# Constant-Depth Circuits for Teleportation, Fanout, and Cat State Creation

Paul Pham

May 11, 2012

**Abstract**

We review the techniques for performing teleportation and unbounded fanout which are behind recent results in performing Shor's algorithm in constant-depth on a nearest-neighbor architecture with a classical controller. We give concrete circuits for both techniques, place them within a historical context, and discuss their limitations.

## 1 Introduction

Many recent works in quantum circuit construction are concentrated around a core group of techniques that execute certain primitive gates in constant-depth. Traditionally, in order to be fault-tolerant, primitive gates have been assumed to come from the Clifford group, which must be efficiently implementable on any physical technology. The typical generating set of the Clifford group is usually given as the following:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z = \Lambda(e^{i\pi}) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad K = \Lambda(e^{i\pi/2}) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{1}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2}$$

This is often augmented with the single-qubit rotation $\Lambda(e^{i\pi/4})$ in order to be universal, although this gate by itself may be hard to implement in many error-correcting codes.

$$\Lambda(e^{i\pi/4}) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \tag{3}$$

Before about 2009, many works measured the circuit resources of depth, size, and width when implementing Shor's factoring algorithm [9] [10] [4] [3]

on various architectural models (AC, 1D NTC, and 2D NTC) [8] using the set of primitive gates above, or a variant which only counts two-qubit gates. However, is there a way to further reduce circuit resources by considering other gates as primitive? And can these new primitive gates be efficiently implemented using some capability previously unconsidered, yet is physically realizable?

The answer to both of these questions is yes. However, there are several parts to this puzzle of showing that Shor's factoring algorithm could be performed in constant-depth on an augmented nearest-neighbor architecture. It is now known that this task in possible, but it remains to be seen what is the optimal size and width of such a constant-depth circuit.

In 2002, Høyer and Špalek showed that if an unbounded quantum fanout gate was taken as a primitive multi-qubit gate (as is physically the case for trapped ions), factoring could be performed in constant-depth. However, how could an unbounded fanout gate be implemented in an architecture where only two-qubit gates, and not multi-qubit gates, are efficient? Can we make use of a classical controller, which is available to us in experiments through fast digital computers?

In 2009, Browne, Kashefi, and Perdrix answered both of these questions in the affirmative by linking the power of measurement-based (one-way) quantum computing to Høyer and Špalek's unbounded fanout results, building upon previous results about the power of the measurement-based model by Broadbent and Kashefi in 2007 [1]. Using this connection, the logarithmic-depth factoring circuit of Cleve and Watrous from 2000 [2] can be done in constant-depth on a $k$-dimensional nearest neighbor architecture with a classical controller, a model which we call $k$D CCNTC, for $k \geq 2$. This construction relies on two new primitives, *constant-depth teleportation* and *constant-depth fanout*, which we will review in these notes.

## 2 Constant-Depth Teleportation (CDT)

In the normal teleportation protocol, a quantum state $|\psi\rangle$ is transported physically from a source qubit (called $A$ for Alice) to a target qubit (called $B$ for Bob) using a so-called two-qubit *Bell pair*, or an entangled state of the following form:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{4}$$

This is actually one of four possible Bell states, or maximally-entangled two-qubit states, which forms an alternate basis from the usual computational basis.

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (5)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (6)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (7)$$

Note that we can form the state $|\Phi^+\rangle$ starting from two unentangled qubits initialized in the $|0\rangle$ state through the following circuit, which enacts a two-qubit gate that we'll call $U_{00}$.

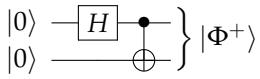


Figure 1: Creating a Bell pair

The other three Bell states can be created using similar circuits. Furthermore, we can perform a measurement in the Bell-state basis (usually simply called the Bell basis) by converting back to the computational basis (by applying $U_{00}^\dagger$) and measuring in the computational basis. This is shown in Figure 2, where the classical bits $j$ and $k$ denote the outcome measurements and tell us which of the four Bell basis states we have projected into.

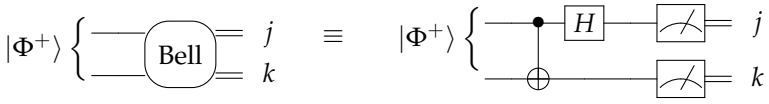


Figure 2: Measuring in the Bell basis

Then the circuit for teleportation from $A$ to $B$ is performed in Figure 3 using a Bell state $|\Phi^+\rangle^{AB}$ that is shared between Alice and Bob and a source state $|\psi\rangle^A$ to teleport that belongs to Alice only. Note that the state that is teleported to Bob is $|\psi\rangle$ up to Pauli corrections, which are measured by Alice and then communicated classically to Bob.

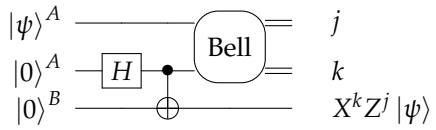


Figure 3: Normal teleportation protocol

Now then, consider two changes to the above circuit. Instead of Alice and Bob being separate parties who may be arbitrarily far away from each other, assume now that Alice and Bob are merged into an omniscient classical controller which can access all qubits at the same time. Further, assume that the qubits are on a regular lattice and can only interact via single-qubit and two-qubit nearest neighbor gates. This architectural model is called 2D CCNTC.

Our problem now is to teleport a state $|\psi\rangle$ from one qubit to another arbitrarily far away (say $n$ qubits away) where all the intervening qubits have been initialized to $|0\rangle$. These intervening qubits are known as the *teleportation channel* and intuitively one can think of it as a road or a railway for transmitting qubits which must be kept clear (reinitialized back to $|0\rangle$ after use). By repeating the normal teleportation procedure $n$ times in sequence, it is easy to see that we can perform this task in depth $O(n)$. However, because we have a classical controller, we can actually interleave Bell measurements, measure all in one step, and then apply Pauli corrections in a second step. This will give us the constant-depth teleportation (CDT) procedure that we are looking for.

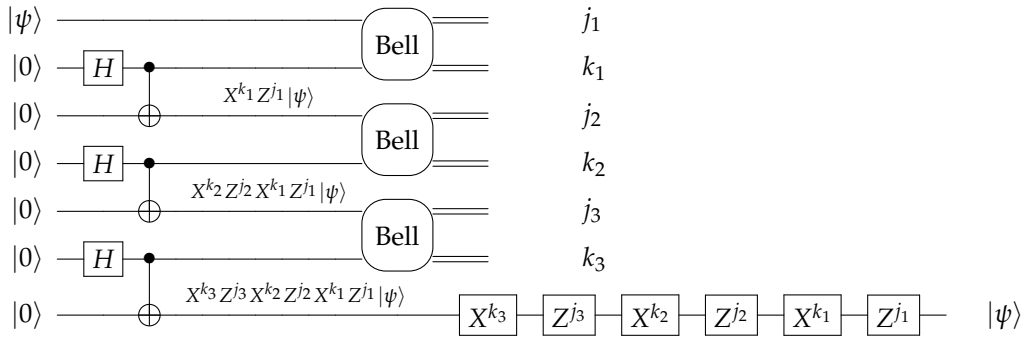


Figure 4: A constant-depth teleportation circuit due to Aram Harrow.

It is important to note that after a CDT has happened, all the qubits in the channel have been projectively measured into a product state of classical bits, including the original source qubit which was in the state $|\psi\rangle$. Therefore,

these can all be simultaneously corrected back to $|0\rangle$ by the classical controller. In this way, we can keep reusing the teleportation channel indefinitely.

If one were to count single-qubit gates, two-qubit gates, and single-qubit computational basis measurements as a single step, CDT can be executed in depth 6.

# 3 Constant-Depth Fanout (CDF)

Now we turn to a harder operation, unbounded quantum fanout in constant depth. Classically, we take it for granted that we can create copies of a bit, but quantumly we are prevented from doing this by the no-cloning theorem. Creating an unentangled copy of a generic quantum state is not even a linear operation, let alone unitary. However, we can create entangled copies using a CNOT into an initialized qubit.

$$|\psi\rangle \otimes |0\rangle \equiv (\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle \rightarrow \alpha |00\rangle + \beta |11\rangle \tag{8}$$

We will denote the unbounded fanout operation as a variation of CNOT with one control but multiple (say $n$) target qubits. Certainly we can create $n$ entangled operations in logarithmic depth by apply a tree of CNOTs as shown in Figure 5. It doesn't matter that the CNOTs operate on non-adjacent qubits, since we can use CDT from the previous section to perform a local CNOT and then teleport the target qubit an arbitrarily far distance.

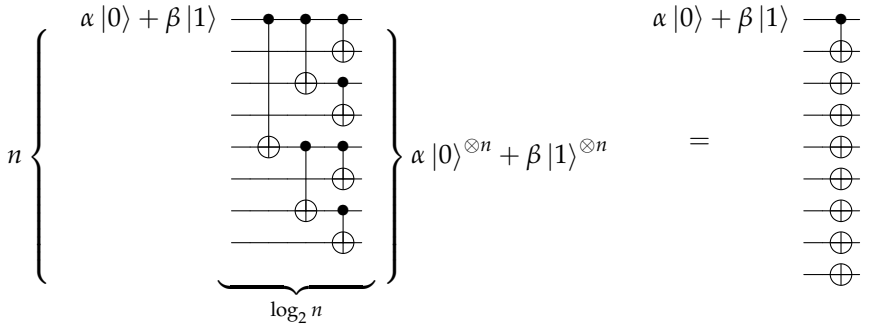


Figure 5: The equivalence of unbounded fanout to a logarithmic depth tree of CNOTs.

How can we improve the depth? To answer that, consider a special state called the $n$-qubit *cat state*, which is the maximally-entangled state on $n$ qubits.

We denote this state as $|\Phi_n\rangle$ as shown in Equation 9. Note that the Bell state $|\Phi^+\rangle$ from the previous section is simply $|\Phi_2\rangle$.

$$|\Phi_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right) \tag{9}$$

Assume that we can create $|\Phi_n\rangle$ efficiently, say in constant-depth. (We will describe how to do this in the next section.) Then we can perform unbounded fanout by entangling the source qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with the cat state as shown in Equation 10. This accomplishes the operation of constant-depth fanout (CDF), as shown in Figure 6.

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle^{\otimes n} \rightarrow \alpha|0\rangle^{\otimes(n+1)} + \beta|1\rangle^{\otimes(n+1)} \tag{10}$$

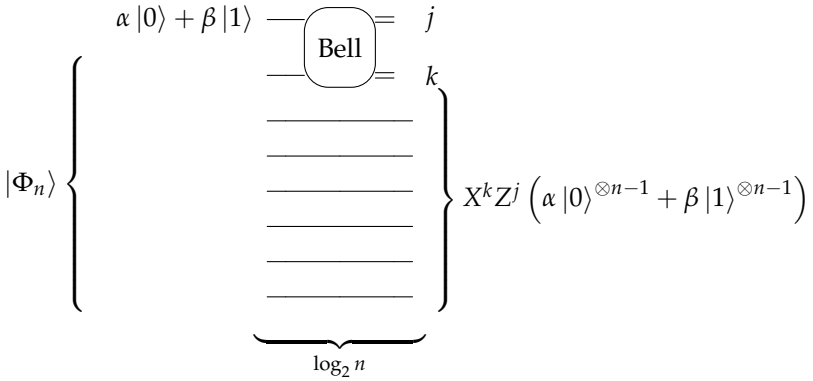


Figure 6: Entangling a source state with an $n$-qubit cat state to perform unbounded fanout.

When we refer to CDF in the rest of this note, we mean the above constant-depth implementation of unbounded quantum fanout on a nearest-neighbor architecture with a classical controller. This is in contrast to the notion of a primitive, unbounded fanout operation which may be available in a particular physical technology (e.g. trapped ions).

# 4 Constant-Depth Cat State Creation CDCSC

Now we discuss how to create the $n$-qubit cat state $|\Phi_n\rangle$ in constant depth. Note that for some fixed-size, small cat states, say $|\Phi_3\rangle$, we can create these simply using a ladder of CNOTs as shown in Figure 7.

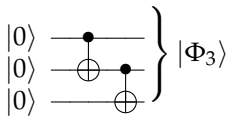


Figure 7: Circuit for creating the 3-qubit cat state.

However, this is not scalable for $|\Phi_n\rangle$. We can build an arbitrary-sized cat state by using a sequence of fixed-size cat states and Bell basis measurements as shown in Figure 8. There are several details to note in this figure. The first is that the majority of the qubits are used in the "scaffolding" to create the cat state (in this case, the six qubits which are measured to obtain a classical outcome $j_i$ and $k_i$). Just like for CDT, these classical outcomes are used for simultaneous Pauli corrections on the qubits which are actually part of the usable cat state (in this case, the four qubits which are labelled with $|\ell\rangle$.

The second detail to note is that the first and last qubit in this chain is $|\Phi_2\rangle$, while the intermediate qubits are $|\Phi_3\rangle$. This is because the first and last qubit in each $|\Phi_3\rangle$ is involved in a Bell measurement that entangles this triplet of qubits with the preceding and the succeeding one. Only the middle qubit in each triplet is usable as a qubit of the usable cat state. However, after the simultaneous round of Bell measurements, the scaffolding qubits are in a classical product state to the cat state, and can be corrected back to $|0\rangle$ and reused again in the future.

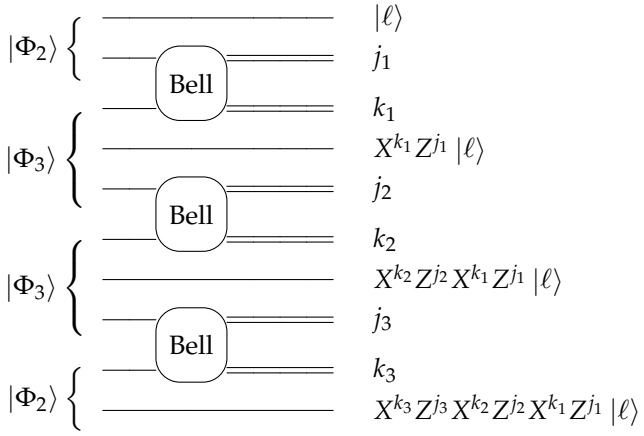


Figure 8: A constant-depth creation circuit for a cat state (in this example, $|\Phi_4\rangle$) due to Aram Harrow.

# 5 Limitation to CDF and CDCSC

In contrast to CDT, there is no way to disentangle $|\Phi_n\rangle$ from $|\psi\rangle$. Therefore, we say that CDF *consumes the cat state*. In order to keep a similar channel clear for unbounded-fanout, we must repeatedly shuffle a used cat state off to one side and shuffle in fresh ancillae initialized to $|0\rangle$. While CDF enables us to compress many circuits to constant-depth, it comes as this cost of maintaining these "garbage" cat states, which are still entangled with our computation state. If any of them decoheres, it will corrupt our output. Therefore, CDF may not be as efficient in practice for physical technologies without efficient multi-qubit gates. This is a major limitation of CDF in practice, and indicates that minimizing depth at all costs may not be desirable, and that some other circuit resource or combination of resources is a better measure of architectural efficiency. This is an open problem. See [6] for one proposed circuit resource.

# 6 Further Progress

In the specific case of factoring, the Browne-Kashefi-Perdrix result showed how to combine CDF with the logarithmic-depth implementation of Høyer-Špalek to get a constant-depth factoring implementation in a CCAC architecture, that is an AC architecture augmented with a classical controller. In this section, we examine two additional questions.

How does the efficiency of a factoring circuit change if we impose the restriction of nearest-neighbor interactions? In particular, for purposes of realistic fabrication, what is the efficiency of a factoring circuit in 2D CCNTC? Pham and Svore showed in 2011 that factoring an $n$-bit number can be performed in this setting in poly-logarithmic depth and with size and width $O(n^6)$. [5]. It is an open question whether the size and width can be improved, and how the size and width scale if the depth is brought down to a constant.

What other kinds of circuits can we efficiently convert from CCAC to $\kappa$D CCNTC? That is, can this conversion be done in constant depth and polynomial overhead in size and width? In 2012, Rosenbaum [7] showed this was possible for any $n$-qubit gate by using a two-dimensional array of $n^2$ qubits. By using CDT to transport each of the qubits to a different column, and then down to the same row again, arbitrary pairs of the original qubits can be made nearest neighbors. Ordinary $\kappa$D NTC operations can then be performed on these "projected" qubits, and then they can be teleported back to their original positions if desired. All ancillae qubits can be reused, and this entire procedure occurs in constant depth.

We hope these notes provide a useful summary of recent constant-depth techniques.

# 7 Acknowledgments

Thanks to Aram Harrow and David Rosenbaum for useful discussions and providing many of the circuits that appear in these notes.

# References

[1] Anne Broadbent and Elham Kashefi: Parallelizing Quantum Circuits. p. 34, April 2007. [arXiv:0704.1736].

[2] Richard Cleve and John Watrous: Fast parallel circuits for the quantum Fourier transform. p. 22, June 2000. [arXiv:0006004].

[3] Austin G. Fowler, Simon J. Devitt, and Lloyd C. L. Hollenberg: Implementation of Shor's Algorithm on a Linear Nearest Neighbour Qubit Array. p. 9, February 2004. [arXiv:0402196].

[4] Samuel A. Kutin: Shor's algorithm on a nearest-neighbor machine. p. 11, August 2006. [arXiv:0609001].

[5] Paul Pham and Krysta M. Svore: A 2d nearest-neighbor quantum architecture for factoring. Unpublished manuscript, February 2012.

[6] Paul Pham and Krysta M. Svore: Low-depth quantum architectures. General examination report, February 2012.

[7] David Rosenbaum: Optimal Quantum Circuits for Nearest-Neighbor Architectures. April 2012. [arXiv:1205.0036].

[8] Rodney Van Meter: *Architecture of a Quantum Multicomputer Optimized for Shor's Factoring Algorithm*. Ph.d., Keio University, 2008. [arXiv:0607065v1].

[9] Christof Zalka: Fast versions of Shor ' s quantum factoring algorithm. pp. 1–37, 1998. [arXiv:9806084v1].

[10] Christof Zalka: Shor's algorithm with fewer (pure) qubits. p. 12, January 2006. [arXiv:0601097].