Quantum Algorithms
Lecture 31
Classical and quantum codes III

Zhejiang University

Symplectic (stabilizer) codes

Introduction

Symplectic (stabilizer) codes are analogous to the classical linear codes. The role of check sums is played by the σ-operators $\sigma(\alpha 1, \beta 1, \ldots, \alpha n, \beta n)$.

For example, the Shor code can be represented in this way. Recall that this is a two-dimensional subspace $M \subseteq B^{\otimes r^2}$ spanned by the vectors

$$|\xi_a\rangle = 2^{-(r-1)/2} \sum_{\substack{y_1,\ldots,y_r \in \mathbb{F}_2 \\ y_1+\cdots+y_r=a}} \left| \begin{matrix} y_1 & \cdots & \cdots & y_1 \\ y_2 & \cdots & \cdots & y_2 \\ \cdots & \cdots & \cdots & \cdots \\ y_r & \cdots & \cdots & y_r \end{matrix} \right\rangle \qquad (a = 0, 1)$$

What equations do vectors of M satisfy?

$|\xi\rangle$ is a linear combination of special basis vectors: each row consists of the repetition of a single bit.

$\prod_{k=1}^{r}\left(\sigma_{jk}^{x}\sigma_{j(k+1)}^{x}\right)$ flips all the bits in the j-th and $j+1$-th rows

$$\left|\begin{array}{ccc} \cdots & \cdots & \cdots \\ y_j & \cdots & y_j \\ y_{j+1} & \cdots & y_{j+1} \\ \cdots & \cdots & \cdots \end{array}\right\rangle \longmapsto \left|\begin{array}{ccc} \cdots & \cdots & \cdots \\ y_j+1 & \cdots & y_j+1 \\ y_{j+1}+1 & \cdots & y_{j+1}+1 \\ \cdots & \cdots & \cdots \end{array}\right\rangle$$

General definition

A symplectic quantum code is a subspace of the form

$$\mathcal{M} = \left\{ |\xi\rangle \in \mathcal{B}^{\otimes n} \,:\, \forall j \; X_j|\xi\rangle = |\xi\rangle \right\}, \qquad \text{where}$$

$$X_j = (-1)^{\mu_j}\sigma(f_j), \qquad f_j \in G^n, \quad \mu_j \in \mathbb{Z}_2.$$

The operators X_j must commute with each other. They are called check operators.

Check operators commute

The requirement that the check operators commute is equivalent to the condition $\omega(f_j, f_k) = 0$.

Without loss of generality we may assume that the f_j are linearly independent.

What makes the code

Note that different choices of check operators may correspond to the same code. In fact, the code depends only on the subspace $F \subseteq G^n$ spanned by the vectors f_j, and on the function $\mu\colon F \to \mathbb{Z}^2$.

Invariant definition

Let $F \subseteq G^n$ be an isotropic subspace, i.e., $\omega(f,g) = 0$ for any $f, g \in F$. Also let a function μ: $F \to \mathbb{Z}^2$ satisfy the equation

$$\mu(f+g) - \mu(f) - \mu(g) = \nu(f,g), \quad \text{where } \nu(f,g) = \frac{\widetilde{\omega}(f,g)}{2} \in \mathbb{Z}_2$$

(The function ν is defined on pairs (f,g) for which $\omega(f,g) = 0$.) Then the corresponding symplectic code is

$$\mathrm{SympCode}(F,\mu) \stackrel{\mathrm{def}}{=} \left\{ |\xi\rangle \in \mathcal{B}^{\otimes n} \,:\, \forall f \in F \;\; \sigma(f)|\xi\rangle = (-1)^{\mu(f)}|\xi\rangle \right\}$$

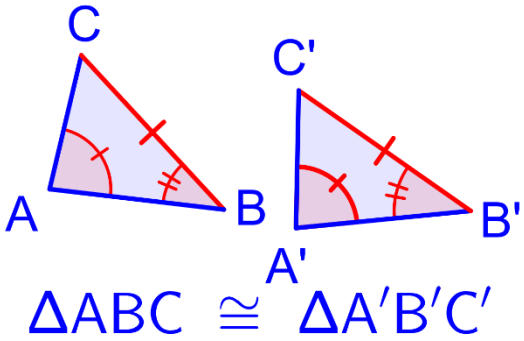
Congruent codes

Equation $\mu(f+g)-\mu(f)-\mu(g)=\nu(f,g)$ has a solution. In fact, there are 2^{dimF} solutions; any two solutions differ by a linear function. We call the corresponding codes congruent.

$$\dim(SympCode(F,\mu))=2^{n-dimF}$$

The congruent codes form an orthogonal decomposition of $B^{\otimes n}$.

In modular arithmetic, congruence means having the same remainder when divided by a specified integer.



Lemma

By symplectic transformations, an arbitrary symplectic code $SympCode(F, \mu)$ can be reduced to a trivial one, for which the check operators are $\sigma^z\,[1], \ldots, \sigma^z[s]$ $(s = dimF)$.

Detecting errors

We now examine whether a symplectic code $SympCode(F, \mu)$ is capable of detecting k-qubit errors. By linearity, it is sufficient to consider errors of the form $Z = \sigma(g)$, $|g| \leq k$. Three cases for $Z = \sigma(g)$:

1. $g \notin F_+$, the code detects such an error.
2. $g \in F$, such an error is indistinguishable from the identity operator, since it does not alter the codevector.
3. $g \in F_+ \backslash \mathrm{F}$. The code does not detect such an error.

Theorem

The code $M = SympCode(F, \mu)$ has distance

$$d(M) = \min\{|f|: f \in F + \backslash \mathrm{F}\}$$

In classical linear codes the minimum is taken over a subspace with 0 excluded, whereas for symplectic codes 0 is replaced by the nontrivial subspace F.

Example

A symplectic code of type (5,1) that corrects 1 error: the subspace F is generated by the rows of the matrix

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

It can be verified that $\omega(f_j, f_k) = 0$ for any two rows f_j, f_k. We note that the columns of the matrix come in pairs. If we take any two pairs, then the corresponding four columns are linearly independent. Consequently, for any $g \neq 0$ supported by these columns, there is a row f_j such that $\omega(f_j, g) \neq 0$. Thus the code distance is greater than 2. (In fact, the distance is 3 since the first 6 columns are linearly dependent.)

5-qubit code summary

Raymond Laflamme and collaborators found a class of 5-qubit codes that does the same as Shor's code, which also have the property of being fault-tolerant. A 5-qubit code is the smallest possible code that protects a single logical qubit against single-qubit errors.

No quantum code of type (4,1) is capable of correcting a single error - see Problem 15.2.

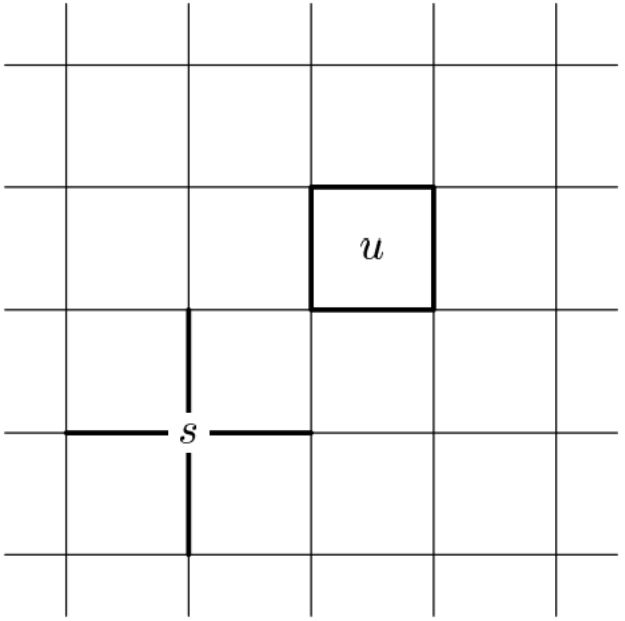
Toric code

Introduction

Toric code is an important example of a symplectic code. It is constructed as follows. Consider an $r \times r$ lattice on the torus. We put a qubit on each of its edges. In this way we have $2r^2$ qubits. The check operators will be of two types.

Vertex s connects 4 qubits, associated operators σ^x

Face u connects 4 qubits, associated operators σ^z



Number of errors

The sets $F_+^{(z)} \backslash \mathrm{F}^{(z)}$ and $F_+^{(x)} \backslash \mathrm{F}^{(x)}$ are formed by cycles and cocycles that are not homologous to 0. Consequently the code distance is the minimum size (the number of nonzero coefficients) of such a cycle or cocycle. It is easy to see that this minimum equals r. This shows that the toric code corrects $\lfloor (r-1)/2 \rfloor$ errors.

The family of Toric codes

The family of Toric codes (with $r = 1,2, \ldots$) provides an example of local check codes. Specifically, the following conditions are satisfied:

- each check operator acts on a uniformly bounded number of qubits;
- each qubit enters a uniformly bounded number of check operators;
- the family contains codes with arbitrarily large distance.

Syndrome measurement

Toric codes are interesting in that syndrome measurement (an important part of error correction) can be realized by a constant depth circuit. Therefore an error in the execution of this circuit will affect only a bounded number of qubits — a useful property for fault-tolerant computation.

Error correction for symplectic codes

Error detection

We examine a special case where the error is a σ-operator, $W = \sigma(g)$. Let $X_j = (-1)^{\mu_j}\sigma(f_j)$ be the check operators, and F the corresponding isotropic subspace. The sequence of bits $\lambda(g) = (\omega(f_1, g), \ldots, \omega(f_s, g))$ is called the syndrome of g. Each of these bits can be measured by measuring the eigenvalue of X_j on the quantum state $|\psi\rangle = W|\xi\rangle$. The measurement of one bit does not change the values of the other, because the check operators commute.

Error correction

We may take a different error g' for g, but only if $g' - g \in F$.

How we should correct errors. After the syndrome is determined, we reconstruct the error (up to an element $f = g' - g \in F$) and apply the operator which is inverse to the operator of the supposed error. Thus we obtain a state that differ from the initial one by a phase factor.

General case

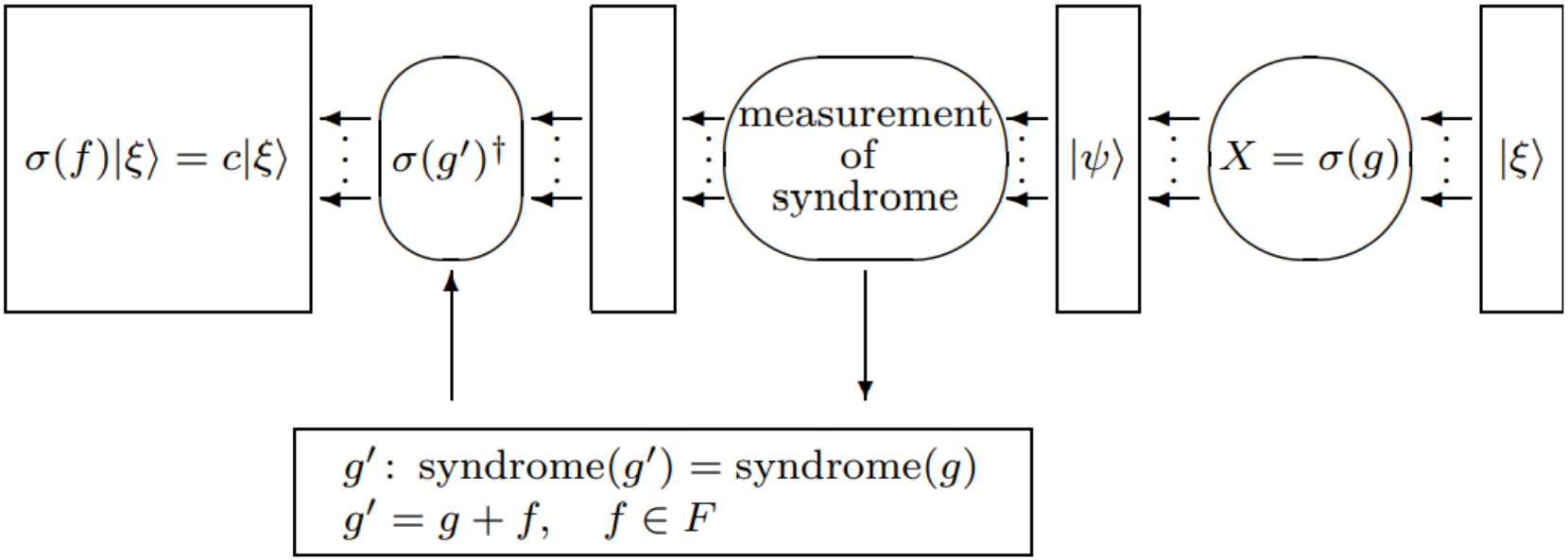
We have considered the case of an error of type $\sigma(g)$. But, actually, it is required that an error-correcting transformation protect against all superoperators of the form

$$T = \sum_{|h|\leq k, |h'|\leq k} b_{h,h'} \sigma(h) \cdot \sigma(h')^{\dagger}$$

There exists a polynomial algorithm for reconstructing an error from its syndrome for the toric code.

Summary

Error correction procedure for symplectic codes:

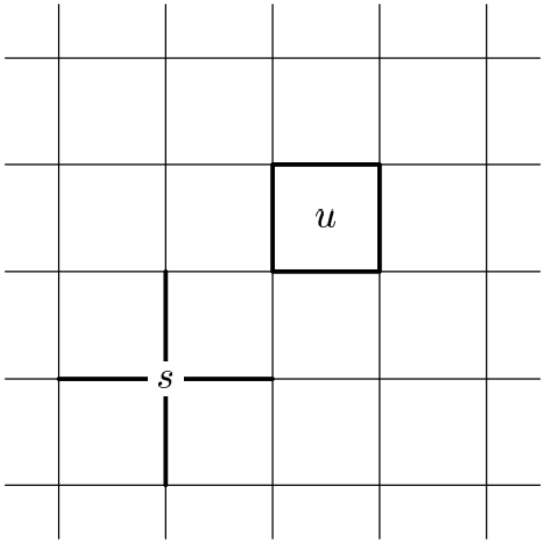


Anyons (an example based on the toric code)

Introduction

Using the construction of the toric code, authors try to give a better idea of Abelian anyons.

Once again, authors consider a square lattice on the torus (or on the plane — now we are only interested in a region with trivial topology). As earlier, operators are associated to each vertex s and each face u.



Quasiparticles

Excited states can be classified by the set of conditions they violate. Specifically, the states violating a particular set of conditions form a subspace; such subspaces form an orthogonal decomposition of the total state space.

Consider an excited state $|\eta\rangle$ with the smallest nonzero energy. Such a state violates precisely two conditions, for instance, at two vertices, s and p.

We say that in the state $|\eta\rangle$ there are two quasiparticles (elementary excitations) located at the vertices s and p. Thus quasiparticle is a mental device for classifying excited states.

Positions as eigenstates

It is a special property of Hamiltonian that states with certain quasiparticle positions are also eigenstates. However, the classification of low energy excited states by quasiparticle positions, though approximate, works amazingly well for most physical media.

Describing the state

An arbitrary state of the system can be described as a set of quasiparticles of two types, one of which “lives” on vertices, the other on faces. Mathematically, a quasiparticle is simply a violated code condition, but now we think of it as a physical object. Particles-excitations can move, be created and annihilated.

Anyons

In physics, an anyon is a type of quasiparticle that occurs only in two-dimensional systems, with properties much less restricted than the two kinds of standard elementary particles, fermions and bosons. In general, the operation of exchanging two identical particles, although it may cause a global phase shift, cannot affect observables. Anyons are generally classified as abelian or non-abelian. Abelian anyons (detected by two experiments in 2020) play a major role in the fractional quantum Hall effect. Non-abelian anyons have not been definitively detected, although this is an active area of research.

Abelian anyons

The state vector gets multiplied by −1. This indicates some sort of long range interaction between the particles: the moving particle somehow “knows” about the second particle without ever touching it! However, the interaction is purely topological: the state evolution depends only on the isotopy class of the braid the particle world lines form in space-time. In the case at hand, the evolution is just the multiplication by a phase factor; such particles are called Abelian anyons.

Moving particles on the torus

On the torus we can move particles over two different cycles that form a basis of the homology group. For instance, create a pair of particles from the ground state, move one of them around a cycle, and annihilate with the second one. Now it becomes important that the ground state is not unique. Recall that there is a 4-dimensional space of ground states — the code subspace. The process we have just described affects an operator acting on this subspace.

Thank you for your attention!