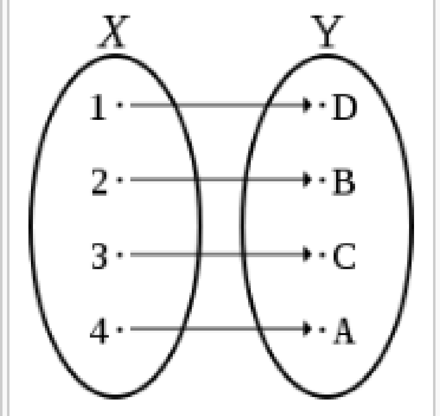
Quantum Gates to Reduce the Quantum Cost of Reversible Circuit

Md. Mazder Rahman†, Anindita Banerjee*, Gerhard W. Dueck†, and Anirban Pathak#
†Faculty of Computer Science, University of New Brunswick, Canada
*Department of Physics and Center for Astroparticle Physics and Space Science,
Bose Institute, Block EN, Sector V, Kolkata 700091, India
#Department of Physics and Material Science Engineering, Jaypee Institute of Information Technology, Noida, INDIA

This work presents a quantum gate library that consists of all possible two-qubit quantum gates which do not produce entangled state as output. Therefore, these gates can be used to reduce the quantum costs of reversible circuits. Experimental results show a significant reduction of quantum cost in benchmark circuits. The resulting circuits could be further optimized with existing tools, such as quantum template matching.

Reversible Function: A logic function is said to be reversible if there is a one-to-one and onto mapping between input vectors and output vector.

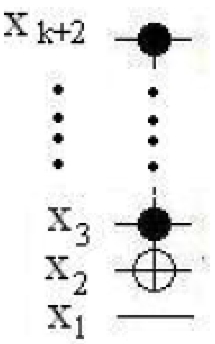


A bijective function, f:X→Y, where set X is {1, 2, 3, 4} and set Y is {A, B, C, D}. For example, f(1) = D.

Reversible gates such as Toffoli, Peres and Fredkin are conventionally used to synthesize reversible circuits. However, Toffoli based synthesis of reversible circuits is prevalent.

Reversible gate library: NCT: NOT, CNOT, Toffoli. This gate library was introduced by Toffoli in his 1980 paper. This library is the smallest complete set of gates. However, an additional garbage bit (not every reversible specification can be realized with zero garbage) may be required by this model.

A generalized multiple-control Toffoli gate is defined as TOFn(C, T) based on number of control lines n, which maps each pattern (xi1 , xi2 , ..., xik) to (xi1 , xi2 , ..., xj−1, xj EXOR xi1 xi2 . . . xj−1 xj+1 . . . xik , xj+1, . . . , xik), where C = {xi1 , xi2 , ..., xik}, T = {xj} and C ∩ T = null set.



C is referred to as the control set

T is referred to as the target set.

TOF0 is NOT gate

TOF1 is CNOT gate

Controlled −V gate is represented as Mv

$$M_v = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{(1+i)}{2} & \frac{(1-i)}{2} \\ 0 & 0 & \frac{(1-i)}{2} & \frac{(1+i)}{2} \end{bmatrix}$$

The **quantum cost** of a circuit is defined by the total number of elementary quantum gates needed to realize the given function. Every elementary quantum gate requires a single operation of **unit cost.**

The quantum gate library which is used in synthesis of all reversible functions.

NOT			Controlled-V
	CNOT		
		Controlled-V+	

Haghparast and Eshghi have given following two prescriptions for calculation of quantum cost:

1. Implement a circuit/gate using only the quantum primitive (2x2) and (4x4) gates and count them.
2. Synthesize the new circuit/gate using the well known gates whose quantum cost is specified and add up their quantum cost to calculate total quantum cost.

In both of these cases we will obtain linear cost metric and consequently the quantum cost obtained in these two procedures may be higher than the actual one unless local optimization algorithms are applied to the entire circuit.

When we apply the local optimization algorithm on the entire circuit then we obtain a nonlinear cost metric.

The proposed algorithm will calculate the nonlinear cost metric.

CRITERION

An arbitrary qubit can be described as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ where α and β are complex numbers which satisfy: $|\alpha|^2 + |\beta|^2 = 1.$

Similarly a generalized two qubit state can be described as $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|10\rangle = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$

This state is separable as tensor product of two states if and only if ad = bc otherwise the state is entangled. This condition can be visualized easily if we consider the tensor product of two single qubit states denoted by $\alpha|0\rangle + \beta|1\rangle$ and $\alpha'|0\rangle + \beta'|1\rangle$

The product state is $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' \\ \alpha\beta' \\ \beta\alpha' \\ \beta\beta' \end{pmatrix}$ which satisfy the condition of separability

$$\alpha\alpha'\beta\beta' \;=\; \alpha\beta'\beta\alpha'$$

This criterion is important because our two qubit gate library does not include those gates which produce an entangled output state.

Consequently after construction of every new gate by multiplication of two existing valid gates we check whether the output states of the new gate is entangled or not (i.e. whether they violate the condition or not). If condition is violated for a gate for any allowed input states then the gate is not valid and is not a member of the library to be constituted.

BUILDING GATE LIBRARY

Any sequence of single qubit and two-qubit elementary quantum gates acting on the same two qubits can be form a new two-qubit quantum gate.

Set of Input vectors

$$I = \{00, 01, 0V_0, 0V_1, 10, 11, 1V_0, 1V_1, V_00, V_01, V_0V_0, V_0V_1, V_10, V_11, V_1V_0, V_1V_1\}.$$

Set of initial gates in gate library

$$Q = \{V(a,b), V(b,a), V^+(a,b), V^+(b,a), T(a,b), T(b,a), T(b), T(a)\}$$

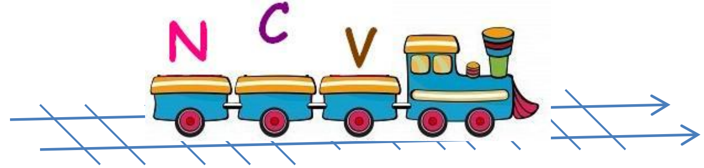
We have considered only binary values 0 and 1 at the control inputs else it results in entangled state vectors.

BEGIN:

$GL = \phi$
foreach $i \in \{1, 2, \cdots, m\}$
$GL = GL \cup QG_i^M$
end
$n = m$
foreach $j \in \{1, 2, \cdots, n\}$
..**foreach** $k \in \{1, 2 \cdots, m\}$
..... $R_M = QG_k^M * GL_j^M$
.......**if**$(R_M \neq I)$ // check Identity
..........**if**$(R_M \notin \forall_n GL_n^M)$ //check match
.... $O_v = \phi$
............**foreach** $p \in \{1, 2, \cdots, l\}$
.... $V_o = R_M * IV_P$ // apply input vectors
.... **if**$(V_o \in \forall_l IV_l)$
.... $O_v = O_v \cup V_o$
.................**end if**
............**end**
.................**if** $(NE(O_v) \geq 4)$ // good outputs?
.... $n = n + 1$
.... $GL = GL \cup R_M$ // gate library update
.................**end if**
..........**end if**
.......**end if**
..**end**
end

END.

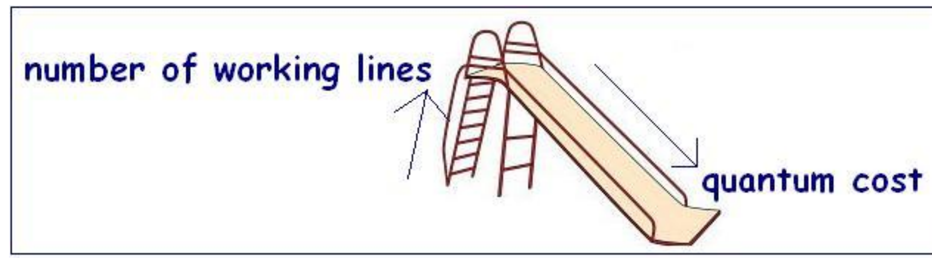
Gate	Possible Outputs
V(a,b)T(b,a)V(a,b)T(a)V+(a,b)	'1b' '0b' '1a' '0a'
V(a,b)T(b,a)V(a,b)T(a)T(a,b)	'11' '0b' '10' '0a'
V(a,b)T(b,a)V+(a,b)T(a)V(a,b)	'1a' '0a' '1b' '0b'
V(a,b)T(b,a)V+(a,b)T(a)V+(a,b)	'1b' '0a' '1a' '0b'
V(a,b)T(b,a)T(a,b)T(b)V(b,a)	'a1' 'b1' '00' '10'
V(a,b)T(b,a)T(a,b)T(b)V+(b,a)	'b1' 'a1' '00' '10'
V(a,b)T(b,a)T(b)V(b,a)T(b)	'a0' '11' '01' 'b0'
V(a,b)T(b,a)T(b)V+(b,a)T(b)	'b0' '11' '01' 'a0'
V(a,b)T(b,a)T(a)V(a,b)T(a)	'0a' '11' '0b' '10'
V(a,b)T(b,a)T(a)V+(a,b)T(a)	'0b' '11' '0a' '10'
V(a,b)T(b,a)T(a)T(a,b)V(b,a)	'b1' 'a1' '10' '00'
V(a,b)T(b,a)T(a)T(a,b)V+(b,a)	'a1' 'b1' '10' '00'
V(a,b)T(b)T(b,a)V(a,b)T(a)	'0b' '10' '0a' '11'
V(a,b)T(b)T(b,a)V+(a,b)T(a)	'0a' '10' '0b' '11'
V(a,b)T(a)V(a,b)V(b,a)T(b)	'b0' '11' 'a0' '01'
V(a,b)T(a)V(a,b)V(b,a)T(a)	'a1' '00' 'b1' '10'
V(a,b)T(a)V(a,b)V+(b,a)T(b)	'a0' '11' 'b0' '01'
V(a,b)T(a)V(a,b)V+(b,a)T(a)	'b1' '00' 'a1' '10'
V(a,b)T(a)V(a,b)T(b,a)V(a,b)	'01' '1a' '1b' '00'
V(a,b)T(a)V(a,b)T(b,a)V+(a,b)	'01' '1b' '1a' '00'
V(a,b)T(a)V(a,b)T(b,a)T(b)	'00' '11' '10' '01'
V(a,b)T(a)V(a,b)T(b,a)T(a)	'11' '00' '01' '10'
V(a,b)T(a)V+(a,b)V(b,a)T(b)	'11' 'b0' 'a0' '01'

REVERSIBLE CIRCUITS  QUANTUM CIRCUITS

☑The decomposition of reversible circuits depends on the number of control lines m of Multiple Controlled Toffoli gate and the number of working lines n in the reversible circuits.

☑At least one working line is needed to decompose a TOFm gate (where n ≥3 and m = n−1) into quantum circuit.

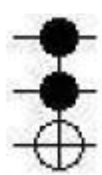
☑Pairing of Toffoli gates in beneficial manner result in lesser QC.

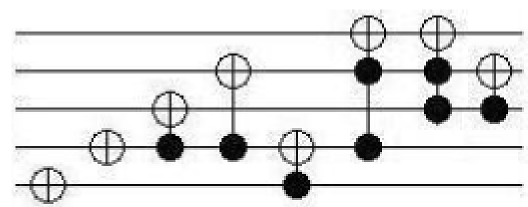


Toffoli gate

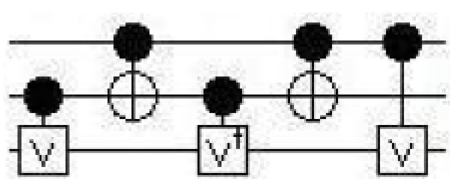
Mod5 function

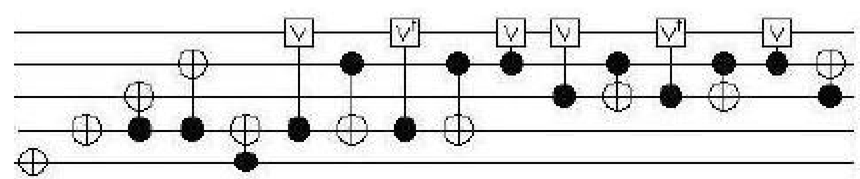
Reversible circuit



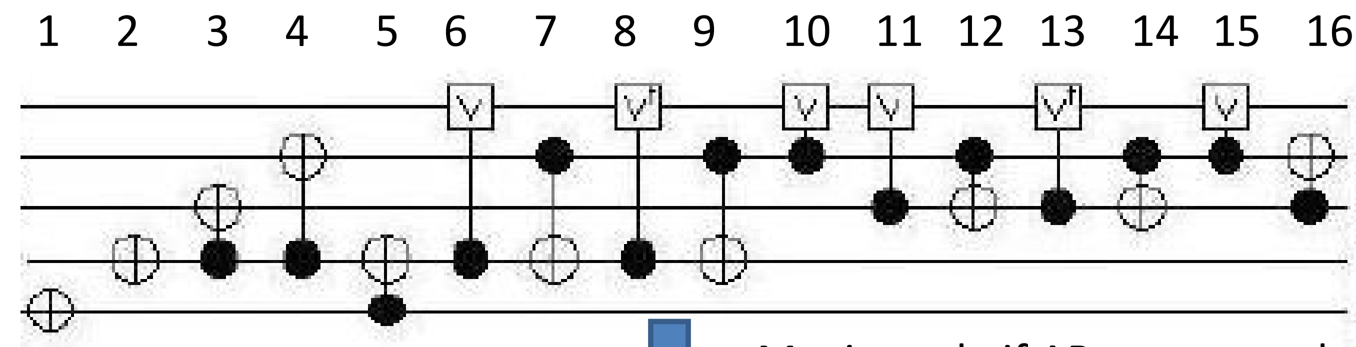


Quantum circuit

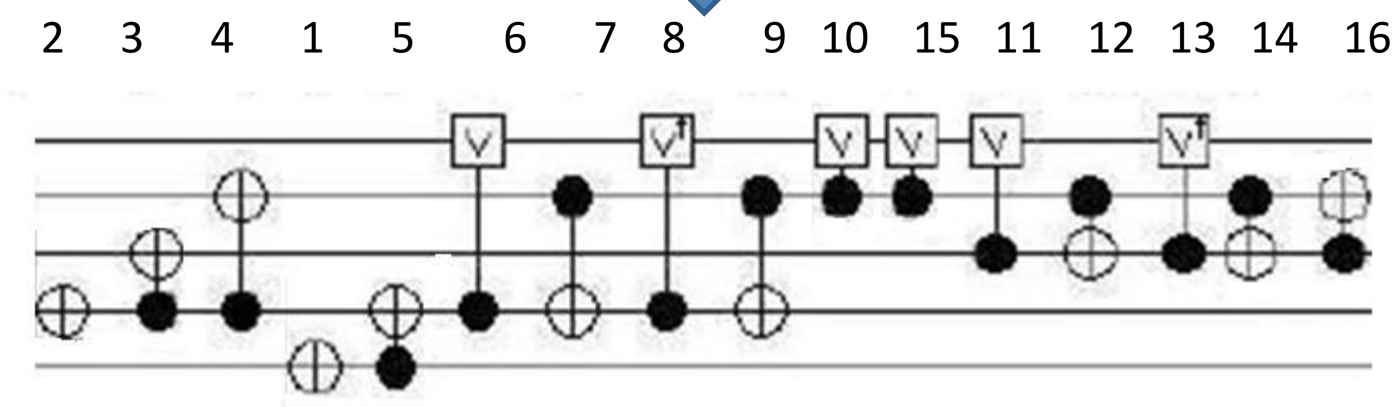




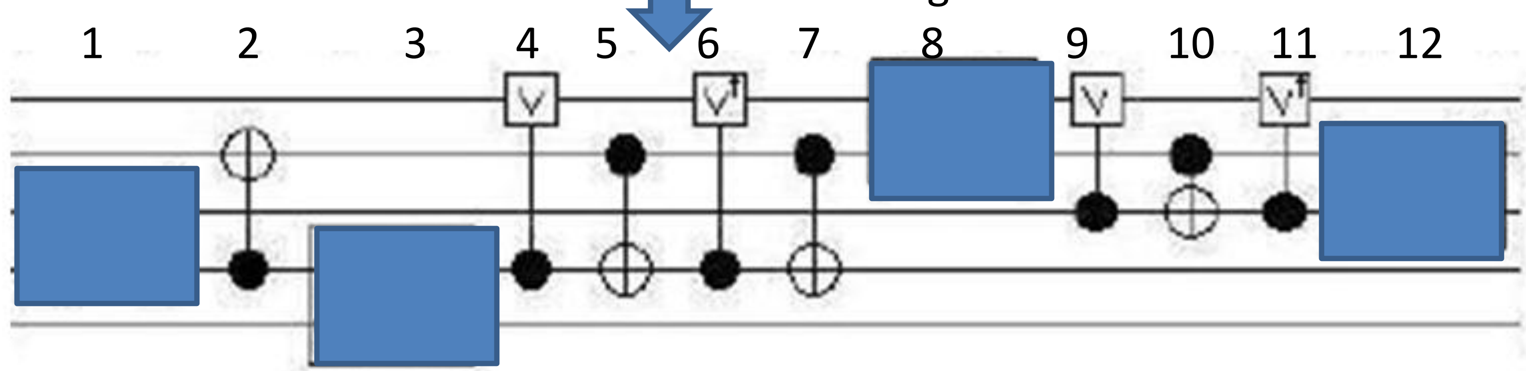
QUANTUM COST OPTIMIZATION BY USING GENERALIZED TWO-QUBIT GATES



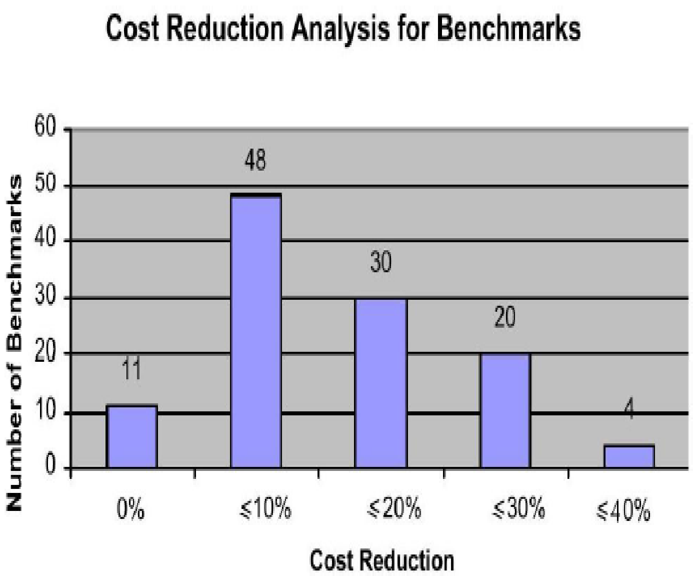
Moving rule if AB commute then move AB=BA



Introducing New Gates



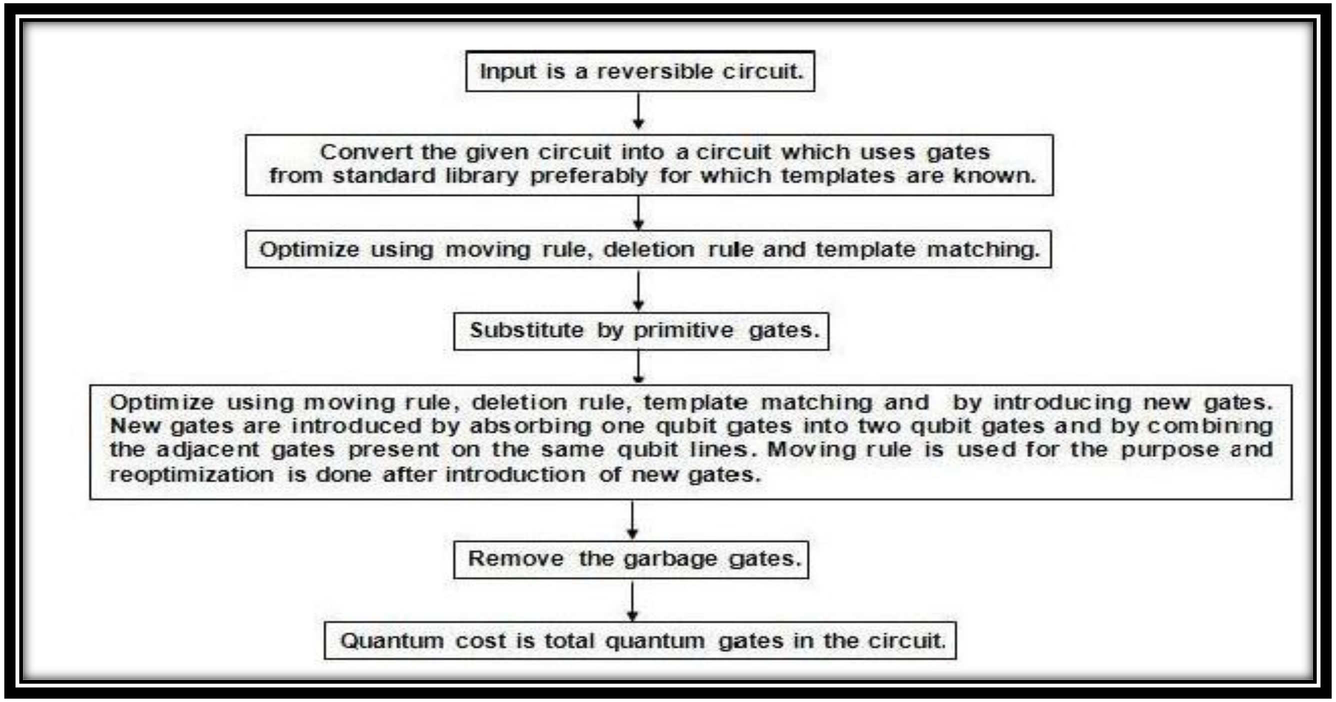
EXPERIMENTAL RESULTS



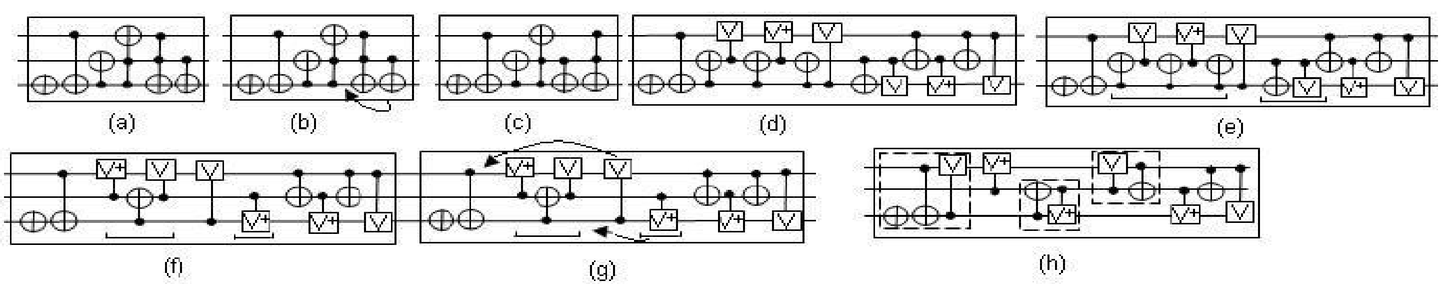
Analysis of costs reduction.

Benchmark	Gates	Lines	QC(before)	WL	QC(after)	Cost Red. (%)
ex-1_166	4	3	8	0	5	37.50
3_17_13	6	3	14	0	9	35.71
4mod5-v0_18	9	5	25	0	17	32.00
3_17_15	10	3	10	0	7	30.00
3_17_14	6	3	14	0	10	28.57
fredkin_5	7	3	7	0	5	28.57
alu-v1_29	7	5	15	0	11	26.67
alu-v2_33	7	5	15	0	11	26.67
alu-v3_35	7	5	15	0	11	26.67
alu-v4_37	7	5	15	0	11	26.67
4gt11_82	12	5	16	0	12	25.00
mod5d2_70	8	5	16	0	12	25.00
4gt11_83	8	5	12	0	9	25.00
miller_12	8	3	8	0	6	25.00
miller_11	5	3	17	0	13	23.53
rd32-v1_68	5	4	13	0	10	23.08
decod24-v2_43	6	4	18	0	14	22.22
decod24-v0_40	9	4	9	0	7	22.22
decod24-v2_44	9	4	9	0	7	22.22
decod24-v3_46	9	4	9	0	7	22.22
alu-v0_27	6	5	14	0	11	21.43
alu-v3_34	7	5	19	0	15	21.05
alu-v1_28	7	5	15	0	12	20.00
fredkin_6	3	3	15	0	12	20.00
4_49_16	16	4	74	1	60	18.92
4_49_17	12	4	32	0	26	18.75
mod5d1_63	7	5	11	0	9	18.18
sym9_146	28	12	108	0	89	17.59
rd73_140	20	10	76	0	63	17.11
sys6-v0_111	20	10	72	0	60	16.67
4gt5_76	13	5	36	0	30	16.67
4mod5-v1_23	8	5	24	0	20	16.67
decod24-v0_38	6	4	18	0	15	16.67
rd32-v0_66	4	4	12	0	10	16.67
rd53_138.	12	8	44	0	37	15.91
hwb4_50	16	4	78	1	66	15.38
4mod5-v0_19	5	5	13	0	11	15.38
4mod5-v1_24	5	5	13	0	11	15.38
rd84_142	28	15	112	0	95	15.18
0410184_170	74	14	74	0	63	14.86
0410184_170	46	14	90	0	77	14.44

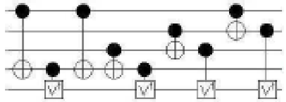
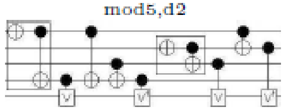
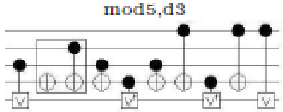
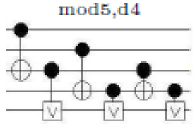
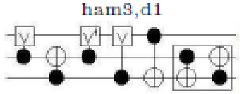
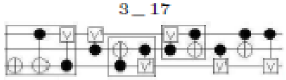
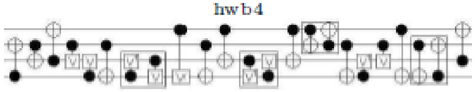
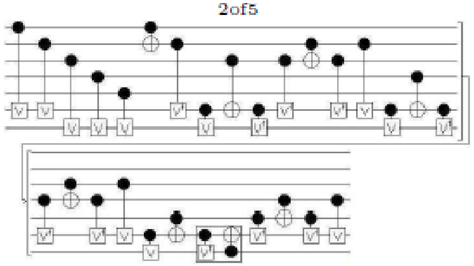
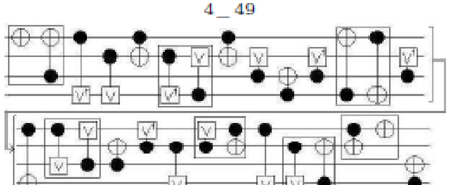
Algorithm for minimization of quantum cost



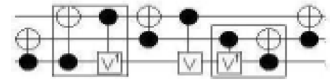
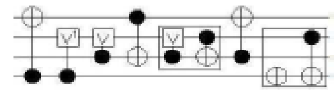
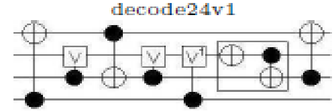
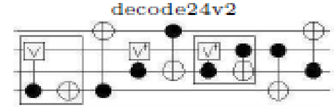
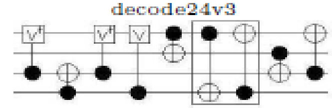
Suppose we have a template: $U_1U_2U_3U_4U_5$=I (where U_i is an unitary gate) and in the optimization procedure we come across a sequence of gates $U_2U_3U_4$ then we can replace this sequence of gates by $U_1^{-1}U_5^{-1}$.



Reversible circuit for function 3_17 . b) Commutation rule is applied and arrow shows the movement of Cnot gate.
c) NCT circuit before substitution of primitives d) Quantum circuit of 3_17 function obtained by substituting the Toffoli gates with primitives. e) Template matching tool is applied to the circuit. f) Quantum circuit with reduced gate count.
g) Modified local optimization rule is applied and two movements have been done in the circuit as indicated by the arrows.
h) New gates are introduced (each box is a new gate) and quantum cost is 7.

Circuit	GC	QC 32	QC 36	QC 6	Ours
mod5,d1 	24	24	14	-	9
mod5,d2 	25	19	11	-	9
mod5,d3 	13	13	9	13	9
mod5,d4 	9	7	-	-	6
ham3,d1 	9	7	7	9	5
3_17 	14	12	10	14	7
hwb4 	23	23	21	-	19
2of5 	40	32	29	-	28
4_49 	32	32	27	-	21

RESULTS

Circuit	GC	QC Revlib	Ours
miller gate 	8	8	6
3_17 	10	10	7
decode24v0 	9	9	7
decode24v1 	9	9	7
decode24v2 	9	9	7
decode24v3 	9	9	8