

**Quantum Algorithms**  
**Lecture 11**  
**Bases for quantum circuits I**

**Zhejiang University**

# Introduction

# Arbitrary 1-qubit operator

$$U = \begin{pmatrix} \cos \frac{\theta}{2} & -e^{i\lambda} \sin \frac{\theta}{2} \\ e^{i\phi} \sin \frac{\theta}{2} & e^{i\lambda+i\phi} \cos \frac{\theta}{2} \end{pmatrix}$$

$$0 \leq \theta \leq \pi \text{ and } 0 \leq \phi, \lambda < 2\pi$$

# Choosing gate set

There are uncountably many unitary operators. So, either a complete basis must contain an infinite (uncountable) number of gates, or else we have to weaken the condition of exact realization of an operator by a circuit, changing it to a condition of approximate realization. We will examine both possibilities.

**Exact realization**

# Theorem

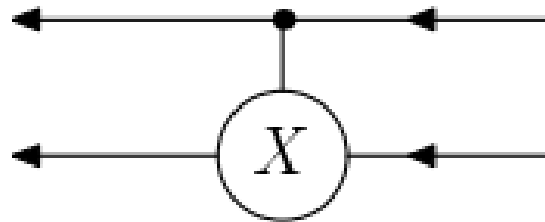
The basis consisting of all one-qubit and two-qubit unitary operators allows the realization of an arbitrary unitary operator.

# **Operators with quantum control**

# Control definition

For each operator  $U: B^{\otimes n} \rightarrow B^{\otimes n}$ , an operator  $\Lambda(U): B \otimes B^{\otimes n} \rightarrow B \otimes B^{\otimes n}$  ("controlled  $U$ ") is defined by the following relations:

$$\begin{aligned}\Lambda(U)|0\rangle \otimes |\xi\rangle &= |0\rangle \otimes |\xi\rangle \\ \Lambda(U)|1\rangle \otimes |\xi\rangle &= |1\rangle \otimes U|\xi\rangle\end{aligned}$$





# Control notation

The top line corresponds to the control qubit while the bottom line represents the other qubits. The direction of the arrows corresponds to the order in which operators act on an input vector.

For example, the first operator is  $\Lambda(Y^{-1})$ . In this book, authors draw arrows from right to left, which is consistent with the convention that  $AB|\xi\rangle$  means “take  $|\xi\rangle$ , apply  $B$ , then apply  $A$ ”.

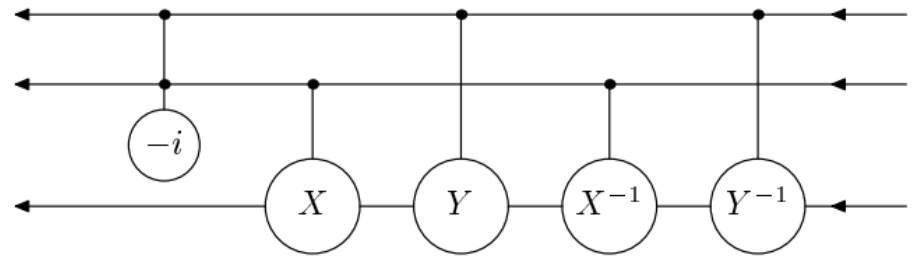


Fig. 8.1. Implementation of the Toffoli gate.

# Several controlling qubits

$$(8.2) \quad \Lambda^k(U)|x_1, \dots, x_k\rangle \otimes |\xi\rangle = \begin{cases} |x_1, \dots, x_k\rangle \otimes |\xi\rangle & \text{if } x_1 \cdots x_k = 0, \\ |x_1, \dots, x_k\rangle \otimes U|\xi\rangle & \text{if } x_1 \cdots x_k = 1. \end{cases}$$

**Example 8.1.** Let  $\sigma^x \stackrel{\text{def}}{=} \hat{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Then  $\Lambda(\sigma^x) = \widehat{\oplus}$ , and  $\Lambda^2(\sigma^x) = \widehat{\Lambda}_{\oplus}$  (the Toffoli gate).

# **The realization of the Toffoli gate**

# Realization

Now we construct the Toffoli gate using transformations on two qubits. To start, we find a pair of operators that satisfy the relation  $XYX^{-1}Y^{-1} = i\sigma^x$ . For example, the following pair will do:

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & -1 \\ 1 & i \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

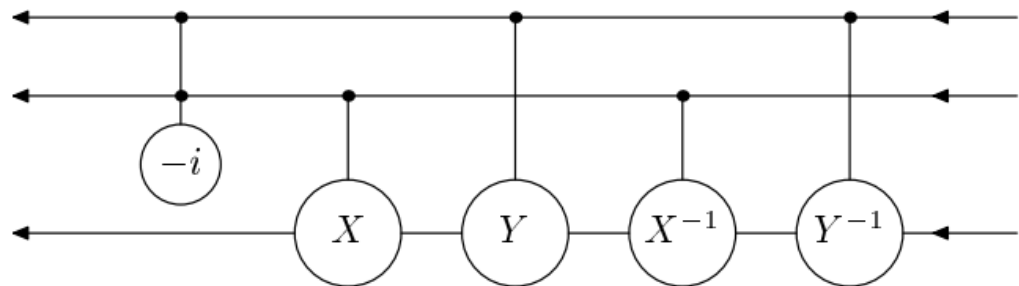


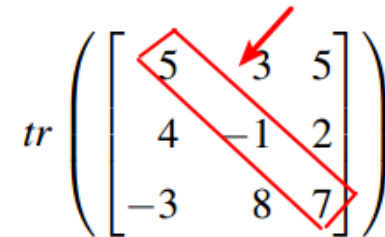
Fig. 8.1. Implementation of the Toffoli gate.

# Some remarks

The group  $U(2)$  is the group of all  $2 \times 2$  matrices (unitary) such that  $U^\dagger U = I$ .

$$U(2) = \left\{ U = \begin{pmatrix} \alpha & \beta \\ \gamma & \omega \end{pmatrix} \mid \alpha, \beta, \gamma, \omega \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\omega|^2 = 1, \alpha\bar{\gamma} + \beta\bar{\omega} = 0 \right\}$$

Trace:



The diagram shows a 3x3 matrix with elements 5, 3, 5 in the first row; 4, -1, 2 in the second row; and -3, 8, 7 in the third row. A red diagonal line connects the top-left element (5) to the bottom-right element (7). A red arrow points to the element 3 in the first row, second column.

$$\text{tr} \left( \begin{bmatrix} 5 & 3 & 5 \\ 4 & -1 & 2 \\ -3 & 8 & 7 \end{bmatrix} \right) = 5 - 1 + 7 = 11.$$

Group isomorphism is a function between two groups that sets up a one-to-one correspondence between the elements of the groups in a way that respects the given group operations.

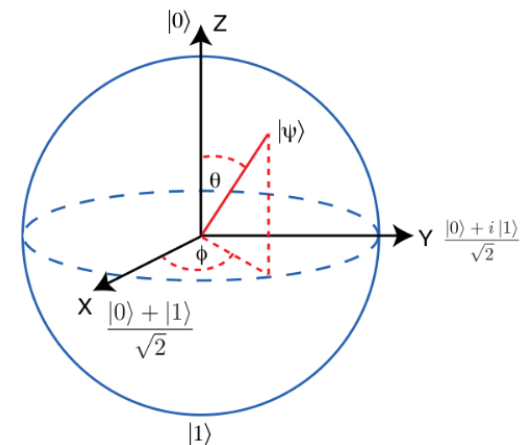
# The geometric meaning

The unitary group  $U(2)$  acts on three-dimensional Euclidean space. To define this action, we note that  $2 \times 2$  Hermitian matrices with zero trace form a three-dimensional Euclidean space: the inner product between  $A$  and  $B$  is given by  $\frac{1}{2}\text{Tr}(AB)$  and an orthonormal basis is formed by the Pauli matrices

$$\sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

# The geometric meaning

A unitary operator  $U \in U(2)$  acts on this space by this rule:  $U: E \rightarrow UEU^{-1}$ . It is possible to show that the action yields an isomorphism  $U(2)/U(1) \cong SO(3)$ , where  $U(1) = \{c \in \mathbb{C}: |c| = 1\}$  is the subgroup of phase shifts, and  $SO(3)$  is the group of rotations of three-dimensional space (i.e., the group of orthogonal transformations with determinant 1).



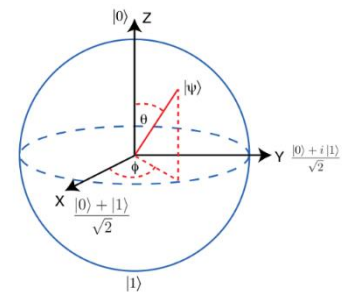
# Explanations

$U(2)$  – unitary  $2 \times 2$  matrices

$U(1)$  – complex numbers with absolute value 1 ( $e^{i\phi}$ ).

$U(2)/U(1)$  – quotient group, as result we have a group of unitary  $2 \times 2$  matrices with global phase being omitted (multiplier  $e^{i\phi}$ ).

$SO(3)$  – the rotation group, is the group of all rotations about the origin of 3-dimensional Euclidean space  $R^3$  under the operation of composition.



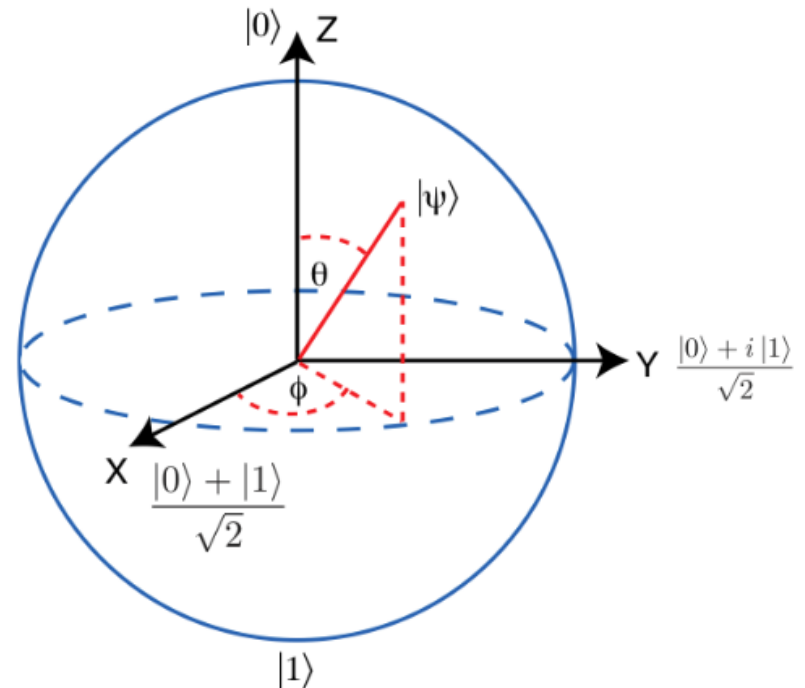


# Rotations

$$R_x(\varphi) := \begin{pmatrix} \cos \frac{\varphi}{2} & -i \sin \frac{\varphi}{2} \\ -i \sin \frac{\varphi}{2} & \cos \frac{\varphi}{2} \end{pmatrix}$$

$$R_y(\varphi) := \begin{pmatrix} \cos \frac{\varphi}{2} & -\sin \frac{\varphi}{2} \\ \sin \frac{\varphi}{2} & \cos \frac{\varphi}{2} \end{pmatrix}$$

$$R_z(\varphi) := \begin{pmatrix} e^{-i \frac{\varphi}{2}} & \\ & e^{i \frac{\varphi}{2}} \end{pmatrix}$$

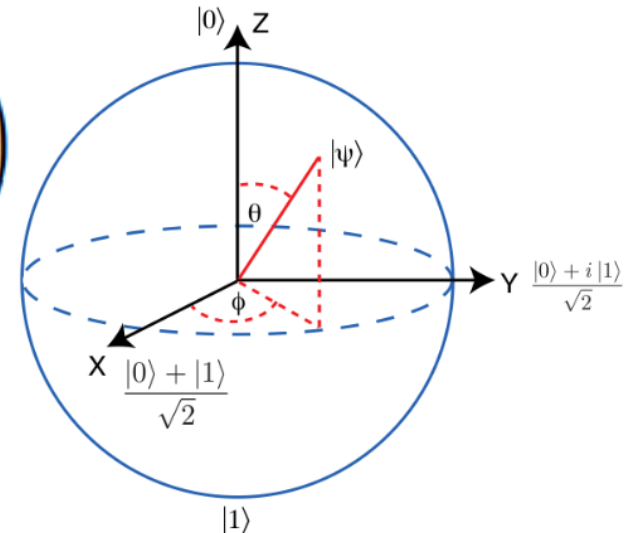


# Geometric meaning

$\sigma^x$  corresponds to a rotation about the x axis by  $180^\circ$ ,  $X$  to a rotation about the vector  $(0, 1, 1)$  by  $180^\circ$ , and  $Y$  to a rotation about the y axis by  $180^\circ$ .

$$\sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & -1 \\ 1 & i \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$



# Toffoli realization

Circuit realizes the Toffoli gate by using the operators  $\Lambda(X)$ ,  $\Lambda(Y)$  and  $\Lambda^2(-i)$ . The last of these is a phase shift (multiplication by  $-i$ ) controlled by two bits.

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & -1 \\ 1 & i \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

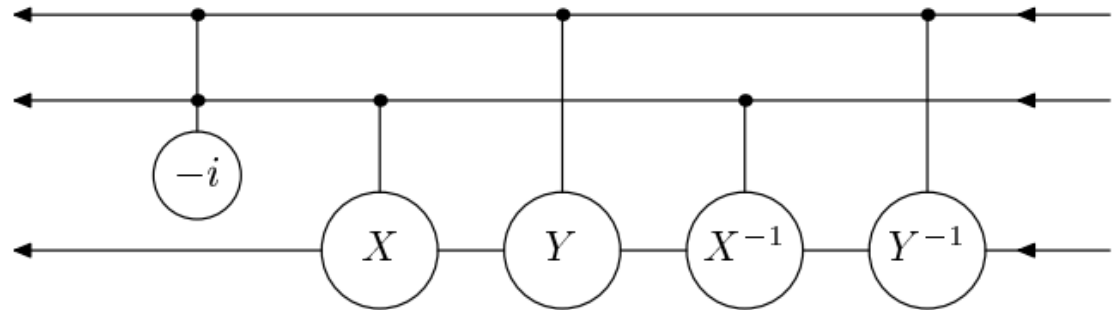


Fig. 8.1. Implementation of the Toffoli gate.

# Testing

Suppose the input vector is  $|a, b, c\rangle = |a\rangle \otimes |b\rangle \otimes |c\rangle$ , where  $a, b, c \in B$ . If  $a = b = 1$ , then the operator  $-iXYX^{-1}Y^{-1} = \sigma^x$  is applied to  $|c\rangle$ , which changes  $|0\rangle$  to  $|1\rangle$  and vice versa. However, if at least one of the controlling bits is 0, then  $|c\rangle$  is multiplied by the identity operator. This is exactly how the Toffoli gate acts on basis vectors. This action extends to the whole space  $B^{\otimes 3}$  by linearity.

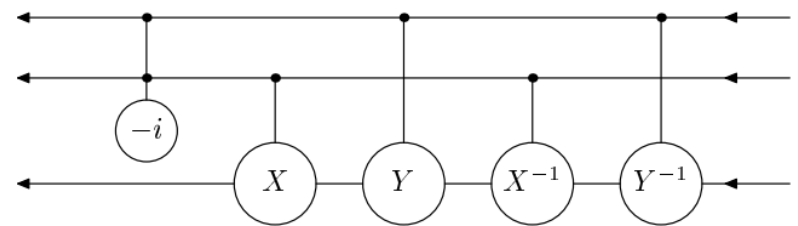


Fig. 8.1. Implementation of the Toffoli gate.

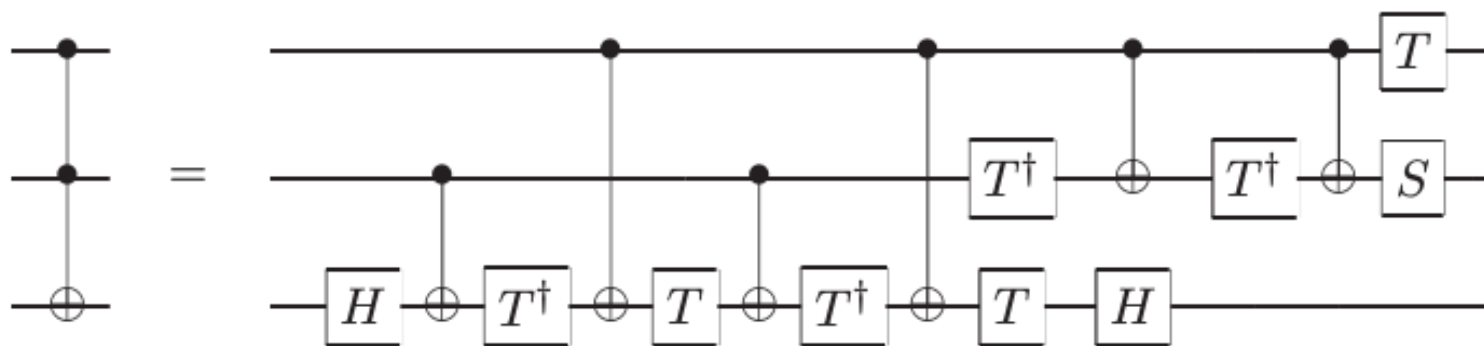
# Toffoli realization

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

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

$$Toffoli = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$



**The realization of  $\Lambda^k(U)$  for  
 $U \in U(B)$**

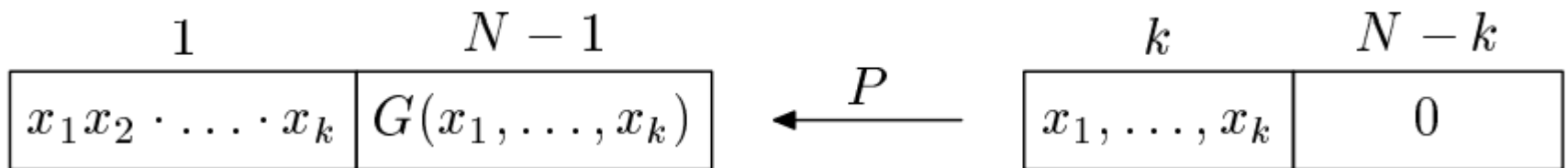
# Multiple control qubits

Let  $U$  be a unitary operator acting on one qubit. We will show how to realize the operator  $\Lambda^k(U)$  for arbitrary  $k$  by acting only on pairs of qubits. Our first solution uses ancillas. We actually construct an operator  $W$  which acts on the space of  $N + 1$  qubits  $B^{\otimes(N+1)}$  and satisfies the condition

$$W(|\eta\rangle \otimes |0^{N-k}\rangle) = \Lambda(U)|\eta\rangle \otimes |0^{N-k}\rangle$$

# Computing product

There exists a reversible circuit  $P$  of size  $O(k)$  and depth  $O(\log k)$  that computes the product of  $k$  input bits  $x_1 \cdots x_k$  (the result being a single bit), and also produces some garbage  $G(x_1, \dots, x_k)$  ( $N - 1$  bits).





# Multiple control implementation

The circuit  $P$  is applied first, followed by the reverse circuit  $P^{-1}$ , so that all  $N$  bits return to their initial state. In the meantime, the first bit (the top line) takes the value  $x_1 \cdot \dots \cdot x_k$ . It is used as the control qubit for  $\Lambda(U)$ , whereas qubit  $N + 1$  is the target. The circuit in the figure can also be described by the equation  $W = P^{-1}\Lambda(U)P$  or, more explicitly,

$$W[\underbrace{1, \dots, k}_{\Lambda(U)}, \underbrace{N+1, k+1, \dots, N}_{\text{ancillas}}] = P^{-1}[1, \dots, N] \Lambda(U)[1, N+1] P[1, \dots, N]$$

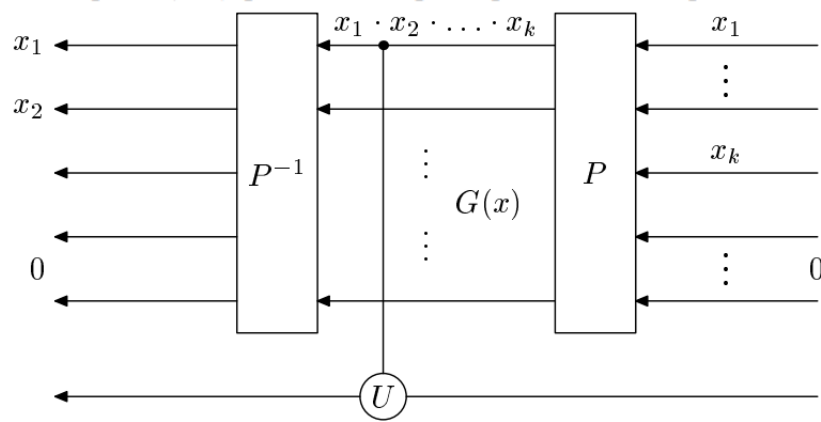


Fig. 8.3. Implementation of the operator  $\Lambda^k(U)$  using ancillas.

# Avoiding ancillas

The use of ancillas can be avoided at the cost of an increase in the circuit size. Let us consider the operator  $\Lambda^k(i\sigma^x)$  first. A circuit  $C_k$  for the realization of this operator can be constructed recursively: it consists of two copies of the circuit  $C_{\lfloor k/2 \rfloor}$ , two copies of the circuit  $C_{\lfloor k/2 \rfloor}$ , and a constant number  $c$  of one-qubit gates. Therefore, we get a recurrence relation for the circuit size,  $L_k = 2L_{\lfloor k/2 \rfloor} + 2L_{\lfloor k/2 \rfloor} + c$ , so that  $L_k = O(k^2)$ .

$$\Lambda^k(\sigma^x)$$

$$= \Lambda^{k/2}(Y) + \Lambda^{k/2}(Y^{-1}) + \Lambda^{k/2}(X) + \Lambda^{k/2}(X^{-1})$$

# Avoiding ancillas

We again use the operators  $X$  and  $Y$  satisfying  $XYX^{-1}Y^{-1} = i\sigma^x$ . Now we apply them with multiple control qubits:  $Y$  is controlled by the qubits  $1, \dots, k/2$ , whereas  $X$  is controlled by the qubits  $k/2 + 1, \dots, k$ .

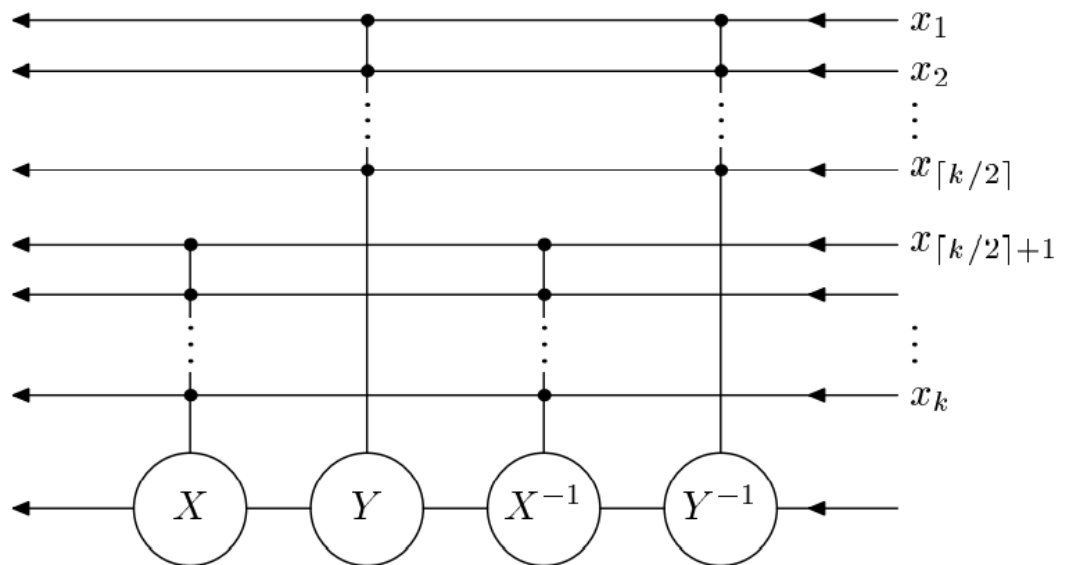


Fig. 8.4. Implementation of the operator  $\Lambda^k(i\sigma^x)$  without ancillas.

# Avoiding ancillas

It remains to notice that  $X$  and  $Y$  are conjugate to  $i\sigma^x$ , i.e.,  $X = V(i\sigma^x)V^{-1}$ ,  $Y = W(i\sigma^x)W^{-1}$  for some unitary  $V$  and  $W$ . Hence  $\Lambda^b(X)$  and  $\Lambda^a(Y)$  (where  $a = \lceil k/2 \rceil$ ,  $b = \lfloor k/2 \rfloor$ ) can be obtained if we conjugate  $\Lambda^b(i\sigma^x)$  and  $\Lambda^a(i\sigma^x)$  by  $V$  and  $W$  (resp.) applied on the last qubit.

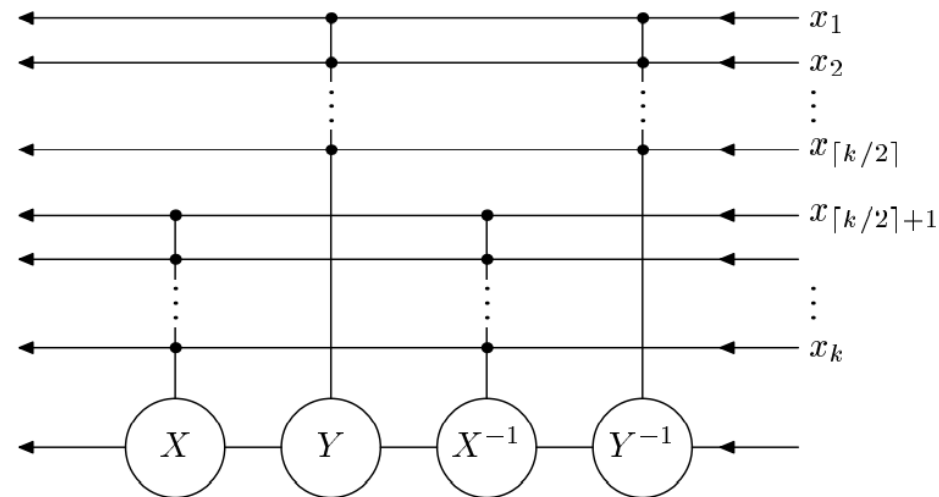


Fig. 8.4. Implementation of the operator  $\Lambda^k(i\sigma^x)$  without ancilla

# Special unitary group

Special unitary group of degree  $n$ , denoted  $SU(n)$ , is the Lie group of  $n \times n$  unitary matrices with determinant 1.

The more general unitary matrices may have complex determinants with absolute value 1, rather than real 1 in the special case.

The group operation is matrix multiplication.

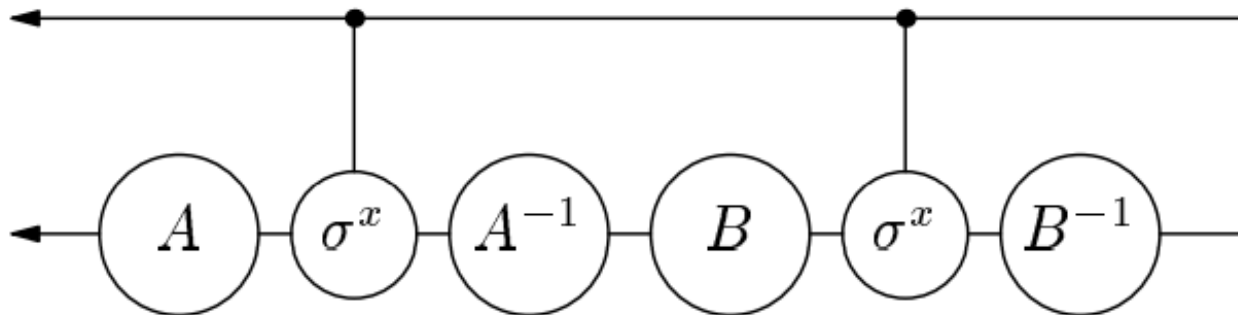
$$SU(2) = \left\{ Z = \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}$$

# **$U(2)$ vs $SU(2)$**

For any  $U \in U(n)$ , there exists  $e^{ix_o}$ ,  $x_o \in \mathbb{R}$ , such that  $e^{ix_o}U \in SU(n)$ .

# Arbitrary operator $SU(2)$

The operator  $\Lambda^k(Z)$  for an arbitrary  $Z \in SU(2)$  can be realized by two applications of  $\Lambda^k(\sigma^x)$  and four applications of one-qubit gates. Note that one copy of  $\Lambda^k(\sigma^x)$  can be replaced by  $\Lambda^k(i\sigma^x)$ , and the other by  $\Lambda^k(-i\sigma^x)$ .



# Arbitrary operator $U(2)$

Consider now the general case,  $\Lambda^k(U)$ , where  $U \in U(2)$ . Let  $U = U_0 = e^{i\phi_1} Z_0$ , where  $Z_0 \in SU(2)$ . Then  $\Lambda^k(e^{i\phi_1}) = \Lambda^{k-1}(U_1)$ , where  $U_1 = \Lambda(e^{i\phi_1}) \in U(2)$ . Thus we have

$$\Lambda^k(U)[1, \dots, k, k+1] = \Lambda^{k-1}(U_1)[1, \dots, k] \Lambda^k(Z_0)[1, \dots, k, k+1].$$

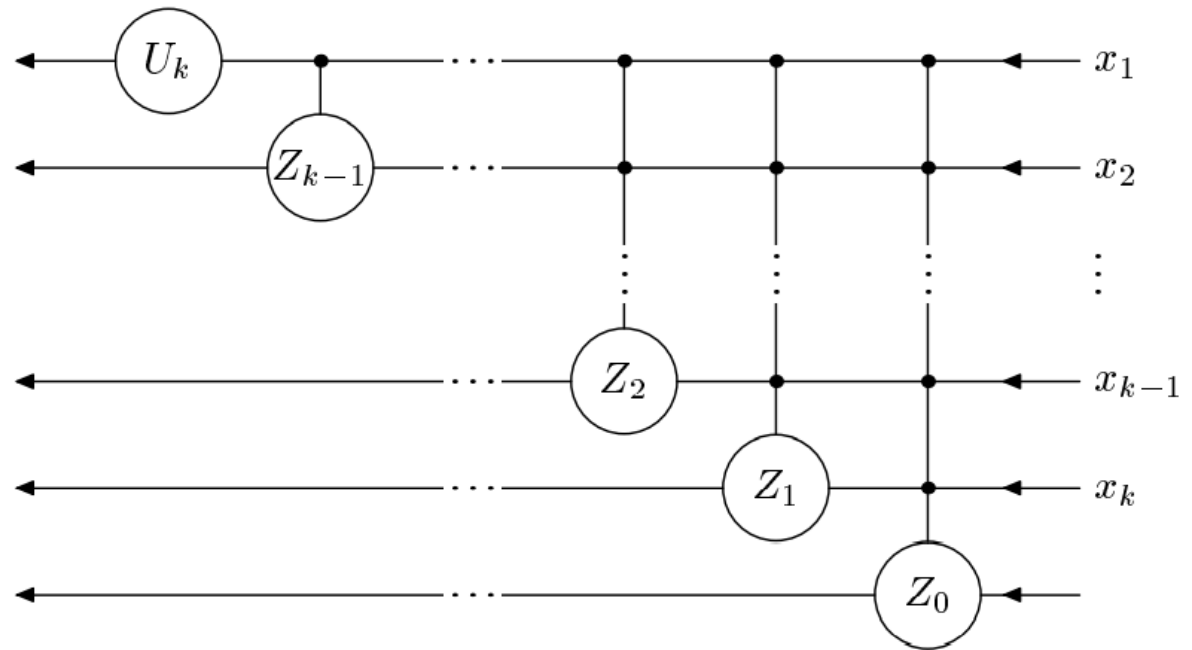


# Arbitrary operator $U(2)$

We proceed by induction, obtaining the equation

$$\Lambda^k(U)[1, \dots, k, k+1] = U_k[1] \Lambda^1(Z_{k-1})[1, 2] \cdots \Lambda^k(Z_0)[1, \dots, k, k+1]$$

The size of the resulting circuit is  $O(n^3)$ .



**Fig. 8.5.** Ancilla-free realization of  $\Lambda^k(U)$ ,  $U \in \mathbf{U}(2)$ .

# Arbitrary operator $U(2)$

The operator  $\Lambda^k(U)$  can be realized by a circuit of size  $O(k^2)$  over the basis of all two-qubit gates without use of ancillas.

# **The realization of an arbitrary operator**

# Currently proven

We continue the proof of Theorem. The action of  $\Lambda^k(U)$  may be described as follows: the operator  $U$  acts on the subspace generated by the vectors  $|1, \dots, 1, 0\rangle$  and  $|1, \dots, 1, 1\rangle$ , and the identity operator acts on the orthogonal complement of this subspace.

# Next task

Our next task is to realize a similar operator in which a nontrivial action is carried out on the subspace spanned by an arbitrary pair of basis vectors. Suppose we want to realize an arbitrary operator on the subspace spanned by  $|x\rangle$  and  $|y\rangle$ , where  $x = (x_1, \dots, x_n)$ ,  $y = (y_1, \dots, y_n)$ ,  $x_j, y_j \in B$ .

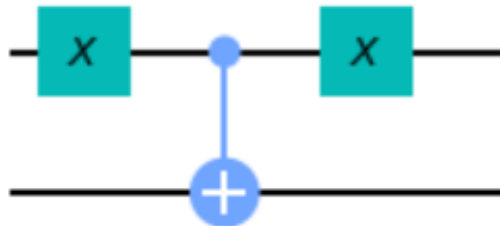
# Permutation function

Let  $f$  be a permutation such that  $f(x) = (1, \dots, 1, 0)$ ,  $f(y) = (1, \dots, 1, 1)$ . We may assume that  $f$  is linear, i.e.,  $f: x \rightarrow Ax + b$ , where  $A$  is an invertible matrix, and  $b$  is a vector over the two-element field  $F_2$ . Such permutations can be realized by reversible circuits over the basis  $\{\neg, \otimes\}$  without ancillas. Then the operator we need is represented in the form  $\hat{f}^{-1} \Lambda^{n-1} (U) \hat{f}$ . (Recall that  $\hat{f}$  is the operator corresponding to the permutation  $f$ .)

# Changing control states

We can control from, e.g., state  $|010\rangle$  instead of  $|111\rangle$ .

$$C_0C_0NOT = \begin{pmatrix} 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix}, \quad C_0C_1NOT = \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix}, \quad \text{and } C_1C_0NOT = \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix}.$$



# Complexity

Therefore, we can act arbitrarily on pairs of basis vectors. Since we only used circuits of size  $\text{poly}(n)$ , the constructed actions are realized efficiently. The final part in the proof of Theorem is not efficient. Now we forget about qubits (i.e., the tensor product structure of our space), so we just have a Hilbert space of dimension  $M = 2^n$ . We want to represent an arbitrary unitary operator  $U$  by the actions on pairs of basis vectors. This will be polynomial in  $M$ , hence exponential in  $n$ .



# Lemma

An arbitrary unitary operator  $U$  on the space  $\mathcal{C}^M$  can be represented as a product of  $M(M - 1)/2$  matrices of the form

$$\begin{pmatrix} 1 & 0 & \dots\dots\dots & & & & \\ \vdots & \ddots & 0 & \dots\dots\dots & & & \\ 0 & \dots & 1 & 0 & \dots\dots\dots & & \\ 0 & \dots\dots\dots & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & 0 & \dots\dots\dots & & \\ 0 & \dots\dots\dots & & 1 & 0 & 0 & \\ \dots\dots\dots & & & & \ddots & 0 & \\ 0 & \dots\dots\dots & & & & & 1 \end{pmatrix}, \text{ where } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{U}(2)$$

# Proof of Lemma

First we note that for any numbers  $c_1, c_2$  there exists a  $2 \times 2$  unitary matrix  $V$  such that

$$V \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|c_1|^2 + |c_2|^2} \\ 0 \end{pmatrix}$$

# Proof of Lemma

Consequently, for a unit vector  $|\xi\rangle \in \mathcal{C}^M$  there exists a sequence of unitary operators  $V^{(1)}, \dots, V^{(M-1)}$  such that  $V^{(1)} \dots V^{(M-1)} |\xi\rangle = |1\rangle$ , where  $V^{(s)}$  acts on the subspace  $\mathcal{C}(|s\rangle, |s+1\rangle)$  (as the matrix) and leaves the remaining basis vectors unchanged.

$$\begin{pmatrix} 1 & 0 & \dots\dots\dots \\ \vdots & \ddots & 0 & \dots\dots\dots \\ 0 & \dots & 1 & 0 & \dots\dots\dots \\ 0 & \dots\dots\dots & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & 0 & \dots\dots\dots \\ 0 & \dots\dots\dots & \dots\dots\dots & 1 & 0 & 0 \\ \dots\dots\dots & \dots\dots\dots & \dots\dots\dots & \ddots & 0 \\ 0 & \dots\dots\dots & \dots\dots\dots & \dots\dots\dots & 1 \end{pmatrix}, \text{ where } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{U}(2)$$

# Proof of Lemma

Now let an  $M \times M$  unitary matrix  $U$  be given. Multiplying  $U^{-1}$  on the left by suitable matrices  $U^{(1,1)}, \dots, U^{(1,M-1)}$ , we can transform the first column into the vector  $|1\rangle$ . Since the columns remain orthogonal, the first row becomes  $\langle 1|$ .

# Proof of Lemma

Acting in the same way on the remaining columns, we obtain a set of matrices  $U^{(j,s)}$ ,  $1 \leq j \leq s \leq M-1$ , (where  $U^{(j,s)}$  acts on  $|s\rangle$  and  $|s+1\rangle$ ) satisfying the condition

$$U^{(M-1,M-1)}(U^{(M-2,M-2)}U^{(M-2,M-1)}) \dots (U^{(1,1)} \dots U^{(1,M-1)})U^{-1} = I$$

# Proof of Lemma

This proof is constructive, i.e., it provides an algorithm for finding the matrices  $U^{(j,s)}$ . The running time of this algorithm depends on  $M$  and another parameter  $\delta$ , the precision of arithmetic operations with real numbers.

Specifically, the algorithm complexity is  $O(M^3) \cdot \text{poly}(\log(1/\delta))$ .

# Complete basis

Any operator  $U \in U(B)$  can be realized (without ancillas) by a constant size circuit over the basis  $\{\Lambda(e^{i\phi}): \phi \in R\} \cup \{H\}$ .

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

# Complete basis

Any rotation in three-dimensional space can be represented as a composition of three rotations: through an angle  $\alpha$  about the z axis, then through an angle  $\beta$  about the x axis, and then through an angle  $\gamma$  about the z axis. Therefore any operator acting on one qubit can be represented in the form

$$U = e^{i\varphi} e^{i(\gamma/2)\sigma^z} e^{i(\beta/2)\sigma^x} e^{i(\alpha/2)\sigma^z}$$



# Complete basis

$$U = e^{i\varphi} e^{i(\gamma/2)\sigma^z} e^{i(\beta/2)\sigma^x} e^{i(\alpha/2)\sigma^z}$$

Each of the operators on the right-hand side of the equation can be expressed in terms of  $H$  and a controlled phase shift:

$$\begin{aligned} e^{i\varphi} &= \Lambda(e^{i\varphi})\sigma^x\Lambda(e^{i\varphi})\sigma^x, & e^{i\varphi\sigma^z} &= \Lambda(e^{-i\varphi})\sigma^x\Lambda(e^{i\varphi})\sigma^x, \\ \sigma^x &= H\Lambda(e^{i\pi})H, & e^{i\varphi\sigma^x} &= He^{i\varphi\sigma^z}H. \end{aligned}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \Lambda(e^{i\varphi}) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

# Complete basis

Any operator of the form  $\Lambda(U)$ ,  $U \in U(B)$  can be realized (without ancillas) by a constant size circuit over the basis of one-qubit gates and the gate  $\Lambda(\sigma^x)$ .

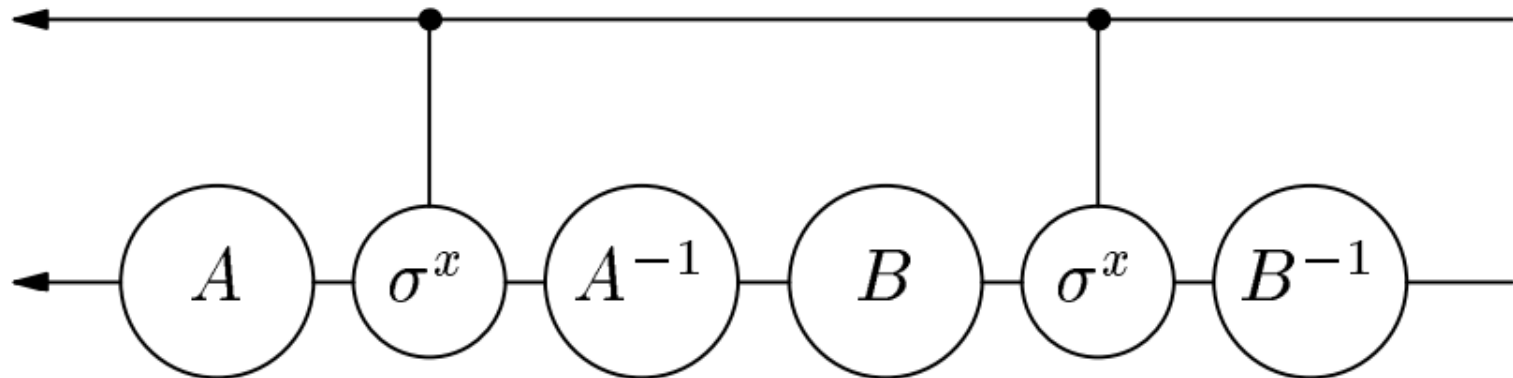
Therefore, this basis allows the realization of an arbitrary unitary operator.

# Complete basis

Let  $U = e^{i\phi}Z$ , where  $Z \in SU(2)$ . Then  $\Lambda(U) = \Lambda(e^{i\phi})\Lambda(Z)$ . The operator  $\Lambda(e^{i\phi})$  acts only on the control qubit, so it remains to realize  $\Lambda(Z)$ . Any operator  $Z \in SU(2)$  can be represented in the form

$$Z = A\sigma^x A^{-1}B\sigma^x B^{-1}, A, B \in SU(2).$$

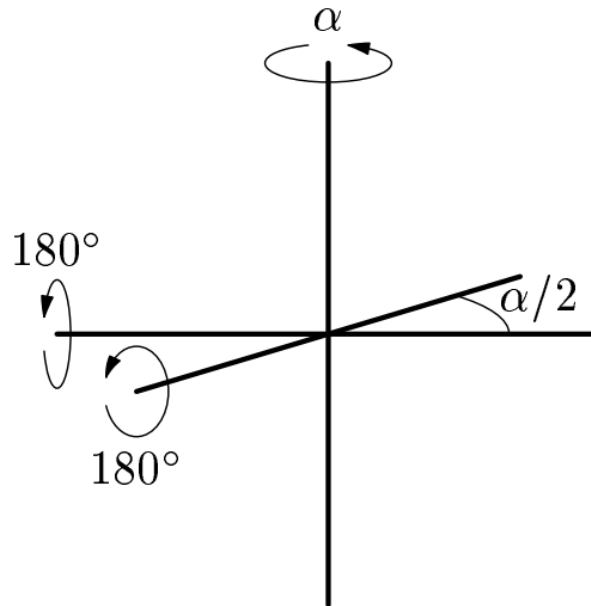
Therefore,  $\Lambda(Z)$  is realized by the circuit



# Complete basis

$$Z = A\sigma^x A^{-1} B\sigma^x B^{-1}, A, B \in SU(2).$$

Geometrically, equation is equivalent to the assertion that any rotation of the three-dimensional space is the composition of two rotations through  $180^\circ$ . The proof of this assertion is shown here:



**Thank you for your  
attention!**