QComp Homework 3

Nikolay Kalinin

October 15, 2020

1 Problem 3

1.1 i

When the size of a codeword is n, the number of possible (non-corrupted and corrupted) states for one logical state is $1 + n + \frac{n(n-1)}{2}$. So, $2^n > 2(1 + n + \frac{n(n-1)}{2})$ must hold. We can check that it holds for $n = 5$, but does not hold for $n = 4$. Thus the minimum possible codeword size to allow corrections for double bit-flips is 5.

1.2 ii

For $n = 5$ we can have the codewords be $|\bar{0}\rangle = |00000\rangle$ and $|\bar{1}\rangle = |11111\rangle$. It is clear that a corrupted codeword will have at least three (the majority) correct bits, the other may be flipped. Let's define the operators

$$M_1 = Z_0Z_1, \quad M_2 = Z_1Z_2, \quad M_3 = Z_2Z_3, \quad M_4 = Z_3Z_4.$$

The corruption operators are X_i, and X_iX_j for $i \neq j$. It is clear that each corruption operator has a distinct pattern of commutations and anticommutations with M_i: M_i anticommutes with a corruption operator iff exactly one of X_{i-1}, X_i is contained in the corruption operator. Thus (using the fact that at most two X_i are present) we can distinguish all X_i and correct the codeword.

Here is the commutation table (+ is commutation, − is anticommutation):

corruption operator	Z_0Z_1	Z_1Z_2	Z_2Z_3	Z_3Z_4
I	+	+	+	+
X_0	−	+	+	+
X_1	−	−	+	+
X_2	+	−	−	+
X_3	+	+	−	−
X_4	+	+	+	−
X_0X_1	+	−	+	+
X_1X_2	−	+	−	+
X_2X_3	+	−	+	−
X_3X_4	+	+	−	+
X_0X_2	−	−	−	+
X_1X_3	−	−	−	−
X_2X_4	+	−	−	−
X_0X_3	−	+	−	−
X_1X_4	−	−	+	−
X_0X_4	−	+	+	−