Quantum Algorithms
Lecture 29
Classical and quantum codes I

Zhejiang University

Introduction

Motivation

Quantum computation is “not too” sensitive to errors in the realization of unitary operators: errors accumulate linearly. But this is not enough to make quantum computation practical.

Is it possible to replace an arbitrary quantum circuit by another circuit that would realize the same unitary operator (or compute the same Boolean function), but in an error-resistant fashion?

Main idea

The new circuit will resist not only inaccurate realization of unitary gates but also some interaction with the environment and stochastic errors (provided that they occur with small probability). The rough idea is to encode (replace) each qubit used in the computation (logical qubit) by several physical qubits. The essential fact is that errors usually affect only few qubits at a time, so that encoding increases the stability of a quantum state.

Classical and quantum

Organization of computation in a way that prevents accumulation of errors is called fault-tolerant computation. In the classical case, fault-tolerance can be achieved by the use of the repetition code: 0 is encoded by (0,..., 0) (n times), and 1 is encoded by (1,..., 1). Such a simple code does not work in the quantum case, but more complicated codes do. The first method of fault-tolerant quantum computation was invented by P. Shor.

Error recovery

Suppose we have a quantum state of n qubits that is subjected to an error. Under what condition is it possible to recover the original state, assuming that the execution of the recovery procedure is error-free? (The fault-tolerant computation deals with the more realistic situation where errors occur constantly, though at a small rate.) Of course, error recovery is not possible for a general state $|\xi\rangle \in B^{\otimes n}$. However, it can be possible for states $|\xi\rangle \in M$, where $M \subseteq B^{\otimes n}$ is a suitable fixed subspace. Likewise, in the classical case we should consider states that belong to a fixed subset $M \subseteq B^n$.

Codewords and codevectors

A classical code of type (n, m) is a subset $M \subseteq B^n$ which consists of 2^m elements (where m — the number of encoded bits — is not necessarily integral). Elements of M are called codewords.

A quantum code of type (n, m) is a subspace $M \subseteq B^{\otimes n}$ of dimension 2^m. Elements of M are called codevectors.

In short, (n, m) means that we encode m bits of information into n bits, $n \geq m$.

Quantum encoding

Firstly, an encoding must be specified, i.e., the subspace M must be identified with a fixed space L; usually, $L = B$. In other words, an encoding is an isometric embedding $V\colon L \to B^{\otimes n}$ such that $M = Im\, V$.

Secondly, sometimes one needs to consider one-to-many encodings (because errors happen and get corrected constantly, so at any moment there are some errors that have not been corrected yet). A one-to-many encoding is an isometric embedding $V\colon L \otimes F \to B^{\otimes n}$, where F is some auxiliary space.

Error model

Besides the code, we need to define an error model. It is also called communication channel: one may think that errors occur when a state (classical or quantum) is transferred from one location to another. Intuitively, this should be something like a multivalued map $B^n \to B^{n'}$ or $B^{\otimes n} \to B^{\otimes n'}$ (where n' is the number of bits at the output of the channel; usually, $n' = n$).

Classical codes

Probabilistic model

According to the probabilistic model, a communication channel is given by a set of conditional probabilities $p(y|x)$ for receiving the word y upon transmission of the word x. We will consider the case of independently distributed errors, where $n' = n$, and the conditional probabilities are determined by the probability $p1$ of an error (bit flip) in the transmission of a single bit:

$$p(y|x) = p1^{d(x,y)}(1 - p1)^{n-d(x,y)}$$

Here $d(x, y)$ is the Hamming distance — the number of distinct bits.

Unlikely errors

There is a standard method for simplifying a probabilistic error model by classifying errors as “likely” and “unlikely”. Let us estimate the probability that in the model defined above, more than k bit flips occur (this probability does not depend on x). Suppose that n and k are fixed, whereas $p1 \to 0$. Then

$$\mathbf{Pr}\left[\text{number of bit flips} > k\right] = \sum_{j>k} \binom{n}{j} p_1^j (1-p_1)^{n-j} = O(p_1^{k+1})$$

Thus the probability that more than k bits flip is small. So we say that this event is unlikely; we can greatly simplify the model by assuming that such an event never happens.

Likely errors

We will suppose that, upon transmission of the word x, some word y is received such that $d(x, y) \leq k$. This simplified model only defines a set of possible (or "likely") outcomes but says nothing about their probabilities.

We introduce the notation:

$$N = \mathbb{B}^n \quad \text{— set of inputs,}$$
$$N' = \mathbb{B}^{n'} \quad \text{— set of outputs,}$$
$$E \subseteq N \times N' \quad \text{— set of transitions (i.e., set of errors),}$$

$$E(n, k) = \{(x, y) : d(x, y) \leq k\}.$$

A code M corrects errors from a set $E \subseteq N \times N'$ if for any $x1, x2 \in M$, $(x1, y1) \in E$, $(x2, y2) \in E$, the condition $x1 \neq x2$ implies that $y1 \neq y2$.

In the particular case $E = E(n, k)$, we say that the code corrects k errors.

Error correction

An error-correcting transformation is a map P: $N' \to N$ such that, if $(x, y) \in E$ and $x \in M$, then $P(y) = x$.

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.

Code distance

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

$$d(M) = \min\{d(x1, x2): x1, x2 \in M, x1 \neq x2\}$$

For the code M_3 the code distance is 3.

A code M corrects k errors if and only if $d(M) > 2k$.

Examples of classical codes

Simple examples

The repetition code (type $(n, 1)$) can be used with the obvious encoding: we repeat a single bit n times. To restore the codeword after an error, we replace the value of the bits with the value that occurs most frequently. This series of codes, as will be shown later, does not generalize to the quantum case.

Parity check is a code of type $(n, n-1)$ and distance 2. It consists of all even words, i.e., of words containing an even number of 1s.

Hamming code

This code is of type $(n, n-r)$, where $n = 2^r - 1$. The Hamming code has distance $d(H_r) = 3$ for any $r \geq 2$ (so it can correct one error). We can also write it as $(2^r - 1, 2^r - 1 - r)$.

Sequences of bits $x = (x_\alpha : \alpha = 1, \ldots, n)$.

The index of each bit can be represented in binary as $\alpha = (\alpha_1, \ldots, \alpha_r)$.

$$\mu_j(x) = \sum_{\alpha:\, \alpha_j = 1} x_\alpha \mod 2,$$

$$H_r = \left\{ x \in \mathbb{B}^{2^r} : \mu_1(x) = \cdots = \mu_r(x) = 0 \right\}$$

Hamming code

Example for H_3:

$$\begin{aligned}
&&&&&&x_{100}+x_{101}+&&x_{110}+x_{111}&=\mu_1(x)=0,\\
&&x_{010}+x_{011}&+&&&&&x_{110}+x_{111}&=\mu_2(x)=0,\\
x_{001}&+&&x_{011}&+&&x_{101}&+&&x_{111}=\mu_3(x)=0.
\end{aligned}$$

We can see, that in first row first bit of index is equal to 1, is second row second bit is equal to 1, and in third row the third bit is equal to 1.

Linear codes

Check matrix

A linear code of type (n, m) can be defined by a dual basis, i.e., a set of $n - m$ linearly independent linear forms (called check sums) which vanish on M. The coefficients of the check sums constitute rows of the check matrix. For example, the check matrix of the Hamming code H_3 is

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\begin{aligned} x_{100} + x_{101} + x_{110} + x_{111} &= \mu_1(x) = 0, \\ x_{010} + x_{011} + x_{110} + x_{111} &= \mu_2(x) = 0, \\ x_{001} + x_{011} + x_{101} + x_{111} &= \mu_3(x) = 0. \end{aligned}$$

Code distance

The code distance of a linear code equals the minimum number of distinct columns of the check matrix that are linearly dependent.

The columns of the check matrix of the Hamming code H_r correspond to the nonzero elements. Any two columns are different, hence they are linearly independent (so minimum is bigger than 2). On the other hand, the sum of the first three columns is 0 (for $r \geq 2$). Therefore the code distance is 3.

Error models for quantum codes

Analogues

Analogue of the transition set $E \subseteq N \times N'$ is an arbitrary linear subspace $E \subseteq L(N, N')$, called an error space.

Analogue of the set $E(n, k)$:

$$\mathcal{E}(n,k) = \sum_{A:\,|A|\leq k} \mathcal{E}[A]$$

We take the sum of linear subspaces:

$$\sum_j \mathcal{L}_j = \left\{ \sum_j X_j : \ X_j \in \mathcal{L}_j \right\}$$

We will be interested in the possibility of correcting errors from the space $E(n, k)$.

Physical model of quantum errors

We assume that the interaction is described by the Hamiltonian

$$H = H_0 + V, \qquad H_0 = I_{\mathcal{B}^{\otimes n}} \otimes Z, \qquad V = \sum_{j=1}^{n} \sum_{\alpha \in \{x,y,z\}} \sigma_j^{\alpha} \otimes B_{j\alpha}$$

If the interaction lasts for some time τ, it results in the evolution of the quantum state by the unitary operator

$$U = \exp(-i\tau H) = e^{-i\tau(H_0+V)} = \lim_{N\to\infty} \left(e^{-i\frac{\tau}{N}H_0} \left(1 - i\frac{\tau}{N} V\right)\right)^N$$

$$= \lim_{N\to\infty} e^{-i\tau H_0} \left(1 - i\frac{\tau}{N} V\left(\tfrac{N-1}{N}\tau\right)\right) \cdots \left(1 - i\frac{\tau}{N} V\left(\tfrac{1}{N}\tau\right)\right) \left(1 - i\frac{\tau}{N} V(0)\right)$$

Physical model of quantum errors

By doing mathematical replacements, authors obtain:

$$U = \exp(-i\tau H) = \sum_{k=0}^{\infty} X_k, \qquad X_k \in \mathcal{E}(n,k) \otimes \mathbf{L}(\mathcal{F}),$$

(15.4)

$$X_k = e^{-i\tau H_0} \left((-i)^k \int_{0<t_1<\cdots<t_k<\tau} \cdots \int V(t_k) \cdots V(t_1)\, dt_1 \cdots dt_k \right),$$

where

$$V(t) = e^{itH_0} V e^{-itH_0} = \sum_{j,\alpha} \sigma_j^{\alpha} \otimes B_{j\alpha}(t), \qquad B_{j\alpha}(t) = e^{itZ} B_{j\alpha} e^{-itZ}.$$

Physical model of quantum errors

If the interaction of the qubits with the environment is small, then we can obtain an upper bound for the norm of each term of U (our error evolution).

If errors from the space $E(n,k)$ are recoverable (assuming that the initial state belongs to $M \bigotimes F$, where M is a suitable code), then the error-correcting procedure will cancel the effect of U with precision $O(\delta^{k+1})$.

Model of independent errors

Each qubit interacts with its own piece of environment, which is initially not entangled with the rest of the system and is discarded after the action of the operator U.

Let us assume that the quantum state of n qubits undergoes the transformation that is described by the physically realizable superoperator T.

$$T = (I+R)^{\otimes n} = \underbrace{\sum_{A:\,|A|\le k} R^{\otimes A} \otimes I^{\otimes(\{1,\ldots,n\}\setminus A)}}_{T^{(k)}} + \underbrace{\sum_{A:\,|A|>k} R^{\otimes A} \otimes I^{\otimes(\{1,\ldots,n\}\setminus A)}}_{P}$$

Coherent and stochastic errors

The model of independent errors includes two extreme cases.

If $T = U \cdot U^{\dagger}$ (where U is unitary, $\|U - I\| \leq \delta/2$), the errors are called coherent.

The errors are called stochastic, indicating that they can be described in terms of probability rather than operator or superoperator norms if:

$$T = (1-p)I \cdot I + \sum_j p_j U_j \cdot U_j^{\dagger}, \quad U_j^{\dagger} U_j = I, \quad p = \sum_j p_j \leq \delta/2$$

Definition of quantum error correction

Introduction

Following the classical analogy, we would like to say that quantum errors are recoverable if they take distinct codevectors to distinct codevectors. However, the general philosophy of quantum mechanics suggests that we replace “distinct” by “orthogonal”.

Correcting errors

A quantum code (a subspace $M \subseteq N$) corrects errors from $E \subseteq L(N, N')$ if

$$\forall |\xi_1\rangle, |\xi_2\rangle \in \mathcal{M}\ \forall X, Y \in \mathcal{E}\ \left(\langle \xi_2 | \xi_1 \rangle = 0\right) \Rightarrow \left(\langle \xi_2 | Y^\dagger X | \xi_1 \rangle = 0\right)$$

In the case where $E = E(n, k)$, one says that the code corrects k errors.

Error-correcting transformation

Let $M \subseteq N$ and $E \subseteq L(N, N')$. A physically realizable superoperator P: $L(N') \to L(M)$ is called an error-correcting transformation for the code M and the error space E if

$$\forall T \in E \cdot E \dagger \ \exists c = c(T) \ \forall \rho \in L(M) \ PT\rho = c(T)\rho$$

Note that if T is trace-preserving, then $c(T) = 1$.

Examples

Trivial code of type (n, m): let $M = B^{\otimes m} \otimes |0^{n-m}\rangle \; and \; E = E[m+1, \ldots, n]$, i.e., the first m qubits are used for the coding whereas the errors act on the other qubits.

There is, of course, little practical use for such a code. It is interesting, however, that any error-correcting quantum code has, in a certain sense, the same structure as the trivial one.

Examples

Authors examine a quantum analog of the repetition code: $M_n^z = C(|0,\dots,0\rangle, |1,\dots,1\rangle)$.

By considering vectors with phase (+ and -), authors conclude that the repetition code of any size does not protect against a one-qubit error.

Error detection

A quantum code $M \subseteq N$ detects an error $Z \in L(N)$ if there exists some $c = c(Z) \in C$ such that

$$\forall |\xi_1\rangle, |\xi_2\rangle \in \mathcal{M} \ \langle \xi_2 | Z | \xi_1 \rangle = c(Z) \langle \xi_2 | \xi_1 \rangle$$

The code distance is the smallest number $d = d(M)$ for which the code does not detect errors from the space $E(n, d)$.

Error correction

A code $M \subseteq N$ corrects errors from $E \subseteq L(N, N')$ if and only if it detects errors from the space

$$\mathcal{E}^\dagger \mathcal{E} = \left\{ \sum_p Y_p^\dagger X_p : \ X_p, Y_p \in \mathcal{E} \right\}$$

In particular, a code $M \subseteq B^{\otimes n}$ corrects k errors if and only if $d(M) > 2k$.

Lemma

Let a quantum code $M \subseteq N$ correct errors from a subspace $E \subseteq L(N, N')$. Then there exist a Hilbert space F, an isometric embedding $V\colon M \otimes F \to N'$ and a linear map $f\colon E \to F$ such that

$$\forall X \in \mathcal{E}\ \forall |\xi\rangle \in \mathcal{M}\ X|\xi\rangle = V\big(|\xi\rangle \otimes |f(X)\rangle\big)$$

Theorem

If the code M corrects errors from E, then an error-correcting transformation exists.

Summary

An error-correcting code is characterized by the property that the error does not mix with the encoded state, i.e., it remains in the form of a separate tensor factor $|\eta\rangle = f(X) \in F$. (We may say that the original state $|\xi\rangle \in M$ gets encoded with the one-to-many encoding V.) The correcting transformation extracts the "built-in" error $|\eta\rangle$ and deposits it in the trash bin.

Thank you for your attention!