Quantum Algorithms
Lecture 30
Classical and quantum codes II

Zhejiang University

Shor’s code

Repetition code

The repetition code of type (3,1):

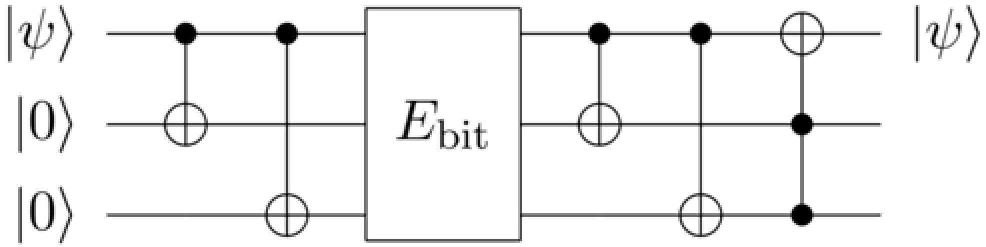
$$M_3 = \{(0,0,0), (1,1,1)\} \subseteq B^3$$

Such a code will correct a single error.

An obvious generalization of this example leads to classical codes M_n of type $(n, 1)$ which correct $k = \lfloor (n-1)/2 \rfloor$ errors.

As we have observed, repetition code helped with bit-flip errors, but did not with phase-flip errors.

Repetition code - quantum

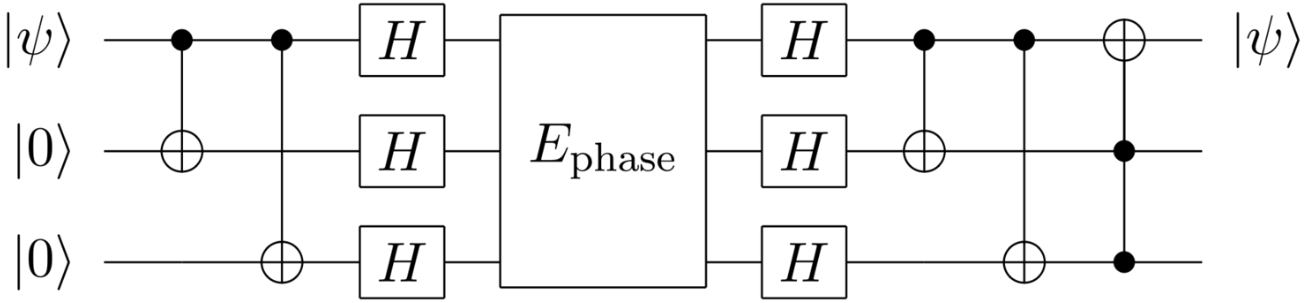


Encoding:

$$|0\rangle \to |000\rangle$$
$$|1\rangle \to |111\rangle$$

If first bit flipped, last CCNOT will flip the value: if $|0\rangle$ flipped to $|1\rangle$, both CNOTs will change values of last 2 qubits to $|1\rangle$, it will affect last CCNOT; if $|1\rangle$ flipped to $|0\rangle$, CNOTs will not change values of last 2 qubits ($|1\rangle$), so last CCNOT will work.

Phase-flip case



Encoding:

$$|0\rangle \rightarrow |+++\rangle = {}^{1}\!/_{\sqrt{2}}\,(|000\rangle + |111\rangle)$$

$$|1\rangle \rightarrow |---\rangle = {}^{1}\!/_{\sqrt{2}}\,(|000\rangle - |111\rangle)$$

Analysis is very similar, just in different basis.

How to combine

The error channel may induce either a bit flip, a sign flip (i.e., a phase flip), or both. It is possible to correct for both types of errors using one code, and the Shor code does just that. In fact, the Shor code corrects arbitrary single-qubit errors.

How to combine

Let E be a quantum channel that can arbitrarily corrupt a single qubit. The 1st, 4th and 7th qubits are for the sign flip code, while the three group of qubits (1,2,3), (4,5,6), and (7,8,9) are designed for the bit flip code. With the Shor code, a qubit state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ will be transformed into the product of 9 qubits $|\psi'\rangle = \alpha_0|0_S\rangle + \alpha_1|1_S\rangle$:

$$|0_{\rm S}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

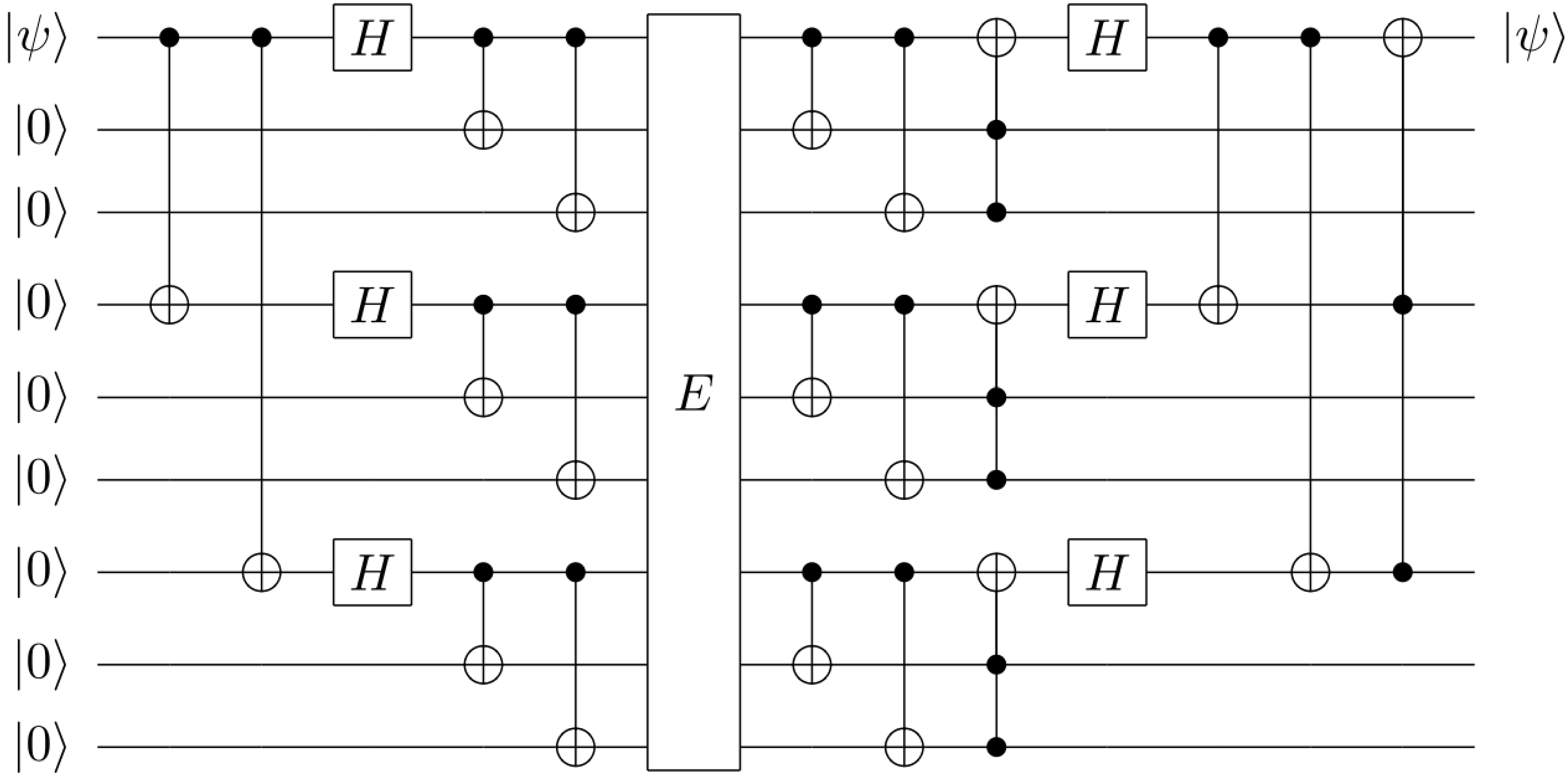
$$|1_{\rm S}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

How to combine

If a bit flip error happens to a qubit, the syndrome analysis will be performed on each set of states (1,2,3), (4,5,6), and (7,8,9), then correct the error.

If the three bit flip group (1,2,3), (4,5,6), and (7,8,9) are considered as three inputs, then the Shor code circuit can be reduced as a sign flip code. This means that the Shor code can also repair sign flip error for a single qubit.

Shor’s code


$|\psi\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
H
H
H
E
H
H
H
$|\psi\rangle$

How to combine

The Shor code also can correct for any arbitrary errors (both bit flip and sign flip) to a single qubit. If an error is modeled by a unitary transformation U, which will act on a qubit $|\psi\rangle$, then U can be described in the form

$$U = c_0 I + c_1 \sigma^x + c_2 \sigma^y + c_3 \sigma^z$$

where c_0, c_1, c_2, and c_3 are complex constants

$$\sigma_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, \qquad \sigma_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma^z,$$

$$\sigma_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma^x, \qquad \sigma_{11} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \sigma^y.$$

Summary

If U is equal to I, then no error occurs. If $U = \sigma^x$, a bit flip error occurs. If $U = \sigma^z$, a sign flip error occurs. If $U = i\sigma^y$ then both a bit flip error and a sign flip error occur. Due to linearity, it follows that the Shor code can correct arbitrary 1-qubit errors.

Shor’s code series

Series of quantum codes with arbitrary large distance. The r-th member of this series encodes one logical qubit into r^2 physical qubits; the distance of this code equals r.

This code allows to correct ${}^{r-1}/_{2}$ errors.

Original Shor’s code has 9 qubits, code distance is 3, and it can correct 1-qubit error.

Try to think how Shor’s code with 25 qubits can look like.

The Pauli operators and symplectic transformations

Introduction

The construction of the Shor code uses the symmetry between σ^x and σ^z.

Pauli operators are remarkable in that they are unitary and Hermitian at the same time.

Pauli matrices are conveniently indexed by elements of the group $G = (\mathbb{Z}_2)^2$. General σ-operators are indexed by $\gamma = (\alpha 1, \beta 1, \ldots, \alpha n, \beta n) \in G^n$. The σ-operators form a basis in $L(B^{\otimes n})$.

$$\sigma(f) = \sigma(\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_n, \beta_n) \overset{\text{def}}{=} \sigma_{\alpha_1,\beta_1} \otimes \sigma_{\alpha_2,\beta_2} \otimes \cdots \otimes \sigma_{\alpha_n,\beta_n}$$

Two indexes for each qubit – first whether σ^x is applied, and second – σ^z.

$$\sigma_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, \qquad \sigma_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma^z,$$

$$\sigma_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma^x, \qquad \sigma_{11} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \sigma^y.$$

G^n-graded algebra

Linear space can be expressed as linear combination of Pauli operators – as Pauli matrices with complex number multipliers.

$$\mathbf{L}(\mathcal{B}^{\otimes n}) = \bigoplus_{\gamma \in G^n} \mathbb{C}\big(\sigma(\gamma)\big)$$

Operator †: $X \to X^\dagger$ preserves the grading.

The direct sum decomposition is usually referred to as gradation or **grading**.

The circle operator here is direct sum.

Rules and formulas

$$\sigma(\gamma_1)\sigma(\gamma_2) = (-1)^{\omega(\gamma_1,\gamma_2)}\sigma(\gamma_2)\sigma(\gamma_1),$$

$$\omega(\alpha_1,\beta_1,\ldots,\alpha_n,\beta_n;\ \alpha'_1,\beta'_1,\ldots,\alpha'_n,\beta'_n) = \sum_{j=1}^{n}(\alpha_j\beta'_j - \alpha'_j\beta_j) \bmod 2.$$

$$\sigma(\gamma_1)\sigma(\gamma_2) = i^{\widetilde{\omega}(\gamma_1,\gamma_2)}\sigma(\gamma_1+\gamma_2), \qquad \widetilde{\omega} : G^n \times G^n \to \mathbb{Z}_4$$

$$\omega(\gamma_1,\gamma_2) = \widetilde{\omega}(\gamma_1,\gamma_2) \bmod 2$$

$$\sigma_{\alpha\beta} = i^{\alpha\beta}\sigma_{\alpha 0}\sigma_{0\beta}$$

$$\widetilde{\omega}(\alpha,\beta;\alpha',\beta') = \alpha\beta + \alpha'\beta' - (\alpha\oplus\alpha')(\beta\oplus\beta') + 2\alpha'\beta \mod 4$$

$$\widetilde{\omega}(\alpha,\beta;\alpha',\beta') = \alpha^2\beta^2 + (\alpha')^2(\beta')^2 - (\alpha+\alpha')^2(\beta+\beta')^2 + 2\alpha'\beta$$

$$\widetilde{\omega}(\gamma,\gamma') = \tau(\gamma) + \tau(\gamma') - \tau(\gamma+\gamma') + 2\varkappa(\gamma,\gamma'),$$

$$\tau(\alpha_1,\beta_1,\ldots,\alpha_n,\beta_n) = \textstyle\sum_{j=1}^{n}\alpha_j^2\beta_j^2 \ \in \mathbb{Z}_4,$$

$$\varkappa(\alpha_1,\beta_1,\ldots,\alpha_n,\beta_n;\ \alpha'_1,\beta'_1,\ldots,\alpha'_n,\beta'_n) = \textstyle\sum_{j=1}^{n}\alpha'_j\beta_j \ \in \mathbb{Z}_2$$

Extended symplectic group

Is denoted by $ESp_2(n)$.

The operators in this group will be called symplectic.

$$U\sigma(\gamma)U^\dagger = (-1)^{v(\gamma)}\sigma(u(\gamma)), \quad u : G^n \to G^n, \quad v : G^n \to \mathbb{Z}_2$$

σ -operators as example: $\sigma(f)\sigma(\gamma)\,\sigma(f)^\dagger = (-1)^{\omega(f,\gamma)}\sigma(\gamma)$. In the case at hand, $u(\gamma) = \gamma$.

Symplectic matrix

In mathematics, a symplectic matrix is a $2n \times 2n$ matrix M with real entries that satisfies the condition

$$M^T \Omega M = \Omega$$

where M^T denotes the transpose of M and Ω is a fixed $2n \times 2n$ nonsingular, skew-symmetric matrix.

Typically Ω is chosen to be the block matrix

$$\Omega = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$$

where I_n is the $n \times n$ identity matrix. The matrix Ω has determinant +1 and its inverse is $\Omega^{-1} = \Omega^T = -\Omega$.

Operators H and K

$$H\sigma^x H^\dagger = \sigma^z, \qquad H\sigma^y H^\dagger = -\sigma^y, \qquad H\sigma^z H^\dagger = \sigma^x$$

$$K\sigma^x K^\dagger = \sigma^y, \qquad K\sigma^y K^\dagger = -\sigma^x, \qquad K\sigma^z K^\dagger = \sigma^z$$

These operators belong to $ESp_2(1)$. Authors show interesting relation between this group and Clifford group.

Controlled NOT

$$U\sigma_1^z U^\dagger = \sigma_1^z, \qquad U\sigma_1^x U^\dagger = \sigma_1^x \sigma_2^x$$

$$U\sigma_2^z U^\dagger = \sigma_1^z \sigma_2^z, \qquad U\sigma_2^x U^\dagger = \sigma_2^x.$$

If the first qubit is in state $|1\rangle$, then NOT operator is applied to the second qubit.

Symplectic maps

Let $T = U \cdot U^{\dagger}$ be an arbitrary symplectic transformation. The associated function $u\colon G^n \to G^n$ has the following properties:

1. u is linear.
2. u preserves the form ω, i.e., $\omega(u(f), u(g)) = \omega(f, g)$.

Maps with such properties, as is known, are called symplectic; they form the symplectic group $Sp_2(n)$.

Image and kernel

The image of a linear transformation or matrix is the span of the vectors of the linear transformation. (Think of it as what vectors you can get from applying the linear transformation or multiplying the matrix by a vector. In other words - all possible outputs)

The kernel of map T consists of all input vectors v such that $T(v) = 0$.

Theorem

The correspondence $\theta\colon T \to u$, $\theta\colon ESp_2(n) \to Sp_2(n)$ is a homomorphism of groups.

$Im\theta = Sp_2(n)$, $Ker\theta = G^n$ (the kernel is the set of σ-operators). Therefore, $ESp_2(n)/G^n \cong Sp_2(n)$.

The function $h\colon G \to H$ is a group homomorphism if whenever
$a * b = c$ we have $h(a) \cdot h(b) = h(c)$.
In other words, the group H in some sense has a similar algebraic structure as G and the homomorphism h preserves that.

Proof

We will check proof from the book.

The following equation is analyzed:

$$v(x+y)-v(x)-v(y)=w(x,y)$$

$Ker\theta = G^n$: correspondence between u and w is checked. The solutions are all linear functions.

The assertion that $Im\theta = Sp_2(n)$ is equivalent to the analyzed equation having a solution for any $u \in Sp_2(n)$.

H, K and CNOT

Ad hoc way of proving that $Im\theta = Sp_2(n)$. Consider the following symplectic transformations: $(H \cdot H^\dagger)[j]$, $(K \cdot K^\dagger)[j]$ and $(\Lambda(\sigma^x) \cdot \Lambda(\sigma^x)^\dagger)[j,k]$. Their images under the homomorphism θ generate the whole group $Sp_2(n)$.

H, K and CNOT

The specified elements of the group $ESp_2(n)$ generate all the σ-operators, i.e., the kernel of the homomorphism θ. Consequently, the following statement is true:

The group $ESp_2(n)$ is generated by these elements
$(H \cdot H^\dagger)[j]$, $(K \cdot K^\dagger)[j]$ and $(\Lambda(\sigma^x) \cdot \Lambda(\sigma^x)^\dagger)[j,k]$

Thank you for your attention!