14756: Quantum Error Correction **WS 2018**

Exercise 1 & 2

Tutor: Chae-Yeun Park *Oct. 14*

Excercise 1

Solution to 1.1 Note that each column of G is a codeword. By the definition of H, $HG = 0$.

Solution to 1.2 For $v = \{v_1, \cdots, v_n\}$, Hv can be written as

$$Hv = \sum_{i=1}^{N} h^i v_i \tag{1}$$

where h^i is a i-th column of H. Suppose that there exists $v \neq 0$ that $Hv = 0$ and $wt(v) \leq d - 1$. Let $A \subset \{1, \cdots, N\}$ be a set of indices i such that $v_i \neq 0$. Then $\sum_{i \in A} h^i v_i = 0$ and $|A| = wt(v)$. This is a contradiction to the assumption that any $d-1$ columns of H are linearly independent. Thus, the distance of the code is $\geq d$. On the other hand, let B be a set of indices of d columns of H that are linearly dependent so $\sum_{i \in B} h_i = 0$. Consider a vector $w = \{w_1, \cdots, w_n\}$ that $w_i = 1$ when $i \in B$ and $w_i = 0$ elsewhere then $Hw = 0$ so w is a codeword and $wt(w) = |B| = d$. This shows that the distance of the code is d.

Solution to 1.3 Recall the theorem of the linear algebra that the row rank and the column rank of a matrix are the same. Then $n - k =$ (row-rank of H) $=$ (column rank of H) $\geq (d - 1)$.

Solution to 1.4 We prove the Gilbert-Varshamov bound using a greedy construction. Let $V = (\mathbb{Z}_2)^n$ be the whole vector space and $C_0 = \{0^n\}$ be an initial codespace. At each step i, we find a vector v that is distance $\geq 2t + 1$ from all C_{i-1} and add it to a codespace. As we here consider a linear code, a new codespace is given by $C_i = C_{i-1} \cup \{v + w | w \in C_{i-1}\}$. This procedure terminates when $|\{w | \exists v \in V \text{ such that } d(w, v) \leq 2t\}| \geq |V| = 2^n$ because we can find another such v otherwise. The left hand side is upper bounded by $2^k \mathrm{Vol}(2t)$ where $|C_i| = 2^k$ is the number of codewords and $\mathrm{Vol}(2t) = |\{w | d(0, w) \leq 2t\}|$. Then the proof is straightforward by the following theorem.

Theorem 1 $\mathrm{Vol}(u) \leq 2^{nH(u/n)}$

Proof: First, note that $\mathrm{Vol}(u) = \sum_{i=0}^{u} \binom{n}{i}$. Then the following inequality is obtained:

$$\begin{aligned}
1 &= \big(\frac{u}{n} + (1 - \frac{u}{n})\big)^n && (2)\\
&= \sum_{i=0}^{n} \binom{n}{i} \big(\frac{u}{n}\big)^i \big(1 - \frac{u}{n}\big)^{n-i} && (3)\\
&\geq \sum_{i=0}^{u} \binom{n}{i} \big(\frac{u}{n}\big)^i \big(1 - \frac{u}{n}\big)^{n-i} && (4)\\
&= \sum_{i=0}^{u} \binom{n}{i} \big(1 - \frac{u}{n}\big)^n \big(\frac{u/n}{1 - u/n}\big)^i && (5)\\
&\geq \sum_{i=0}^{u} \binom{n}{i} \big(1 - \frac{u}{n}\big)^n \big(\frac{u/n}{1 - u/n}\big)^u && (6)\\
&= \mathrm{Vol}(u) \big(1 - \frac{u}{n}\big)^{n-u} \big(u/n\big)^u. && (7)
\end{aligned}$$

Eq. 6 is from $\big(\frac{u/n}{1-u/n}\big) \leq 1$ and $u \geq i$ in the summation. The remaining term can be arranged as

$$\big(1 - \frac{u}{n}\big)^{n-u} \big(u/n\big)^u = 2^{(n-u)\log_2(1-u/n) + u\log_2(u/n)} = 2^{-nH(u/n)}$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$. Thus,

$$1 \geq \mathrm{Vol}(u) 2^{-nH(u/n)} \tag{8}$$

and the desired inequality is obtained. ■

Note The proof here is based on that by Gilbert and not restricted to a linear code. Varshamov's proof utilizes the linearity of a code and non-constructive. If you are interested, you may check the Wikipedia page "GV-linear-code".

Exercise 2

Solution The classical repetition code $[n, 1, n]$ has the code distance n so an error up to $\lfloor n/2 \rfloor$ bits can be corrected. This implies that an error $e \in \{0, 1\}^n$ yields a logical error when $wt(e) \geq \lfloor n/2 \rfloor + 1$. Let $wt(e) = l$ then there are $\binom{n}{l}$ different configurations of error and the probability of each configuration is given by $p^l(1-p)^l$. Thus the logical error probability is given as

$$P_{\mathrm{logical}} = \sum_{l=\lfloor n/2 \rfloor + 1}^{n} \binom{n}{l} p^l (1-p)^{n-l}. \tag{9}$$

This is nothing but the tail distribution of the binomial distribution. To obtain an approximated expression, let us define $f(l/n) = \binom{n}{l} p^l (1-p)^{n-l}$. Using the Stirling's formula $\log(n!) \approx n\log n - n$ (note that we here consider the asymptotic limit $n \gg 1$), we can approximate

$$\begin{aligned}
\log \binom{n}{l} &\approx n\Big[-\frac{l}{n}\log\frac{l}{n} - \big(1 - \frac{l}{n}\big)\log\big(1 - \frac{l}{n}\big)\Big] && (10)\\
&= nH(l/n). && (11)
\end{aligned}$$

where we have used $H(x) = -x\log(x) - (1-x)\log(1-x)$ that is also used in the above problem. It is also simple to show that

$$p^l(1-p)^{n-l} = \exp\Big\{n\Big[\frac{l}{n}\log p + \big(1-\frac{l}{n}\big)\log\big(1-p\big)\Big]\Big\}. \tag{12}$$

To sum up,

$$f(l/n) \approx \exp\Big\{n\Big[H(l/n) + \frac{l}{n}\log p + \big(1-\frac{l}{n}\big)\log\big(1-p\big)\Big]\Big\}. \tag{13}$$

Recall that $f(l/n)$ is a binomial distribution centered at $l/n = p$, for $l/n > p$ (which is true by the assumption that $p \le 1/2$) the sum $\sum_{l \ge \lfloor n/2 \rfloor + 1} f(l/n)$ is dominated by the value when $l = \lfloor n/2 \rfloor + 1$ (one may use the central limit theorem). Thus, we obtain

$$\sum_{l > n/2} f(l/n) \approx \exp\Big\{n\Big[H(1/2) + \frac{1}{2}\log p + \frac{1}{2}\log\big(1-p\big)\Big]\Big\}. \tag{14}$$

As $H(1/2) + 1/2\log p + 1/2\log(1-p) < 0$ for $0 \le p < 1/2$, we obtain $P_{\text{logical}} < e^{-\alpha n}$ for $0 \le p < 1/2$. Thus the error threshold is $p = 1/2$.

Note 1 In fact, the Stirling's formula we have used is correct proportionally, i.e. $\log(n!)/(n\log n - n) \to 1$ as $n \to \infty$. And the summation also introduces another error term. When we trace all error terms in the approximation, we obtain extra $o(n)$ term in the exponent. Of course, this does not alter the final result.

Note 2 More simple proof is also possible using the Markov's (or Chebyshev's) inequality. Using this, we obtain $P(X \ge an) = P(e^{\beta X} \ge e^{\beta an}) \le E[e^{\beta X}]/e^{\beta an} = [e^{-a\beta}(1-p+pe^{\beta})]^n$ for all $\beta > 0$. Letting β that minimize the last equality and set $a = 1/2$ yield Eq. (14) in an inequality form.