Comparison of the Cost Metrics through Investigation of the Relation between Optimal NCV and Optimal NCT 3-qubit Reversible Circuits

Dmitri Maslov[1] and D. Michael Miller[2]

dmitri.maslov@gmail.com, mmiller@cs.uvic.ca

[1] Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada

[2] Department of Computer Science, University of Victoria, Victoria, BC, V8W 3P6, Canada

December 4, 2006

Abstract

A breadth-first search method for determining optimal 3-qubit circuits composed of quantum NOT, CNOT, controlled-V and controlled-V^+ (NCV) gates is introduced. Results are presented for simple gate count and for technology motivated cost metrics. The optimal NCV circuits are also compared to NCV circuits derived from optimal NOT, CNOT and Toffoli (NCT) gate circuits. The work presented here provides basic results and motivation for continued study of the direct synthesis of NCV circuits, and establishes relations between function realizations in different circuit cost metrics.

1 Introduction

Reversible and quantum logic synthesis have attracted recent attention as a result of advances in quantum and nano technologies. Many of the proposed synthesis methods, especially in the area of reversible logic synthesis, assume large gate libraries where implementation costs of the gates may vary significantly. However, these methods most often target minimization of the gate count. Use of such a circuit cost metric is likely to result in seemingly small circuits, which are in fact expensive to construct.

The synthesis of circuits composed of NOT, CNOT and Toffoli (NCT) gates [18] and multiple control Toffoli gates [1, 5, 10, 11, 20] has recently been extensively studied. Converting an NCT or a multiple control Toffoli gate circuit into one composed of NOT, CNOT, controlled-V and controlled-V^+ (NCV) gates has also been considered

[2, 9]. Further simplification of NCV circuits has also been well studied [9].

It is an important question how close the circuits found by the above approaches are to optimal. The direct synthesis of NCV circuits is also of considerable interest since intuitively one would expect direct synthesis to produce better results than the indirect route via NCT circuits. Finally, we note that observing optimal circuits for small cases often will shed light on good (if not optimal) synthesis approaches applicable to larger problems.

For these reasons, we here present an approach to finding optimal 3-qubit NCV circuits using various cost metrics. We compare these results to those found by mapping optimal NCT circuits to NCV circuits. The advantage of direct NCV synthesis will be clear even for the 3-qubit case. Also, the results clearly demonstrate the difference between using simple gate count and technology motivated cost metrics.

The necessary background is reviewed in Section 2. A breadth-first search procedure to find optimal 3-qubit NCV circuits is given in Section 3 and properties identified in those circuits are discussed in Section 4. Section 5 presents comparative results to circuits derived from NCT circuits and for various cost metrics. Restricted qubit-to-qubit interaction is considered in Section 6. The paper concludes with remarks and suggestions for ongoing research in Section 7.

2 Background

We here provide a brief review of the basic concepts required for this paper. For a more detailed and formal introduction we refer the reader to [14].

A single quantum bit (qubit) has two values, 0 or 1, traditionally depicted as $|0\rangle$ and $|1\rangle$ respectively. The state of a single qubit is a linear combination $\alpha|0\rangle+\beta|1\rangle$ (also written as a vector (α,β)) in the basis $\{|0\rangle,\ |1\rangle\}$, where α and β are complex numbers called the amplitudes, and $|\alpha|^2+|\beta|^2=1$. Real numbers $|\alpha|^2$ and $|\beta|^2$ represent the probabilities (p and q) of reading the values $|0\rangle$ and $|1\rangle$ upon physical measurement of the qubit. The state of a quantum system with $n>1$ qubits is described as an element of the tensor product of the single state spaces yielding a normalized vector of length 2^n called the state vector. Quantum system evolution results in changes of the state vector expressible as products of $2^n\times 2^n$ unitary matrices. This formulation characterizes a transformation but provides no indication of its implementation cost.

In one common approach, small gates are used as elementary building blocks with unit cost [2, 3, 4, 7, 9, 14]. The commonly used gates include:

- NOT ($x\rightarrow\bar{x}$) gate is defined by the matrix $NOT := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

- CNOT gate can be defined as a Boolean transformation $(x,y)\rightarrow(x,x\oplus y)$. In matrix form it is defined as follows

$$CNOT := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

- The 2-bit controlled-V gate is defined by the matrix

$$\text{controlled-}V := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1+i}{2} & \frac{1-i}{2} \\ 0 & 0 & \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}.$$

- Controlled-V^+ is the inverse of controlled-V. Its matrix is the complex conjugate of the matrix for controlled-V.

Controlled-V and controlled-V^+ are also referred to as controlled-sqrt-of-NOT gates since squaring each matrix gives the matrix representation of the CNOT gate. In order to implement a Boolean specification, and assuming an auxiliary qubit is available in addition to the minimal set of qubits needed for reversibility [8], the set of gates NOT, CNOT, controlled-V and controlled-V^+ is complete [14, 18]. We call this set the **NCV** gates.

Definition 1. *The* **NCV-111 cost** *of a circuit composed of NCV gates is the number of gates in the circuit.*

In an alternative approach [12, 17], it is observed that any circuit can be composed with single qubit and CNOT gates and the circuit cost is calculated based on the number of CNOT gates required.

With regards to the NCV library, we next define NCV-012 cost and motivate our definition by the fact that controlled-V and controlled-V^+ gates require at most 2 CNOT gates when decomposed into a circuit with single qubit and CNOT gates ([14], page 181).

Definition 2. *The* **NCV-012 cost** *of an NCV circuit is linear with weights 0, 1, 2, and 2 associated with the gates NOT, CNOT, controlled-V and controlled-V^+, respectively.*

The third cost metric that we consider in this paper is motivated by a recent investigation of the technological costs of quantum and reversible primitives [3, 7] in a quantum system described by an Ising type Hamiltonian ($H = \frac{1}{2}\sum_i w_i \sigma_z^i + \frac{\pi}{2}\sum_{i \neq j} J_{ij}\sigma_z^i\sigma_z^j$). Assuming the Hamiltonian is in a strong-coupling regime (when time scales for addressing a single qubit and a coupling are similar), the cost can be defined as follows:

Definition 3. *The* **NCV-155 cost** *of an NCV circuit is linear with weights 1, 5, 5, and 5 associated with the gates NOT, CNOT, controlled-V and controlled-V^+, respectively.*

However, actual liquid NMR implementations [3] work in a weak-coupling regime. It is likely that using cost metrics where gates NOT, CNOT, and controlled-V (controlled-V^+) have costs 1, $3+x$ and $3+\frac{x}{2}$ for values of x close to or more than 10 would be appropriate in this case. This is because rotations in the $x-y$ plane require pulsing; z-rotations are free (equivalent to changing the rotating reference frame); the zz-coupling operational time is typically greater, on an order of magnitude, than addressing a single qubit; and controlled-V (controlled-V^+) gates use zz interaction half the time of CNOT [3, 7]. Actual timings of the gates will strongly depend upon the chemical properties of the particular molecule chosen for computation [3, 6, 13]. All costs we define here are thus generic.

The approach discussed in this paper is not restricted to the cost metrics we have chosen for illustrative purposes. The search method for example is directly applicable to any cost metric where the cost of a gate is context-free, *i.e.* the cost does not depend on the neighboring gates. It could be adapted to a context-sensitive situation, but we have not yet pursued that. Doing so would significantly complicate and likely slow the search substantially as circuit cost could potentially decrease when a gate is added. Indeed, convergence could only be guaranteed if there is some restriction on when the addition of gates would reduce circuit cost.

Finally, we define the multiple control Toffoli gate [19].

Definition 4. *For the set of Boolean variables* $\{x_1, x_2, ..., x_n\}$ *the* **Toffoli gate** *has the form* $TOF(C;T)$, *where* $C = \{x_{i_1}, x_{i_2}, ..., x_{i_k}\}$, $T = \{x_j\}$ *and* $C \cap T = \emptyset$. *It maps each Boolean pattern* $(x_1^+, x_2^+, ..., x_n^+)$ *to* $(x_1^+, x_2^+, ..., x_{j-1}^+, x_j^+ \oplus x_{i_1}^+ x_{i_2}^+ ... x_{i_k}^+, x_{j+1}^+, ..., x_n^+)$. *$C$ will be called the* **control** *set and T, which always contains a single element, will be called the* **target**.

The Toffoli gate and its generalizations with more than two controls form a good basis for synthesis purposes and have been used by many authors [1, 5, 10, 11, 20]. However, in quantum technologies, Toffoli gates are not simple entities [14, 3]. Rather they are composite gates themselves and Toffoli gates with a large set of controls can be quite expensive [2, 9]. As a result, the NCV-111 cost of a 100-gate Toffoli circuit with 10 input/output qubits can be as low as 100, or may be as high as 15,200. These are, of course, extreme numbers. In Section 5, we show a better analysis of how the costs may differ.

Circuit diagrams are drawn in the popular fashion as used in [14]. Horizontal "wires" represent a single qubit each; the time in the circuit diagrams is propagated from left to right; gate controls are depicted with •; targets appear as $\oplus$ for NOT and CNOT gates, $\boxed{\text{V}}$ for controlled-V gate, and $\boxed{\text{V+}}$ for controlled-V^+ gate with vertical lines joining the control(s) of a gate to its target.

3 The Search Procedure

Our main tool for the investigation of the relations amongst the NCV cost metrics considered and their relation to the most commonly used reversible circuit cost metric, multiple control Toffoli gate count, is a search procedure for the optimal synthesis of NCV circuits for all 40,320 3-variable reversible Boolean functions. For this problem, we use a prioritized, pruned breadth-first search and restrict the set of possible circuits. This is because the search tree for simple full breadth-first search grows too fast for a search to be accomplished in feasible time and space. This is in contrast to using a full breadth-first search for NCT optimal synthesis [18], which is tractable for 3 variable circuits with no search optimizations.

To see the size of the problem, note that the number of base transformations for NCV gates is 21: 3 transformations involve a NOT gate, and the use of the gates CNOT, controlled-V and controlled-V^+ each result in 6 transformations. The results in Table 2 show that the length of the optimal implementations can be up to 16. Thus, the number of nodes at one level of the search tree can be as high as $21^{16} \approx 1.4 * 10^{21}$.

Breadth-first search was previously applied to the synthesis of optimal circuits for the size 3 reversible functions using the NOT, CNOT, and Toffoli gate library [18]. The size of the bottom level of their search tree (branching factor to the power of tree depth) is $9^8 \approx 4.3 * 10^7$ showing that such a search is significantly simpler than the one we are pursuing and requires no techniques to reduce the search space or make the search efficient. In addition, in quantum technologies, Toffoli gates are not simple transformations [14], while synthesis of optimal circuits makes more sense in terms of simple transformations. Our search procedure can find optimal circuits in any weighted gate count metric, not just in the simple gate count metric used in [18]. The authors of [18] do not discuss synthesis of optimal circuits in weighted bases, and we thus assume this was not done.

An earlier attempt to synthesize optimal NCV circuits [21] was capable of synthesizing optimal implementations of maximal cost 7 counting only CNOT, and controlled-sqrt-of-NOT gates. The maximum number of synthesized functions was 10,136 [21], which is about a quarter of all 3-variable reversible functions. Our program synthesizes optimal implementations for *all* 40,320 3-variable reversible functions, and is not tied to a specific cost metric. Further, our search procedure is *significantly* faster: it completes the entire search in less time than the search of all optimal 5-gate implementations in [21].

In [4], the synthesis of some small optimal quantum circuits composed of NCV gates is discussed. The largest 3-variable function synthesized (the so-called Miller gate) has a 6 gate optimal implementation. The reported runtime for the synthesis of this circuit is 318.29 seconds. Hence, the method in [4] cannot synthesize all 3-variable reversible functions in practical time, unlike our approach which requires on the order of one minute for the synthesis optimal circuits for all 40,320 3-variable reversible functions.

In our work, we do not allow a quantum gate (controlled-V and controlled-V^+) to have a control qubit that at that point in the circuit takes a quantum (non-Boolean) value. We do not have a mathematical proof that deleting this *restriction* will not result in construction of smaller circuits. However, numerous experiments indicate that use of a quantum gate with a quantum control qubit does not lead to a more efficient circuit than the one we construct. The above restriction cuts down the search tree and allows us to work with quaternary logic instead of continuous values.

The techniques we have used to reduce the size of the search include:

- Based on the observation above, we can view a quantum function as a base reversible Boolean function plus a quantum signature. In other words, each of the values that may occur in the truth table is stored as a 2-bit number. The values are $|0\rangle$, $|1\rangle$, $\frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle$ and $\frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle$ which are represented by the patterns 00, 10, 01 and 11, respectively. $\frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle$ is the result of applying a controlled-V gate with control value $|1\rangle$ to a qubit in state $|0\rangle$ and the result of applying a controlled-V^+ gate with control value $|1\rangle$ to a qubit in state $|1\rangle$. $\frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle$ is the result of applying a controlled-V gate with control equal $|1\rangle$ to a qubit in state $|1\rangle$ and the result of the application of a controlled-V^+ gate with control equal $|1\rangle$ to a qubit in state $|0\rangle$.

  If every qubit of a 3-qubit quantum function is written using the above encoding, it can be noticed that the set of first bits (24 bits arranged in a 3×8 table) forms a truth table for a reversible specification. This further explains how gates controlled-V and controlled-V^+ operate and motivates our intuition behind calling the set of first bits a reversible parent, and the set of second bits a quantum signature.

- While our final goal is to synthesize all 3-variable reversible functions, and none of the quantum (non-Boolean) functions, the latter still have to be stored and referred to during the search process. Each such function is stored in a queue associated with its parent reversible Boolean function. The quantum function itself is then identified by the function's quantum signature. Clearly, any quantum function is uniquely defined by the parent Boolean function and its quantum signature.

- When we assign a new gate to the existing optimal cascade we never choose a gate with the same set of controls and targets as the immediately previous one in the circuit. This is because such a sequence can always be reduced by template application [9], and thus will not be part of an optimal circuit. This reduces the number of gates that one must consider at each step.

- We note that in an NCV implementation of a reversible function one can interchange controlled-V with controlled-V^+ gates without changing the function realized, provided all such gates are interchanged. In our search procedure, this is accounted for by never using a controlled-V^+ gate as the first quantum gate during construction of an NCV circuit. In this context, the *first quantum gate* is the one that transforms a qubit that contains a Boolean value to a quantum value.

- Once an optimal implementation of a function is found, we have also found an optimal implementation for all functions that differ from this one only by their input-output labeling. This accounts for up to 6 different functions.

- If $G_1G_2...G_k$ is a circuit for a reversible function f, $G_k^{-1}G_{k-1}^{-1}...G_1^{-1}$ is a valid circuit for f^{-1} [9]. It can be shown that for each metric considered in this paper, as well as in any weighted linear metric, if $G_1G_2...G_k$ is optimal for f, then $G_k^{-1}G_{k-1}^{-1}...G_1^{-1}$ will be an optimal implementation for f^{-1} provided each gate type and its inverse are assigned the same cost. From the point of view of the search for optimal circuits, this means that once an optimal circuit for f is found, so is an optimal circuit for f^{-1}. This observation would further help to cut down the search space, however, we have not yet implemented it since our program is fast enough at present. It takes approximately 1 minute to synthesize optimal 3-qubit NCV circuits in each metric on a single 750 MHz processor Sun Blade 1000.

Due to the differing costs of the basis gates, our procedure maintains several queues of functions, each corresponding to the cost associated with the circuits it contains. During the search, new gates are assigned to the circuits with smallest cost not yet considered thereby yielding new circuits to be considered. Lowest cost gates are applied first. However, due to varying gate costs, the first circuit found realizing a Boolean function may not be optimal. To see this, consider the example in Figure 1. Our program finds the non-optimal circuit with NCV-155 cost 7 before the optimal implementation with NCV-155 cost 6. This is because the procedure generates a circuit with two NOT gates before a circuit with a single CNOT gate, and consequently finds the three gate circuit in advance of the cheaper two gate alternative. Note that for the simple gate count metric NCV-111 these two circuits are generated in the opposite order.

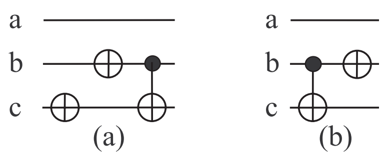

Figure 1: (a) Non-optimal, but first found and (b) optimal in NCV-155 cost metric circuits.

4 Observations on the optimal 3-qubit NCV circuits

Using the above search procedure we found several interesting properties of the optimal 3-qubit NCV circuits.

Optimal implementations found with cost metrics NCV-111 and NCV-155 are interchangeable, and optimal NCV-111 implementations correspond to optimal costs in the NCV-012 cost metric. The diagram in Figure 2 shows which optimal implementations can be substituted without loosing the property of optimality in the corresponding metric. This means that the set of optimal NCV-111 circuits contains circuits optimal in other (NCV-012 and NCV-155) metrics. In Section 5, we make some observations with regard to the NCV-111 metric optimal circuits. The same comparisons apply for optimal NCV-012 and optimal NCV-155 implementations. Further, our experiments with different metrics suggest that the set of optimal NCV-111 circuits will contain optimal implementations in NCV-*xyz* cost metric as long as non-negative integer numbers x, y, and z which represent costs of the gates NOT, CNOT, and controlled-V (and assuming the cost of the controlled-V^+ equals the cost of the controlled-V) satisfy the inequality $y \leq 2z$.

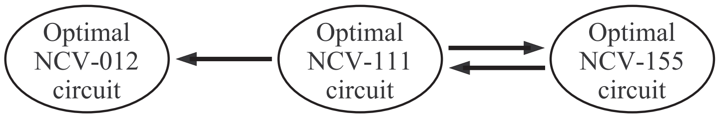

Figure 2: Interchangeability of the optimal implementations.

For the cost metrics NCV-111, NCV-155, and NCV-012, the total number of controlled-V and controlled-V^+ gates in any single circuit is divisible by 3 and is never more than 9. We conjecture that the overall number of controlled-V and controlled-V^+ gates in any NCV implementation of any reversible function is divisible by three.

A 3-variable Toffoli gate and a 3-variable Toffoli gate with one negative control have the same cost in each of the metrics NCV-111, NCV-155, and NCV-012. Some optimal circuits are illustrated in Figure 3. An optimal implementation of a 3-line Toffoli gate with two negative controls has 6 gates.

This observation allows us to generalize the well known result by Barenco *et al.* [2] and improve on the implementation costs of the generalized multiple controlled Toffoli gates in [8] by noting that multiple control Toffoli gates with some, but not all, negative controls, can be implemented with the same cost as the same size Toffoli gate with all positive controls. Figure 4 shows a Toffoli gate with 5 controls, and a circuit implementing it, similar to the one from [2]. Since the cost of a 3-variable Toffoli gate with one negative control equals the cost of a 3-variable Toffoli gate with two positive controls, the multiple control Toffoli gate illustrated in Figure 4 will have a cost equal to the cost of the same size Toffoli gate having only positive controls. It turns out that further

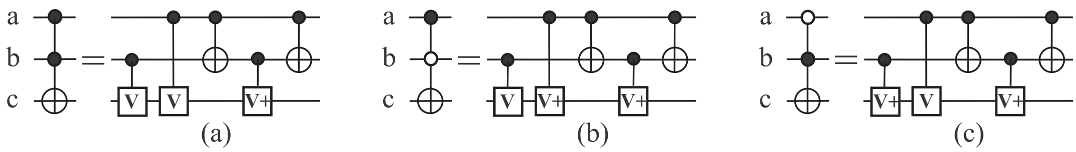

Figure 3: (a) optimal NCV realization of the Toffoli gate (b),(c) optimal NCV realizations of the Toffoli gate with a single negative control.

simplification of the circuits for a multiple control Toffoli gate and a multiple control Toffoli gate with some but not all negations results in equal reductions in terms of the associated quantum gate count [9]. However, such simplified realizations are still not guaranteed to be optimal.

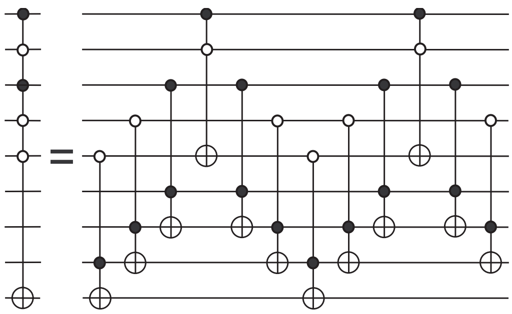

Figure 4: Construction of a large Toffoli gate with some but not all negative controls.

Observing all optimal implementations in the NCV-111 metric we came to the conclusion that every Boolean function $f(x_1,x_2)$ of two variables can be computed by a quantum circuit with no more than 5 gates. If this function is from Boolean class 0 (when $f(0,0)=0$), only 4 quantum gates are required.

As noted above the search procedure can be applied for other cost metrics. For example, we have synthesized optimal circuits assuming a weak coupling computational mode as would be supported by liquid NMR technology with the qubit-to-qubit interaction strength approximately 10 times weaker than addressing a single qubit. The cost metric applied in this case is $Cost(NOT)=1$, $Cost(controlled-V)=Cost(controlled-V^{+})=9$, and $Cost(CNOT)=14$. The distribution of the number of functions with respect to optimal cost realizations, given as (cost, number of functions), is (0, 1), (1, 3), (2, 3), (3, 1), (14, 6), (15, 24), (16, 18), (28, 24), (29, 117), (30, 51), (41, 24), (42, 159), (43, 342), (44, 75), (55, 132), (56, 762), (57, 597), (58, 45), (69, 396), (70, 2424), (71, 540), (82, 360), (83, 2508), (84, 4208), (85, 140), (96, 1440), (97, 8988), (98, 1764), (110, 552), (111, 3860), (112, 4), (123, 1232), (124, 8228), (125, 396), (137, 112), (138, 784). This example is included to show the flexibility of the approach and is not pursued further in this paper.

5 Comparisons of the Sets of Optimal Circuits

In this section, we compare the NCV-111 (NCV-012 and NCV-155) costs for the optimal synthesis of 3-variable reversible functions using Toffoli gates up to size 3 (NCT library, [18]) with the costs of optimal NCV circuits. We note that our implementation of the breadth-first search for the 3-variable reversible NCT circuits may differ from the original as discussed in [18]. Due to the large number of optimal NCT circuits for some functions, the results shown below may vary slightly depending on the actual program implementation. Further, the comparison is done through substitution of every Toffoli gate in an optimal NCT circuit with a 5-gate NCV circuit ([14], page 182), and thus assigning a cost of 5 in the NCV-111 metric. Gates NOT and CNOT are present in both libraries, NCT and NCV, and thus require no specific attention.

5.1 Optimal NCV-111 vs. Optimal NCT Circuits

Table 1 shows the number of 3-variable reversible functions with circuits of the costs indicated. The second and third columns refer to the optimal NCT circuits reported in [18] for NCT gate count and NCV-111 cost. The fourth column is the NCV-111 cost for the circuits found by our search procedure. Table 1 also reports the weighted average (WA) for the three scenarios.

The third and fourth columns of Table 1 show the substantial difference between the NCV-111 cost of the optimal NCT and optimal direct NCV-111 implementations for all 3-variable reversible functions. By comparing the two circuits for each function, we have found that the maximal ratio of the cost of one optimal implementation over the other is $3.375 = \frac{27}{8}$. That is, even for circuits with a small number of inputs/outputs an optimal Toffoli circuit transformed to NCV can be a factor of 3.375 larger that the optimal NCV realization. We also observe that on average, the optimal NCT circuit is 1.3902 times more expensive (for the NCV-111 metric) than the corresponding optimal NCV circuit found by our search procedure.

The important question of whether the NCT and NCV costs are related is addressed by computing the correlation between the NCV-111 costs of the optimal NCT and optimal (in NCV-111 metric) NCV circuits. The correlation coefficient equals 0.896. We conclude that the costs are reasonably but not strongly correlated. Finally, we found it interesting to determine how many optimal NCT circuits have optimal NCV-111 cost. There are 1,610 (4%).

The results are illustrated in the cost comparison chart in Figure 5.

	Opt. NCT		Opt. NCV-111
Cost	GC [18]	NCV-111	NCV-111
0	1	1	1
1	12	9	9
2	102	51	51
3	625	187	187
4	2780	392	417
5	8921	475	714
6	17049	259	1373
7	10253	335	3176
8	577	1300	4470
9	0	3037	4122
10	0	3394	10008
11	0	793	5036
12	0	929	1236
13	0	4009	8340
14	0	8318	1180
15	0	4385	0
16	0	255	0
17	0	1297	0
18	0	4626	0
19	0	4804	0
20	0	475	0
21	0	106	0
22	0	503	0
23	0	357	0
24	0	4	0
27	0	17	0
28	0	2	0
WA	5.8655	14.0548	10.0319

Table 1: Optimal NCT and optimal NCV-111 NCV circuits.

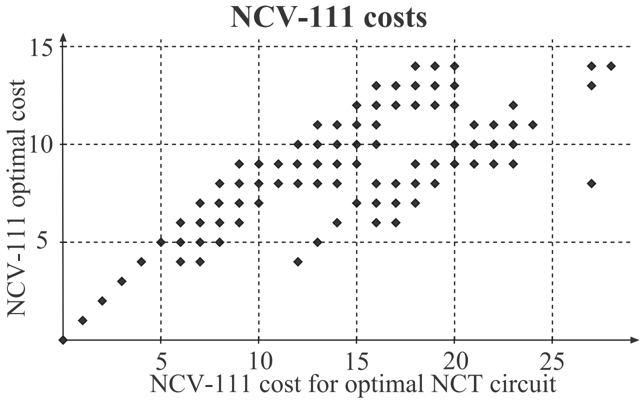

Figure 5: Optimal NCT (X-coordinate) vs. optimal NCV-111 (Y-coordinate) circuits for the NCV-111 cost metric. Each data point corresponds to a number of functions.

5.2 Optimal NCV-012 vs. Optimal NCT Circuits

We considered the set of optimal NCV-012 circuits as created by our program. Optimal NCV-111 implementations were not substituted for those optimal NCV-012 circuits whose NCV gate count is not optimal.

A comparison of the NCV-012 costs of optimal NCV-012 NCV circuits and NCT circuits is made in Table 2 and Figure 6. The presentation is analogous to the one above for the NCV-111 costs metric. The maximum ratio of NCT optimal circuit for NCV-012 cost over NCV-012 optimal circuit NCV-012 cost equals 8 ($= \frac{16}{2}$). The optimal NCT and optimal NCV-012 circuits for one such function are illustrated in Figure 7). On average, however, this ratio is 1.2728. Correlation between the costs is 0.8999, which is almost identical to the correlation between optimal NCT and optimal NCV-111 circuits in the NCV-111 cost metric. The number of functions where the NCV-012 cost of an optimal NCT circuit equals the NCV-012 cost of an optimal NCV-012 circuit is 1,774 (4.4%).

6 Optimal Implementations with Restricted Qubit-to-Qubit Interactions

In the work above, we assumed that a direct interaction between any two qubit can be established (*e.g.* a 2-qubit gate can use any two qubits). However, due to the specifics of a particular physical realization, this may not always be the case. Some of the qubit-to-qubit interactions may only be available indirectly. On the other hand, in every n-bit quantum computation it must always be possible to construct a connected graph with vertices representing qubits and edges representing the possibility of the direct interaction between qubits. In the case $n = 3$, there are only two non-isomorphic connected graphs. One is the complete graph, and the second is a star (all vertices

	Opt. NCT		Opt. NCV-012	
Cost	GC	NCV-012	NCV-012	NCV-111
0	1	8	8	1
1	12	48	48	9
2	102	183	192	45
3	625	398	408	142
4	2780	486	480	315
5	8921	201	192	585
6	17049	16	16	1169
7	10253	0	192	2286
8	577	47	1056	3414
9	0	352	3168	4790
10	0	1347	4320	6744
11	0	3130	672	6420
12	0	3340	0	4328
13	0	561	0	4360
14	0	3	2880	4032
15	0	0	11520	1568
16	0	162	4416	112
17	0	1219	0	0
18	0	4435	0	0
19	0	8029	0	0
20	0	3872	0	0
21	0	128	9856	0
22	0	0	896	0
24	0	341	0	0
25	0	1946	0	0
26	0	4482	0	0
27	0	3977	0	0
28	0	609	0	0
29	0	6	0	0
32	0	289	0	0
33	0	489	0	0
34	0	194	0	0
35	0	3	0	0
40	0	16	0	0
41	0	3	0	0
WA	5.8655	19.1011	14.9800	10.5800

Table 2: Optimal size 3 reversible circuit NCV-012 costs in NCT and NCV bases. Each data point corresponds to a number of functions.

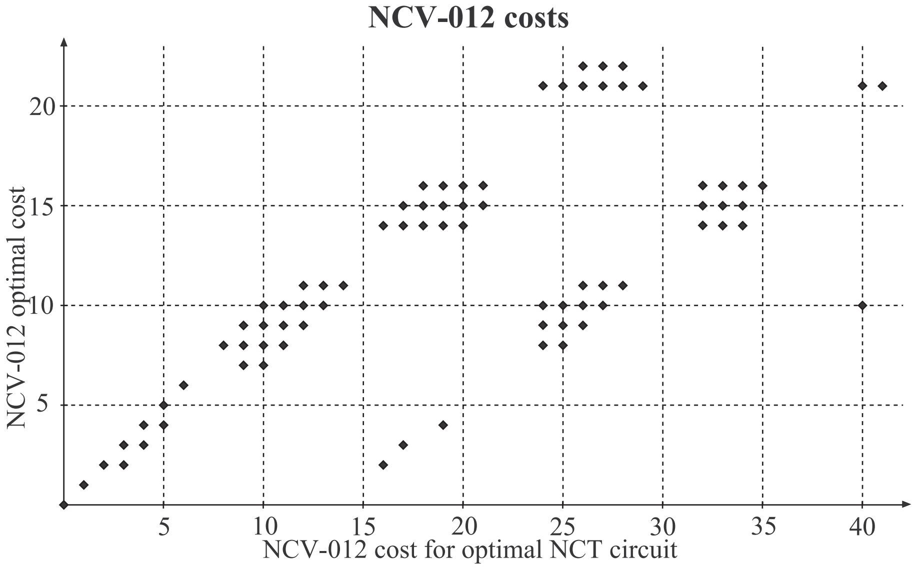

Figure 6: Optimal NCT (X-coordinate) vs. optimal NCV-012 (Y-coordinate) circuits for the NCV-012 cost metric. Each data point corresponds to a number of functions.

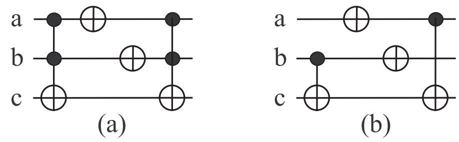

Figure 7: (a) optimal NCT and (b) optimal NCV-012 circuits for the function $[7,6,4,5,2,3,1,0]$.

are connected to one), see Figure 8. In this section we report results for the optimal synthesis assuming direct interactions are allowed between qubits *a* and *b*, and *b* and *c*, but not between *a* and *c*. We assume the NCV-111 cost metric, however, the results can be calculated for other metrics. The numbers of functions requiring 0..23 gates are 1, 7, 29, 82, 181, 334, 374, 334, 337, 753, 1652, 2654, 2482, 1674, 1350, 3236, 6304, 6028, 1508, 1302, 2566, 4314, 2804, and 14. There are no functions requiring more than 23 gates.

It is interesting that in the case of non-restricted qubit interactions one of the cheapest non-linear (with respect to EXOR) reversible gates is the Peres gate [15] defined by the transformation $(a,b,c) \mapsto (a, b \oplus a, c \oplus ab)$. It can be implemented with 4 quantum NCV gates. An analogous (smallest non-linear reversible gate with a similar transformation) of this gate in the case of restricted qubit interactions is the gate defined by the transformation $(a,b,c) \mapsto (b,a,c \oplus ab)$. It requires 6 quantum NCV gates as illustrated in Figure 9(a). Toffoli gates $TOF(a,b;c)$ and $TOF(b,c;a)$ require 9 elementary quantum gates each and can be thought of as a SWAP gate (3 CNOTs)

Figure 8: Non-isomorphic graphs with three vertices: star (left) and complete graph (right).

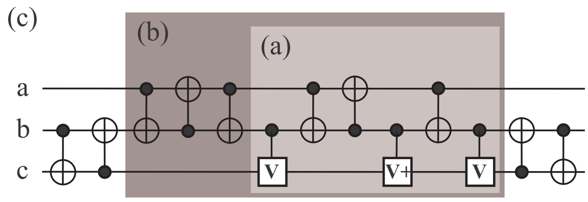

Figure 9: Optimal circuits for (a) $(a,b,c) \mapsto (b,a,c \oplus ab)$, (b) $TOF(a,b;c)$, and (c) $TOF(a,c;b)$.

followed by the $(a,b,c) \mapsto (b,a,c \oplus ab)$ transformation. An optimal implementation of $TOF(a,b;c)$ is illustrated in Figure 9(b). Toffoli gate $TOF(a,c;b)$ is somewhat more expensive. It requires 13 elementary quantum operations in its optimal implementation (see Figure 9(c)).

7 Conclusion

The results in Section 5 lead us to the following conclusion. Minimization of Toffoli gate count as a criterion for a reversible synthesis method is not optimal with respect to implementation technologies and even for small parameters may result in a seemingly small circuit which may be as far off a technologically favorable implementation as a factor of 8. It is natural to expect that for circuits with more variables the difference will grow. We suggest that for estimating implementation cost, the commonly used gate count metric should be replaced with a metric that accounts for the different costs of large building block (*i.e.*, Toffoli gates), such as the weighted gate cost presented here. Using such a metric would lead to the technologically favorable circuit (b) in Figure 7. To further illustrate the application of this work, we note that libraries of optimal implementations form a basis for peep-hole type optimizations such as the one reported in [16], and optimal implementation of Toffoli gate with a negative control was used in [9] for the improved realization of multiple control Toffoli gates with negative controls.

Acknowledgments

This work was supported in part by a Post-Doctoral Fellowship and a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

References

[1] Agrawal, A., and Jha, N. K.: 'Synthesis of reversible logic'. *Proc. Conf. on Design Automation and Test in Europe*, February 2004, pp. 21384–21385.

[2] Barenco, A., Bennett, C. H., R.,Cleve, DiVinchenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J. A., and Weinfurter, H.: 'Elementary gates for quantum computation'. *Phys. Rev. A*, 1995, 52, pp. 3457–3467.

[3] Cory, D. G., Laflamme, R., Knill, E., Viola, L., Havel, T. F., Boulant, N., Boutis, G., Fortunato, E., Lloyd, S., Martinez, R., Negrevergne, C., Pravia, M., Sharf, Y., Teklemariam, G., Weinstein, Y. S., and Zurek, W. H.: 'NMR based quantum information processing: achievements and prospects', http://arxiv.org/abs/quant-ph/0004104, April, 2000.

[4] Hung, W. N. N., Song, X., Yang, G., Yang, J., and Perkowski, M. A.: 'Quantum logic synthesis by symbolic reachability analysis', *Proc. Design Automation Conf.*, June, 2004, pp. 838–841.

[5] Kerntopf, P.: 'A new heuristic algorithm for reversible logic synthesis', *Proc. Deaign Automation Conf.*, June, 2004, pp. 834–837.

[6] Knill, E., Laflamme, R., Martinez, R., and Negrevergne, C.: 'Implementation of the five qubit error correction benchmark', *Physical Review Letters*, 86:5811, 2001.

[7] Lee, S., Lee, S., Kim, T., Lee, J.-S., Biamonte, J., and Perkowski, M. A.: 'The cost of quantum gate primitivess', *Journal of Multi-valued Logic and Soft Computing*, 12 pp., in press.

[8] Maslov, D., and Dueck, G. W.: 'Reversible cascades with minimal garbage,' *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, 2004, 23, (11), pp. 1497–1509.

[9] Maslov, D., Dueck, G. W., and Miller, D. M.: 'Quantum circuit simplification and level compaction', April 2006, http://arxiv.org/abs/quant-ph/0604001.

[10] Miller, D. M., Maslov, D., and Dueck, G. W.: 'A transformation based algorithm for reversible logic synthesis', *Proc. Design Automation Conf.*, June 2003, pp. 318–323.

[11] Mishchenko, A., and Perkowski, M. A.: ‘Logic synthesis of reversible wave cascades’, *Proc. Intl. Workshop on Logic Synthesis*, June 2002, pp. 197–202.

[12] Mottonen, M., Vartiainen, J. J., Bergholm, V., and Salomaa, M. M.: ‘Quantum circuits for general multiqubit gates’, *Physical Review Letters*, 2004, 93(130502).

[13] Negrevergne, C., Mahesh, T. S., Ryan, C. A., Ditty, M., Cyr-Racine, F.,Power, W., Boulant, N., Havel, T., Cory, D. G., and Laflamme, R.: ‘Benchmarking quantum control methods on a 12-qubit system’, *Physical Review Letters*, 2006, 96:170501.

[14] Nielsen, M., and Chuang, I.: ‘Quantum Computation and Quantum Information’ (Cambridge University Press, 2000)

[15] Peres, A.: ‘Reversible logic and quantum computers’, *Physical Review A*, 1985, 32:3266–3276.

[16] Prasad, A. K., Shende, V. V., Patel, K. N., Markov, I. L., and Hayes, J. P.: ‘Data structures and algorithms for simplifying reversible circuits’, *ACM Journal on Emerging Technologies in Computing Systems*, in press.

[17] Shende, V. V., Markov, I. L., and Bullock, S. S.: ‘Synthesis of quantum logic circuits’, *Proc. Asia-South Pacific Design Automation Conf.*, January 2005, pp. 272-275.

[18] Shende, V. V., Prasad, A. K., Markov, I. L., and Hayes, J. P.: ‘Synthesis of reversible logic circuits’, *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, 2003, 22, (6), pp. 723–729.

[19] Toffoli, T.: ‘Reversible computing’, *Tech. memo MIT/LCS/TM-151, MIT Lab for Comp. Sci*, 1980.

[20] Tsai, I. M., and Kuo, S. Y.: ‘Quantum Boolean circuit construction and layout under locality constraints’, *Proc. IEEE Conf. on Nanotechnology*, 2001, pages 111–116.

[21] Yang, G., Hung, W. N. N., Song, X., and Perkowski, M. A.: ‘Exact synthesis of 3-qubit quantum circuits from non-binary quantum gates using multiple-valued logic and group theory’, *Proc. Conf. on Design Automation and Test in Europe*, 2005, pp. 434–435.