Ph/CS 219b

Exercises
Due: Thursday 22 February 2018

3.1 Bound on D-dimensional codes

In class we proved a bound on $[[n,k,d]]$ for local stabilizer codes in 2 dimensions: $kd^2 = O(n)$, where k is the number of encoded qubits, d is the code distance, and n is the code length. For your convenience, the proof is appended to the end of this assignment.

Using similar reasoning, derive a bound on D-dimensional stabilizer codes of the form $kd^\alpha = O(n)$. Express α in terms of D.

3.2 Price of a code

The distance d of a stabilizer code is the size of the smallest set of qubits in the code black that supports a nontrivial logical operator. In contrast, the *price* p of a code is defined as the size of the smallest set of qubit that supports *all* of the codes logical operators. Evidently $p \geq d$.

a) What is the price of the [[7,1,3]] quantum code?

b) Use the cleaning lemma to show that $p \leq n - d + 1$.

c) Show that $p \geq k + d - 1$. **Hint**: Use this result proved in class: Suppose that the code block can be divided into three parts ABC such that A and B are both correctable. Then $k \leq |C|$, where $|C|$ is the number of qubits in C.

Note that the results from (*b*) and (*c*) imply $n - k \geq 2(d-1)$, the *quantum Singleton bound.*

3.3 Price of a local code

Show that the price p of a D-dimensional stabilizer code satisfies the bound $p = O(nd^{-1/(D-1)})$. **Hint**: Use the holographic principle and the union lemma. (See the discussion appended to the end of this assignment.)

3.4 Higher-dimensional toric codes

To understand the logical operators of the 2D toric code, we found it convenient to use the concept of a *chain complex*. We defined vector spaces V_0, V_1, V_2 over $\mathbb{F}^2$ and boundary operators ∂_1, ∂_2 such that

$$V_2 \xrightarrow{\partial_2} V_1 \xrightarrow{\partial_1} V_0 \tag{1}$$

and

$$\partial_1 \circ \partial_2 = 0. \tag{2}$$

For example, for the purpose of formulating the $\boldsymbol{Z}$-type logical operators of the toric code, vectors in V_2 are *2-chains*, which assign a bit to each lattice plaquette, vectors in V_1 are *1-chains*, which assign a bit to each edge, and vectors in V_0 are *0-chains*, which assign a bit to each site. We saw that a 2-chain ω may be interpreted as a stabilizer element (a product of $\boldsymbol{Z}$-type plaquette operators), a 1-chain ϵ may be interpreted as a $\boldsymbol{Z}$-type error operator, and the 0-chain $\sigma = \partial_1 \epsilon$ may be interpreted as the syndrome of ϵ (determined by measuring the $\boldsymbol{X}$-type site operators). The property $\partial_1 \circ \partial_2 = 0$ expresses that a $\boldsymbol{Z}$-type stabilizer operator has a trivial syndrome.

A $\boldsymbol{Z}$-type operator which lies in the code stabilizer S is the boundary $\partial_2 \omega$ of some 2-chain ω; it is contained in the image of ∂_2. A $\boldsymbol{Z}$-type operator ϵ which lies in the normalizer $S^\perp$ (commutes with the stabilizer) is a *1-cycle* with trivial boundary, $\partial_1 \epsilon = 0$; it is contained in the kernel of ∂_1. Thus the code's $\boldsymbol{Z}$-type logical Pauli operators are elements of the coset space. $\mathrm{Ker}(\partial_1)/\mathrm{Im}(\partial_2)$.

We have also seen how this chain-complex language can be applied to any CSS stabilizer code. In this problem, we'll apply it to toric codes in more than 2 dimensions.

Consider a 3D version of the toric code defined on an $L \times L \times L$ cubic lattice with periodic boundary conditions. Qubits reside on lattice links. There is a weight-4 $\boldsymbol{Z}$-type stabilizer generator associated with each lattice plaquette, and a weight-6 $\boldsymbol{X}$-type stabilizer generator associated with each lattice site.

a) Construct a chain complex suited for describing the $\boldsymbol{Z}$-type logical operators of this code, and find the logical operators. How many encoded qubits are there? What is the minimal weight d_Z of a $\boldsymbol{Z}$-type logical operator?

b) Construct a chain complex suited for describing the $\boldsymbol{X}$-type logical operators of this code, and find the logical operators. Check that these $\boldsymbol{X}$-type logical operators have the expected commutation relations with the $\boldsymbol{Z}$-type logical operators. What is the minimal weight d_X of an $\boldsymbol{X}$-type logical operator?

Consider a 4D version of the toric code defined on an $L \times L \times L \times L$ hypercubic lattice with periodic boundary conditions. Qubits reside on lattice plaquettes. There is a weight-6 $\boldsymbol{Z}$-type stabilizer generator associated with each lattice cube, and a weight-6 $\boldsymbol{X}$-type stabilizer generator associated with each lattice link.

c) Construct a chain complex suited for describing the $\boldsymbol{Z}$-type logical operators of this code, and find the logical operators. How many encoded qubits are there? What is the minimal weight d_Z of a $\boldsymbol{Z}$-type logical operator?

d) Construct a chain complex suited for describing the $\boldsymbol{X}$-type logical operators of this code, and find the logical operators. Check that these $\boldsymbol{X}$-type logical operators have the expected commutation relations with the $\boldsymbol{Z}$-type logical operators. What is the minimal weight d_X of an $\boldsymbol{X}$-type logical operator?

A bound on topological stabilizer codes

We say that a stabilizer code family is *local* if we may choose all stabilizer generators to be geometrically local in D spatial dimensions, for some finite D. If in addition the code distance d increases with the code length n, we say that the code is *topological*. For example, if the qubits are arranged in a D-dimensional (hyper)cubic lattice, the code is local if each stabilizer generator has its support on a (hyper)cube with side length r, where r is a constant independent of the length n of the code. When a code is local in D dimensions, we may call it a *D-dimensional code*, dropping the word "local" which is understood. We say that r is the *range* of the code generators. Note that for a topological code family, any set of qubits of constant size is correctable for sufficiently large n.

In class we proved a bound on the code parameters $[[n,k,d]]$ for two-dimensional (2D) stabilizer codes: $kd^2 = O(n)$. Here we review the argument leading to this conclusion.

The proof of the bound makes use of three lemmas — the cleaning lemma, the union lemma, and the expansion lemma. The cleaning lemma for stabilizer codes asserts that for any correctable set M and logical Pauli operator x, we may choose x to be supported on the complement M^c of M. That is, for any logical operator x (commuting with the code stabilizer S) there exists $y \in S$ such that xy is supported on M^c. A proof of the cleaning lemma was appended to Problem Set 2.

We say that two sets of qubits are *separated* if no stabilizer generator has support on both sets. For a 2D code this is ensured if no $r \times r$ square intersects with both sets. The union lemma says that if M_1 and M_2 are separated and both are correctable, then their union $M_1 \cup M_2$ is also correctable. To prove the union lemma by contradiction, suppose that $M_1 \cup M_2$ is not correctable, in which case there exists a nontrivial logical operator x supported on $M_1 \cup M_2$, of the form

$$x = (y_1)_{M_1} \otimes (y_2)_{M_2} \otimes I_{(M_1 \cup M_2)^c}. \tag{3}$$

Because x is logical, it commutes will all stabilizer generators, and since no generator has support on both M_1 and M_2, it must be that

$$x_1 = (y_1)_{M_1} \otimes I_{M_2} \otimes I_{(M_1 \cup M_2)^c} \quad \text{and} \quad x_2 = I_{M_1} \otimes (y_2)_{M_2} \otimes I_{(M_1 \cup M_2)^c} \tag{4}$$

also commute with all stabilizer generators, and hence are logical. Furthermore, since $x = x_1 x_2$, and x is nontrivial, either x_1 or x_2 must be nontrivial. This contradicts our assumption that M_1 and M_2 are correctable, proving the lemma.

The expansion lemma requires a bit more explanation. Let M' denote the support of all stabilizer generators which act nontrivially on M. The *external boundary* $\partial_+ M$ of M is $M' \cap M^c$, and the *internal boundary* $\partial_- M$ of M is $(M^c)' \cap M$. For a local code with range r, we may visualize $\partial_+ M$ as a thin shell surrounding M (with thickness no greater than r), while $\partial_- M$ is a thin shell surrounding M^c. The expansion lemma specifies conditions under which we can slightly augment the size of a correctable set while preserving its correctability. It asserts the following: Suppose that $M = NA$ (that is, $M = N \cup A$, where N and A are disjoint). Suppose further that A contains $\partial_- M$, and that N, A, and $\partial_+ M$ are correctable. Then M is correctable.

To prove the expansion lemma by contradiction, suppose that M is not correctable, in which case there is a nontrivial logical Pauli operator x which is supported on M. Furthermore, because A is correctable, there is a stabilizer element y, which we may choose to be supported on M', such that $z = xy$ is cleaned on A:

$$z = (w)_N \otimes I_A \otimes v_{\partial_+ M} \otimes I_{(M')^c}. \tag{5}$$

Because z is logical, it commutes with all stabilizer generators, and because $A \subseteq \partial_- M$, no stabilizer generator acts nontrivially on both N and $\partial_+ M$. Therefore, the restriction z_1 of z to N is logical, and the restriction z_2 of z to $\partial_+ M$ is also logical. Furthermore, since $z = z_1 z_2$ and z is nontrivial, either z_1 or z_2 must be nontrivial. This contradicts our assumption that N and $\partial_+ M$ are correctable, proving the lemma.

Next, we use the cleaning lemma and expansion lemma to infer the *holographic principle* for 2D codes, which asserts that, for some constant α, any square on the lattice with side length $\ell = \alpha d$ is a correctable set of qubits. Note that this is not obvious, since the number of qubits contained in the square is $\Omega(d^2)$, and hence, for a topological code family becomes much larger than the code distance d (the size of the smallest noncorrectable set) for sufficiently large n.

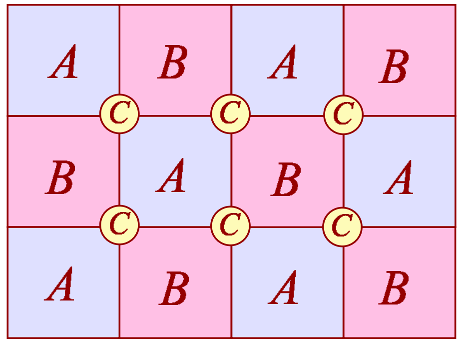
To prove the holographic principle, consider two concentric squares N and M, where N has side length $\ell - 4r$, and M has side length $\ell - 2r$; therefore, M' is contained in a square with side length ℓ, and $A = M \setminus N$ contains $\partial_- M$. The expansion lemma ensures that M is correctable if N, A, and $\partial_+ M$ are all correctable. By definition of distance a set is correctable if it contains fewer than d qubits, and therefore $\partial_+ M$ and A are both correctable provided that

$$|\partial_+ M| \leq |M'| - |M| \leq \ell^2 - (\ell - 2r)^2 < 4r\ell < d. \tag{6}$$

Now imagine starting with a small square, with area less than d so that the square is correctable, and gradually increasing the side length step-by-step, where the length grows by $2r$ in each step. According to eq.(6), the square continues to be correctable as long as the side length ℓ remains less than $d/4r$. This proves the holographic principle. We call this the holographic principle, somewhat whimsically, because if logical information is encoded in the square, then some of that logical information (though perhaps not all) must be accessible near the square's boundary.

To prove our bound on $[[n, k, d]]$ we need one more result, which applies to more general binary quantum codes, not just to stabilizer codes. Suppose the code block is divided into three regions ABC, where A and B are both correctable. Then the number k of encoded qubits can be no larger than $|C|$, the number of qubits in C. I proved this in class using properties of the Von Neumann entropy, and I won't repeat the proof here.

Now we are ready to prove the bound. For a 2D stabilizer code, consider partitioning the code block into three sets ABC as shown here:



Each connected component of A is a square with side length less than $d/4r$, with corners clipped off as shown, and same for B. Each connected component of C has constant size, but is sufficiently large to separate the components of A by a distance larger than the range r of the stabilizer generators (and same for B). By the holographic principle, each component of A is correctable, and because the components are separated, A is correctable by the union lemma. Likewise, B is also correctable. The number of components of C is $O(n/d^2)$, and each component has constant size. We conclude that

$$k \leq |C| = O(n/d^2), \tag{7}$$

which proves the bound.