Research Center for Quantum Information

Towards optimization of quantum circuits

Michal Sedlák
msm@sedos.sk

Supervisor: PhD. Martin Plesch

Introduction

Practical realization of

- **quantum communication**
- **quantum cryptography**
- **quantum computation**

assumes that we are able to control chosen quantum system i.e.:

- **Prepare it in chosen state**
- **Perform a desired operation on it**
- **carry out measurement**

Introduction

In the real experiments we are able to control only:

- interaction between pairs of two-level subsystems **(qubits)**
- interaction between selected qubit and the environment

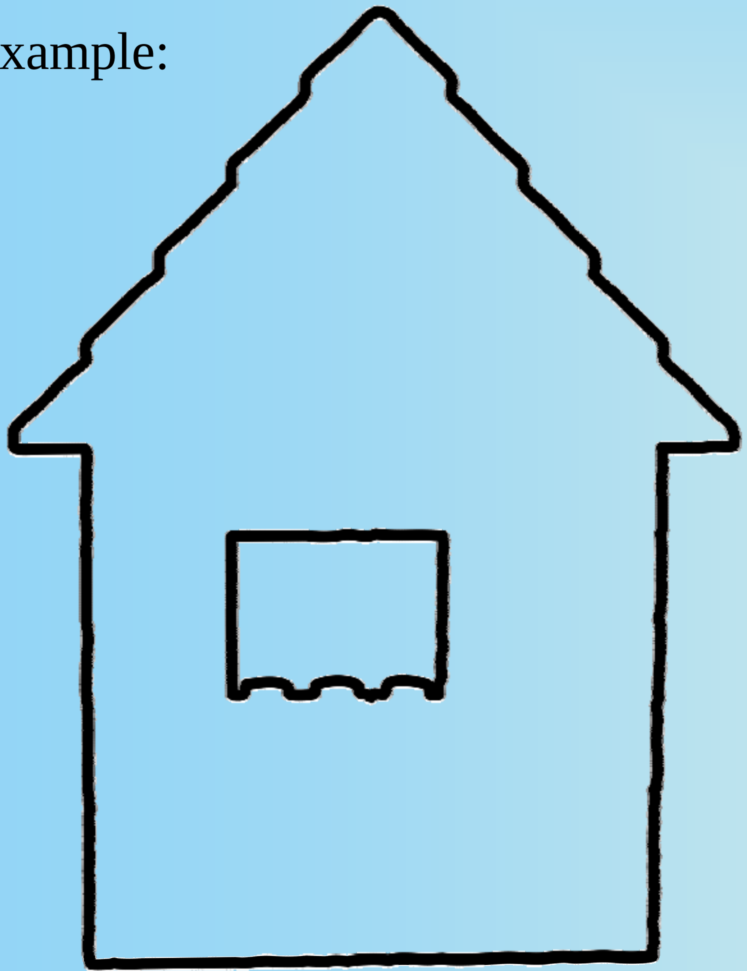
Due to this reason:

- The desired operation is performed as a sequence of simpler steps – **quantum gates**

Therefore seeking for such sequence, called **quantum logic circuit**, is inseparable part of the design of quantum devices

Similarity to „LEGO“

Example:



- **We know what we want to build**
- **We can use a few types of bricks**

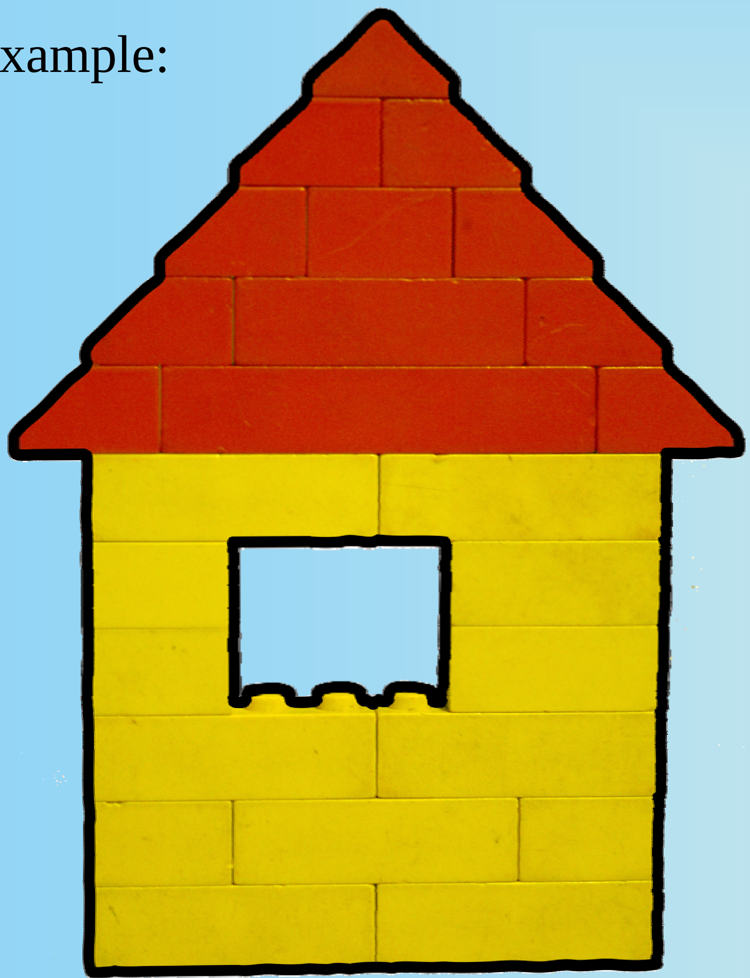
- A set of bricks can be universal
- Each thing can be build in many ways

Our task:

Find a way how to build the specified thing efficiently using only bricks from some set.

Similarity to „LEGO“

Example:



- We know what we want to build
- We can use a few types of bricks

- **A set of bricks can be universal**
- Each thing can be build in many ways

Our task:

Find a way how to build the specified thing efficiently using only bricks from some set.

Basic notions

Qubit / System of n-qubits

- base vectors of $\mathcal{H}$ (state space of qubit) $|0\rangle$ a $|1\rangle$
- state space of *n-qubit system* $\mathcal{H}_n = \bigotimes_{i=1}^{n} \mathcal{H}$
- ON base of $\mathcal{H}_n$ are for example vectors of the type: $|01\ldots1\rangle \equiv |0\rangle \otimes |1\rangle \otimes \ldots \otimes |1\rangle$

Operation on isolated system of qubits = unitary operator U

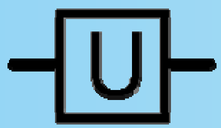
- we want to write this operator U as successive action of simpler unitary operations – quantum gates

$$U = U_m \ldots U_3 \cdot U_2 \cdot U_1$$

- **k-qubit quantum gate** = unitary operator, which acts nontrivially only on subsystem of k qubits

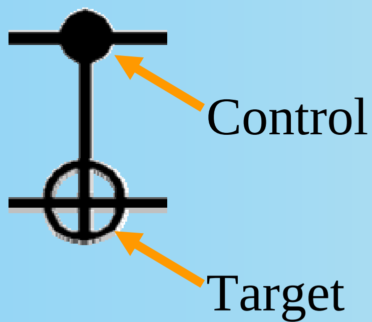
Basic quantum gates

- basic realizable operations



All one-qubit operations (rotations)

This gate is fully specified by U - unitary matrix 2x2



CNOT
Controlled NOT

Flips target qubit if control is in state $|1\rangle$

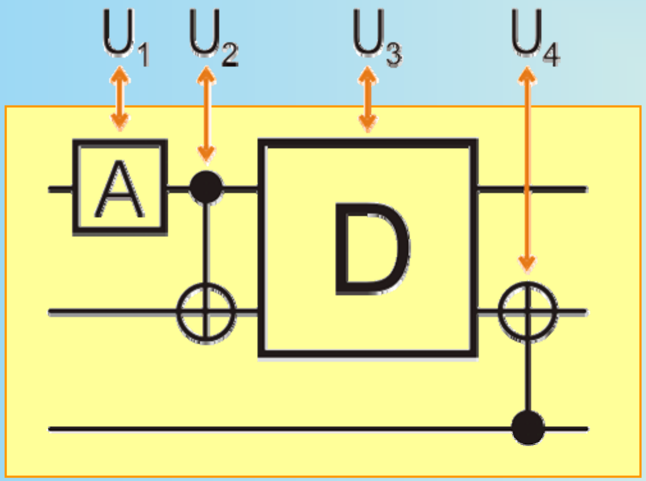
$$\begin{array}{l} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{array} \Leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Quantum Logic Circuit

= sequence of quantum gates

- are drawn using diagrams with following rules

Example:



$$U = U_4 \cdot U_3 \cdot U_2 \cdot U_1$$

- each horizontal line symbolizes one qubit
- quantum gate = symbol connecting qubits, on which the gate acts
- gates are carried out from left to right

Universality of basic gates

- A.Barenco et.al. proved that basic quantum gates form a universal set of quantum gates

- Each procedure, which for an arbitrary given unitary operator creates quantum logic circuit realizing it exactly, we denote as **universal decomposition**

- For dimensional reasons universal decomposition have to create QLC containing exponentially many CNOT gates (with respect to the number of qubits) in the worst case.

$$\geq \frac{1}{4}\left(4^n - 3n - 1\right)$$

A. Barenco, et.al., "**Elementary gates for quantum computation**", PRA AC5710(1995)

Decomposition of n-qubit unitary operators

- It's believed that interesting operators for quantum computation are realizable by polynomial number of basic gates (with respect to number of qubits)

Problem:

Present universal decompositions produce exponential number of gates also for those operators, which are known to be realizable with polynomial number of basic gates.

Possible solutions:

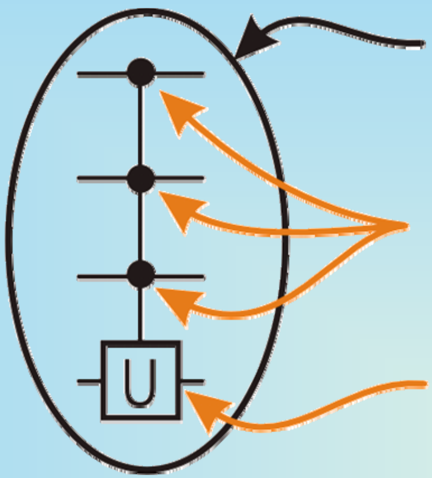
- guess the quantum logic circuit
- find a better universal decomposition
- optimize existing decomposition

Aim of my work

- Search for such improvements of Barenco’s procedure, which will decrease the number of CNOT gates in the resulting quantum logic circuit for the chosen operator

- create a computer program, which will perform Barenco’s procedure together with the proposed optimalization

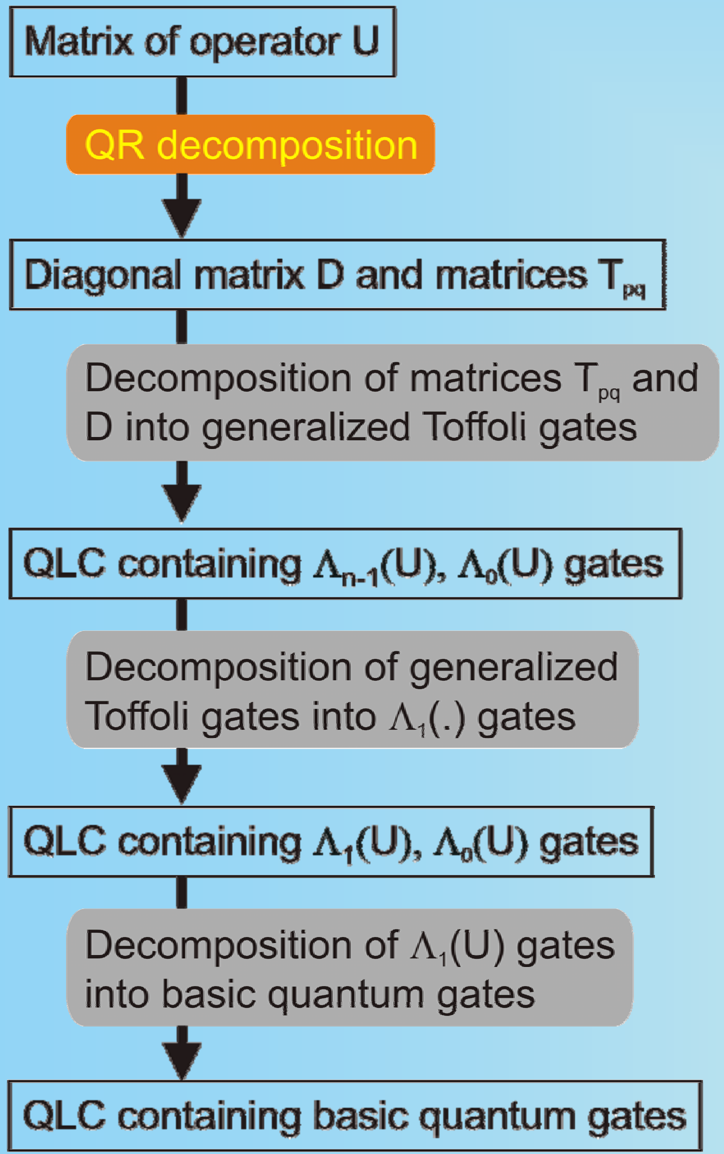
Generalized Toffoli gate $\Lambda_m(\mathrm{U})$



- m+1-qubit quantum gate
- It acts by 1-qubit operation U on the target qubit, if all control qubits are in the state $|1\rangle$

$$\Lambda_m(U)|x_1,\ldots,x_m,y\rangle = |x_1,\ldots,x_m\rangle \otimes U^{x_1\wedge\cdots\wedge x_m}|y\rangle$$

A. Barenco's procedure



- Each unitary matrix NxN ($N=2^n$) can be written as multiplication:

$$U = D^{-1} \cdot T_{2,1}^{-1} \cdot T_{3,1}^{-1} \cdot T_{3,2}^{-1} \cdots T_{2^n,2^n-2}^{-1} \cdot T_{2^n,2^n-1}^{-1}$$

- where:

$$T_{pq}(\phi,\omega) = \begin{pmatrix} 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & e^{i\phi}\sin\omega & & & & e^{i\phi}\cos\omega & & \\ & & & & 1 & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 1 & & & \\ & & & \cos\omega & & & & -\sin\omega & & \\ & & & & & & & & 1 & \\ & & & & & & & & & \ddots \\ & & & & & & & & & & 1 \end{pmatrix},$$

$$D = diag\left(e^{-i\alpha_1}, e^{-i\alpha_2}, \cdots, e^{-i\alpha_N}\right)$$

A. Barenco’s procedure

Matrix of operator U

↓ QR decomposition

Diagonal matrix D and matrices T_{pq}

↓ Decomposition of matrices T_{pq} and D into generalized Toffoli gates

QLC containing $\Lambda_{n-1}(U)$, $\Lambda_0(U)$ gates

↓ Decomposition of generalized Toffoli gates into $\Lambda_1(.)$ gates

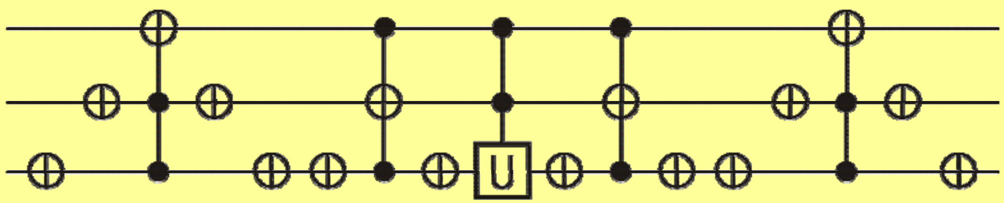
QLC containing $\Lambda_1(U)$, $\Lambda_0(U)$ gates

↓ Decomposition of $\Lambda_1(U)$ gates into basic quantum gates

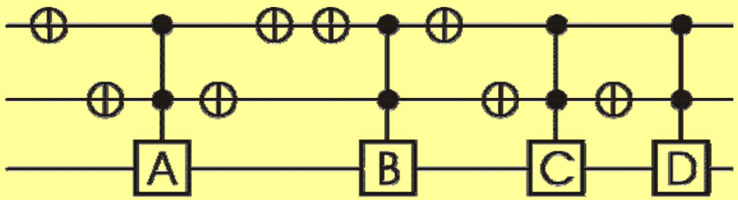
QLC containing basic quantum gates

Example for decomposition of 3-qubit operator:

$T_{8,1} \leftrightarrow$



$D \leftrightarrow$



A. Barenco's procedure

Matrix of operator U

↓ QR decomposition

Diagonal matrix D and matrices T_{pq}

↓ Decomposition of matrices T_{pq} and D into generalized Toffoli gates

QLC containing $\Lambda_{n-1}(U)$, $\Lambda_0(U)$ gates

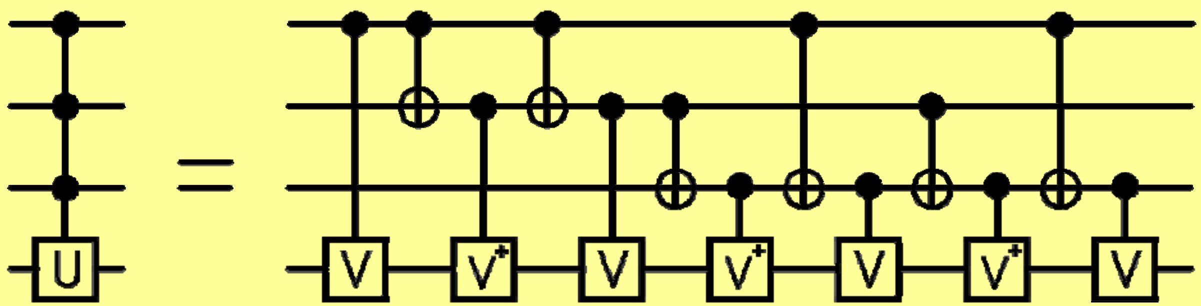
↓ **Decomposition of generalized Toffoli gates into $\Lambda_1(.)$ gates**

QLC containing $\Lambda_1(U)$, $\Lambda_0(U)$ gates

↓ Decomposition of $\Lambda_1(U)$ gates into basic quantum gates

QLC containing basic quantum gates

Example decomposition of $\Lambda_3(U)$ gate:



A. Barenco's procedure

Matrix of operator U

QR decomposition

Diagonal matrix D and matrices T_{pq}

Decomposition of matrices T_{pq} and D into generalized Toffoli gates

QLC containing $\Lambda_{n-1}(U)$, $\Lambda_0(U)$ gates

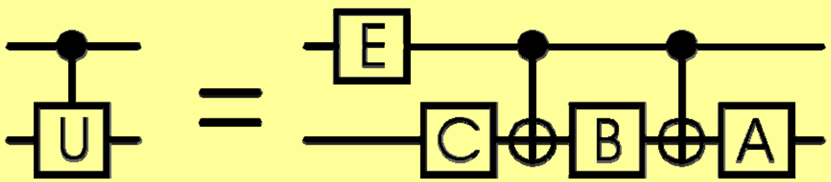
Decomposition of generalized Toffoli gates into $\Lambda_1(.)$ gates

QLC containing $\Lambda_1(U)$, $\Lambda_0(U)$ gates

Decomposition of $\Lambda_1(U)$ gates into basic quantum gates

QLC containing basic quantum gates

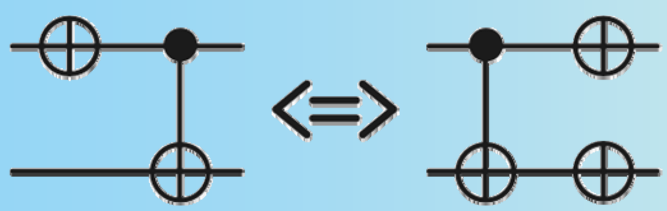
Example decomposition of $\Lambda_1(U)$ gate:

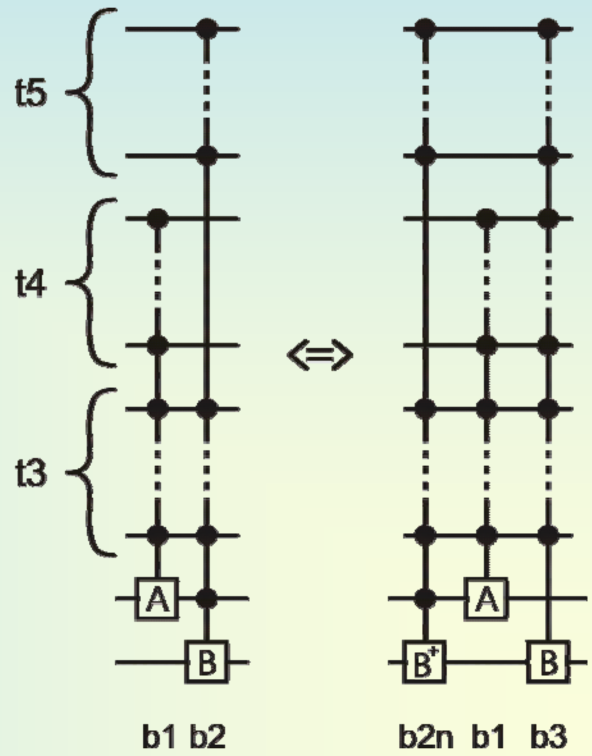


Properties of Generalized Toffoli gates

I have examined:

- commuting of pair of gates
- order exchange of two gates with modification of one gate
- conditions of merging two gates into one
- possible generalizations of identity:





Results - qualitatively

- I have created a computer program, which performs Barenco's decomposition of unitary operators (for $n<7$)
- Computer program contains also proposed optimization, which can be used for arbitrary n-qubit quantum logic circuit containing generalized Toffoli gates.
- For some 2-qubit unitary operators proposed optimization decrease the number of CNOT gates in the quantum circuit obtained by Barenco's decomposition to minimum

Results - quantitatively

• number of CNOT gates in different decompositions of typical unitary operators

Number of qubits	Barenco's decomposition	Optimized Barenco's decomposition	Decrease [%]	NQ decom-position	CS decom-position
2	20	10	50	3	4
3	576	379	35	21	26
4	8 000	6 278	21	105	118
5	91 520	76 208	16	465	494

$\approx n^3 4^n$

$\approx \frac{1}{2} 4^n$