Q. Inf. Science II (6.443/8.371/18.436) — Spring 2018

Assignment 3b

Due: **Friday***, Mar 23, 2018 at* ***5pm***

Turn in a paper copy of your solutions in the drop box on the third floor between buildings 8 and 16. If you collaborated with other students, please list their names, and make sure that you write up solutions on your own.

1. **Tillich-Zémor product of cycles** In problem 1b of pset 2, you showed that a stabilizer code could be built from any two classical codes by defining check matrices

$$H_X = \begin{pmatrix} H_1 \otimes I_{n_2} & I_{k_1} \otimes H_2^T \end{pmatrix} \qquad \text{and} \qquad H_Z = \begin{pmatrix} I_{n_1} \otimes H_2 & H_1^T \otimes I_{k_2} \end{pmatrix} \tag{1}$$

This product is called the Tillich-Zémor product, after its inventors. Suppose that we take $n = n_1 = n_2 = k_1 = k_2$ and choose $H_1 = H_2$ to be the check matrices corresponding to the repetition code on a cycle. That is, the constraints are $x_1 + x_2 = 0, x_2 + x_3 = 0, \ldots, x_n + n_1 = 0$, corresponding to check matrices

$$H_1 = H_2 = \begin{pmatrix} 1 & 1 & & \\ 0 & 1 & 1 & \\ & \ddots & \ddots & \\ 1 & & & 1 \end{pmatrix} \tag{2}$$

The resulting code is equivalent to the toric code. Explain why.

2. **Toric code random errors** Consider the toric code on an $L \times L$ grid. While the distance of this code is L, it can correct a constant rate of random errors with high probability. That is, suppose that each qubit experiences an X error with probability ϵ, and independently, a Z error with probability ϵ. (This means the probability of Y errors is ϵ^2. We could also discuss depolarizing noise in which X, Y, Z errors are equally likely but this make things more complicated without changing the conclusions by much.) This will allow us to focus on X and Z errors separately.

Consider the problem of correcting Z errors. If error Z^e occurs for $e \in \mathbb{F}_2^E$ then the syndrome will be $\partial e \in \mathbb{F}_2^V$. Our recovery map will apply Z^r where r is a minimum weight $r \in \mathbb{F}_2^E$ satisfying $\partial r = \partial e$. This is the "maximum-likelihood" decoder and we can find r using Edmond's algorithm for perfect matchings. For convenience, we will sometimes consider e, r to be elements of $\mathbb{F}_2^E$ and sometimes to be subsets of E.

(a) $e+r$ should be a collection of closed loops (why?). For any closed loop c contained in $e + r$ of length ℓ, show that e should contain at least $\ell/2$ of the edges in c. *[Hint: Use the fact that r has minimal weight.]*

(b) Use part (a) to show that for any loop c of length ℓ we have

$$\Pr[c \subseteq e + r] \leq 2^\ell \epsilon^{\ell/2}. \tag{3}$$

(c) Next we would like to count the number of loops of length ℓ. We can upper bound this by the number of length-ℓ paths, which do not have to be closed. Write a formula for the number of paths of length ℓ. It is ok if you overcount paths, say by allowing repeating edges, or saying that paths are distinct if they traverse the same edges in some different order. This should yield an upper bound on the number of loops of the form $c_1 c_2^\ell$.

(d) Combine (b) and (c) to put an upper bound on the probability that $e + r$ will contain a nontrivial loop. Conclude that the probability of failure is

$$\text{poly}(L)(\epsilon/\epsilon_0)^{L/2}, \tag{4}$$

so the probability of logical error goes down exponentially with L once $\epsilon < \epsilon_0$. What is ϵ_0?