x < q \\ |x\rangle & \text{if } x \geq q \end{cases}$$

Then if we start with  $k$  ancillae in the state  $|0\rangle$  and apply a controlled- $M$  gate to them from each input, the state will differ from  $|0\rangle$  on at least one qubit if and only if the number of true inputs is not a multiple of  $q$ . (Note that this controlled- $M$  gate applies to  $k$  target qubits at once in an entangled way.) We can then apply an  $n$ -ary OR from these  $k$  qubits to the target qubit, i.e. a Toffoli gate with its inputs conjugated with  $X$  and the target qubit negated before or after the gate. We end by applying the inverse series of controlled- $M^\dagger$  gates to return the  $k$  ancillae to  $|0\rangle$ .

Now we use Proposition 4 of [13] to parallelize this set of controlled- $M$  gates. We can convert them to diagonal gates by conjugating the  $k$  qubits with a unitary operator  $T$ , where  $T^\dagger DT = M$  and  $D$  is diagonal. If we have a parity gate, we can fan out the  $k$  ancillae to  $n$  copies each using Proposition 1. We can then simultaneously apply the  $n$  controlled- $D$  gates from each input to the corresponding copy, and then uncopy them back.

This is shown in Figure 5. For  $q = 3$ , for instance, we have  $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ ,

$$T = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & & & \sqrt{3} \\ e^{4\pi i/3} & 1 & & \\ e^{2\pi i/3} & e^{4\pi i/3} & 1 & \\ & & & 1 \end{pmatrix}, \text{ and } D = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & e^{2\pi i/3} & \\ & & & e^{4\pi i/3} \end{pmatrix}.$$

The operators  $T$ ,  $T^\dagger$ , and the controlled- $D$  gate can be carried out in some finite depth by controlled-nots and one-qubit gates by the results of [2]. The total depth of our  $\text{Mod}_q$  gate is a function of these and so of  $q$ , but not of  $n$ . Finally, the number of ancillae used is  $(n-1)k = \mathcal{O}(n \log q)$  as promised.  $\square$

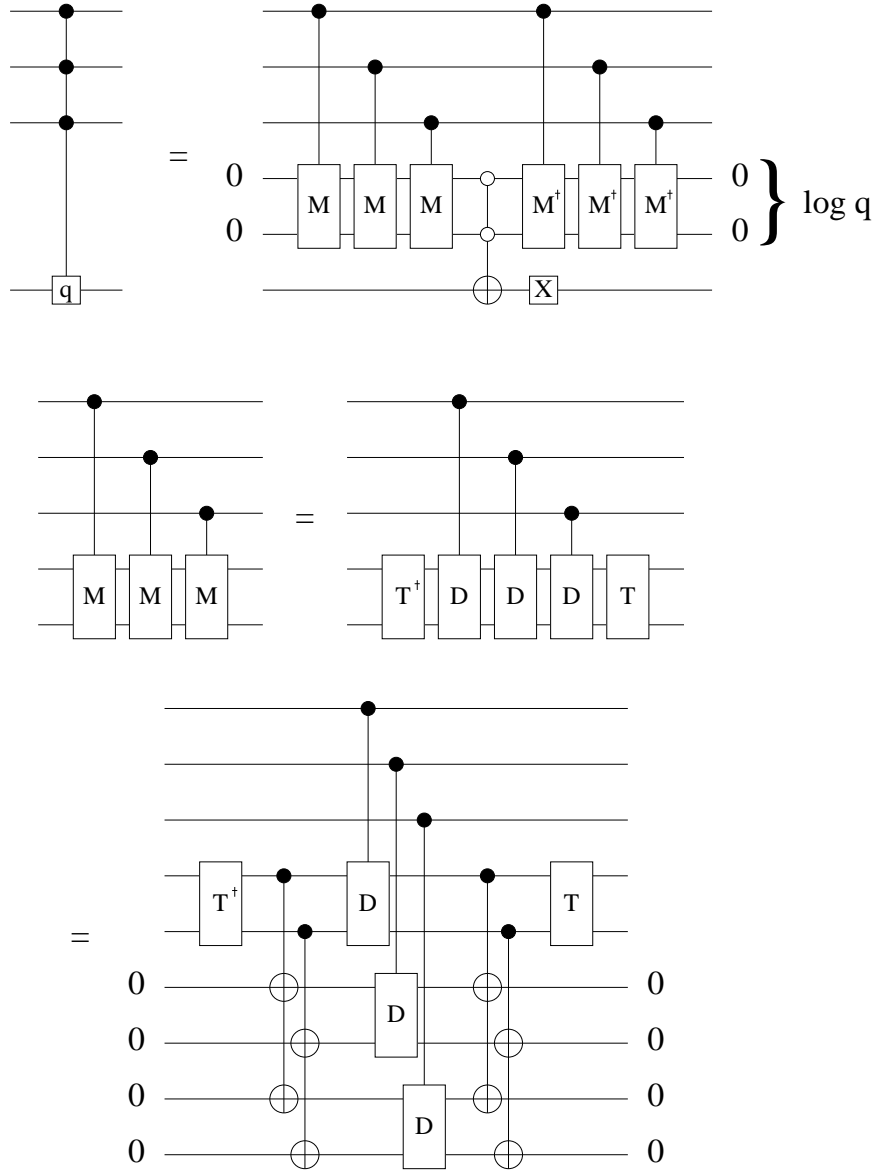
To look more closely at the depth as a function of  $q$ , we note that using the methods of Reck et al. [17] and Barenco et al. [2], any operator on  $k$  qubits can be performed with  $\mathcal{O}(k^3 4^k)$  two-qubit gates. Since  $k = \lceil \log_2 q \rceil$ , this means that the depths of  $T$ ,  $T^\dagger$  and the controlled- $D$  gates are at most  $\mathcal{O}(q^2 \log^3 q)$ .

Since we can construct  $\text{Mod}_q$  gates in constant depth, we have  $\mathbf{QACC}^k[q] \subset \mathbf{QACC}^k[2]$  for all  $q$ , so  $\mathbf{QACC}^k = \mathbf{QACC}^k[2]$ . By Proposition 1, these are both also equal to  $\mathbf{QACC}_{\text{wf}}^k$ . In particular, we have

$$\mathbf{QACC}_{\text{wf}}^0 = \mathbf{QACC}^0[2] = \mathbf{QACC}^0$$

while classically both equalities are strict inclusions. Note that we also have  $\mathbf{QACC}_{\text{wf}}^0[q] = \mathbf{QACC}_{\text{wf}}^0 = \mathbf{QACC}^0$  for all  $q$ . Without fanout,  $\mathbf{QACC}^0[q]$  might be smaller than  $\mathbf{QACC}^0$  for  $q$  odd.

To compare these with classical circuits requires a little care. For any Boolean function  $\phi$  with  $n$  inputs and  $m$  outputs, we can define a reversible version  $\phi'$  on  $n+m$  bits where  $\phi'(x, y) = (x, y \oplus \phi(x))$  keeps the input  $x$  and xors the output  $\phi(x)$  with  $y$ . Then if  $\phi$  has a circuit with depth  $d$  and width  $w$ , it is easy to construct a reversible circuit for  $\phi'$  of depth  $2d-1$  where  $wd$  ancillae start and end in the zero state. We do this by assigning an ancilla to each gate in the original circuit, and replacing each gate with a reversible one that xors that ancilla with the output. Then we can erase the ancillae by moving backward through the layers of the circuit.



**Fig. 5.** Building a  $\text{Mod}_q$  gate. We choose a matrix  $M$  on  $k = \lceil \log_2 q \rceil$  qubits such that  $M^q = \mathbf{1}$ , apply controlled- $M$  gates from the  $n$  inputs to  $k$  ancillae, apply an OR from these  $k$  qubits to the target qubit, and reverse the process to return the ancillae to  $|0\rangle$ . To parallelize this, we can diagonalize  $M$  by writing it as  $T^\dagger D T$ , fan the  $k$  qubits out into  $n$  copies each using Proposition 1, and apply controlled- $D$  gates simultaneously from each input to a set of copies. The total depth depends on  $q$  but not on  $n$ .



Then if we adopt the convention that a Boolean function with  $n$  inputs and  $m$  outputs is in a quantum circuit class if its reversible version is, we clearly have  $\mathbf{AC}^k \subseteq \mathbf{QAC}_{\text{wf}}^k$  and  $\mathbf{ACC}^k \subseteq \mathbf{QACC}^k$ . Thus we have

$$\mathbf{AC}^0 \subset \mathbf{ACC}^0[2] \subset \mathbf{ACC}^0 \subseteq \mathbf{QAC}_{\text{wf}}^0 = \mathbf{QACC}^0[2] = \mathbf{QACC}^0$$

showing that  $\mathbf{QAC}_{\text{wf}}^0$  and  $\mathbf{QACC}^0[2]$  are more powerful than  $\mathbf{AC}^0$  and  $\mathbf{ACC}^0[2]$  respectively.

Interestingly, if  $\mathbf{QAC}^0$  as we first defined it cannot do fanout, i.e. if  $\mathbf{QAC}^0 \subset \mathbf{QAC}_{\text{wf}}^0$ , then in a sense it fails to include  $\mathbf{AC}^0$ , since the fanout function from  $\{0, 1\}$  to  $\{0, 1\}^n$  is trivially in  $\mathbf{AC}^0$ . However, it is not clear whether it fails to include any  $\mathbf{AC}^0$  functions with a one-bit output. On the other hand, if  $\mathbf{QAC}^0$  can do fanout, it can also do parity and is greater than  $\mathbf{AC}^0$ , so either way  $\mathbf{AC}^0$  and  $\mathbf{QAC}^0$  are different. I am indebted to Pascal Tesson for pointing this out.

## 5 Conclusion

We have shown that fanout and parity are intimately related in quantum circuits, and that either of these makes it possible to construct a  $\text{Mod}_q$  gate in constant depth for any  $q$ . Thus  $\mathbf{QAC}_{\text{wf}}^0 = \mathbf{QACC}^0[2] = \mathbf{QACC}^0$ , and so  $\mathbf{QAC}_{\text{wf}}^0$  and  $\mathbf{QACC}^0[2]$  are more powerful than  $\mathbf{AC}^0$  and  $\mathbf{ACC}^0[2]$  respectively. This adds another case where quantum classes are provably more powerful than their classical cousins.

We suggest three questions for further work:

1. Is  $\mathbf{QAC}^0 = \mathbf{QAC}_{\text{wf}}^0$ ? That is, can the fanout gate be constructed in constant depth when each qubit can only act as an input to one gate in each layer?
2. Without explicit fanout, is  $\mathbf{QACC}^0[q] = \mathbf{QACC}^0$  for all  $q$ ? That is, can  $\text{Mod}_q$  gates with odd  $q$  generate fanout, parity, and  $\text{Mod}_p$  gates for all other  $p$ ?
3. Is  $\mathbf{QAC}_{\text{wf}}^0 = \mathbf{QTC}^0$ ? That is, can the techniques used here be extended to construct threshold gates in constant depth?

We conjecture that the answer to all these questions is ‘no,’ but quantum circuits can be surprising...

**Acknowledgments.** I thank Denis Thérien for organizing the 1999 McGill Workshop on Computational Complexity, and Pascal Tesson, Charles Bennett, Daniel Gottesman, Cesar Miquel, Daniel James, and Manny Knill for helpful conversations. I also thank Molly Rose and Spootie the Cat for their support.

## References

1. M. Ajtai, “ $\Sigma_1^1$  formulae on finite structures.” *Ann. Pure Appl. Logic* **24** (1983) 1–48.
2. A. Barenco, C. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin and H. Weinfurter, “Elementary gates for quantum computation.” quant-ph/9503016, *Phys. Rev. A* **52** (1995) 3457–3467.

3. D. A. Barrington, "Bounded-width polynomial-size branching programs recognize exactly those languages in  $\mathbf{NC}^1$ ." *J. Comput. System Sci.* **38** (1989) 150–164.
4. M. Beaudry, P. McKenzie, P. Péladeau, and D. Thérien, "Circuits with monoidal gates." *Proc. Symposium on Theoretical Aspects of Computer Science (STACS)* (1993) 555–565.
5. C.H. Bennett, "Time/space trade-offs for reversible computation." *SIAM Journal of Computing* **4**(18) (1989) 766–776.
6. J.I. Cirac and P. Zoller, "Quantum computers with cold trapped ions." *Phys. Rev. Lett.* **74** (1995) 4091-4094.
7. D.P. DiVincenzo and P.W. Shor, "Fault-tolerant error correction with efficient quantum codes." quant-ph/9605031.
8. M. Furst, J.B. Saxe, and M. Sipser, "Parity, circuits, and the polynomial-time hierarchy." *Math. Syst. Theory* **17** (1984) 13–27.
9. N. Gershenfeld and I. Chuang, "Bulk spin resonance quantum computation." *Science* **275** (1997) 350.
10. A. Kondacs and J. Watrous, "On the power of quantum finite state automata." *Proc. 38th Symposium on Foundations of Computer Science (FOCS)* (1997) 66–75.
11. C. Moore, D. Thérien, F. Lemieux, J. Berman, and A. Drisko, "Circuits and Expressions with Non-Associative Gates." To appear in *J. Comput. System Sci.*
12. C. Moore and J.P. Crutchfield, "Quantum automata and quantum grammars." quant-ph/9707031, to appear in *Theoretical Computer Science*.
13. C. Moore and M. Nilsson, "Parallel quantum computation and quantum codes." quant-ph/9808027.
14. C. Moore and M. Nilsson, "Some notes on parallel quantum computation." quant-ph/9804034.
15. C.H. Papadimitriou, *Computational Complexity*. Addison-Wesley, 1994.
16. A.A. Razborov, "Lower bounds for the size of circuits of bounded depth with basis  $\{\&, \oplus\}$ ." *Math. Notes Acad. Sci. USSR* **41**(4) (1987) 333–338.
17. M. Reck, A. Zeilinger, H.J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator." *Phys. Rev. Lett.* **73** (1994) 58-61.
18. M. Saks, "Randomization and derandomization in space-bounded computation." *Proc. 11th IEEE Conference on Computational Complexity* (1996) 128–149.
19. P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring." *Proc. 35th Symposium on Foundations of Computer Science (FOCS)* (1994) 124–134.
20. P.W. Shor, "Fault-tolerant quantum computation." quant-ph/9605011.
21. R. Smolensky, "Algebraic methods in the theory of lower bounds for Boolean circuit complexity." *Proc. 19th ACM Symposium on the Theory of Computing (STOC)* (1987) 77–82.
22. John Watrous, "Relationships between quantum and classical space-bounded complexity classes." *Proc. 13th IEEE Conference on Computational Complexity* (1998) 210–227.