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

Assignment 2b(written part)

Posted: Wednesday, Feb 21, 2018
Due: **Friday**, *Mar 9, 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. The online part of the assignment can be found

1. **Combining codes**

   (a) Suppose we have two stabilizer codes S_1 (an $[[n_1, k_1, d_1]]$ code) and S_2 (an $[[n_2, k_2, d_2]]$ code). Suppose S_1 has generators $s_1, \ldots, s_{n_1-k_1}$ and S_2 has generators $t_1, \ldots, t_{n_2-k_2}$. Suppose we take the generators $s_i \otimes I^{\otimes n_2}$ and $I_{\otimes n_1} \otimes t_j$. Show that these generators yield a stabilizer code on $n_1 + n_2$ qubits. Let k and d denote the number of encoded qubits and the distance respectively of this new code. Find k and d in terms of parameters of the original codes. If the original code spaces are C_1 and C_2, then write down a formula for the new code space.

   (b) *Tillich-Zémor product.* Now suppose we have two classical linear codes C_1, C_2 on n_1, n_2 bits with parity check matrices H_1, H_2 of dimensions $k_1 \times n_1$ and $k_2 \times n_2$. Define a CSS code with $n_1^2 + n_2^2$ qubits and check matrices

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

   These are block matrices with $n_2 k_1$ and $n_1 k_2$ rows respectively (corresponding to stabilizers) and each with $n_1 n_2 + k_1 k_2$ columns (corresponding to qubits). Each row r of H_X corresponds to the stabilizer generator X^r while each row r' of H_Z corresponds to the stabilizer generator $Z^{r'}$. Verify that these indeed form a stabilizer group (i.e. that the X and Z generators commute). How many logical qubits are there? (We will not ask you to find the minimum distance of this code; however, the answer is $\min(d_1, d_2, d_1^T, d_2^T)$ where d_1, d_2 are the distances of C_1, C_2 and d_1^T, d_2^T are distances of the classical codes with parity check matrices H_1^T, H_2^T.)

2. **Random stabilizer codes** In this problem we will show that random stabilizer codes achieve high minimum distance. Unlike with the classical linear codes, though, we cannot simply choose random generators, since we need to worry about them commuting. To get around this problem, let U be a uniformly random Clifford unitary on n qubits and consider the code stabilized by $S = \langle U Z_1 U^\dagger, \ldots, U Z_{n-k} U^\dagger \rangle$. You will want to review the union bound from probability and Stirling's approximation for factorials if you are not already familiar with them.

   (a) Let P be a fixed Pauli operator, not equal to the identity. What is the probability that it anticommutes with some element of S? *[Hint: If Q is a fixed non-identity Pauli and U is a uniformly random Clifford unitary then $UQU^\dagger$ is a uniformly random non-identity Pauli.]*

(b) Roughly how many non-identity n-qubit Paulis are there with weight $< d$? Your answer should be of the form $2^{nf(d/n)}$ for some function $f(\cdot)$. Here you should think of d/n as a constant, and you may neglect terms in the exponent that grow more slowly than n.

(c) How large can d be as a function of n and k so that there is still a nonzero chance that a random code of this form will have distance $\geq d$?