# TUTORIAL 13

## 1 Homework 10

1. Assume $W$ is such that $\exists x, x' \in \mathcal{X}, \exists y \in \mathcal{Y}, W(y|x) \neq W(y|x')$. Show that $C(W) > 0$.

   ***A:*** *Recall that $C(W) = \max_{P_X} I(X:Y)$, with $P_{XY}(x,y) = P_X(x)W(y|x)$, and that $I(X:Y) = 0$ iff $X$ and $Y$ are independent. It is thus enough to find $P_X(x)$ such that $X$ and $Y$ are not independent.*

   *We have that $P_Y(y) = \sum_{x' \in \mathcal{X}} P_X(x')W(y|x')$, we want to find $x, y$ such that it is different from $P_Y(y|x) = \frac{P_{XY}(x,y)}{P_X(x)} = W(y|x)$ if $P_X(x) \neq 0$. Let us take $P_X(x) = \frac{1}{|\mathcal{X}|}$. Thus, it is enough to find $x, y$ such that $W(y|x) \neq \sum_{x' \in \mathcal{X}} P_X(x')W(y|x') = \frac{1}{|\mathcal{X}|}\sum_{x'} W(y|x')$. Let us fix $y$ given by hypothesis, and take $x = \text{argmax}_x W(y|x)$. Then we have by hypothesis that there exists $x'$ such that $W(y|x) > W(y|x')$, and for all $x''$ we have $W(y|x) \geq W(y|x'')$, so we have $W(y|x) > \frac{1}{|\mathcal{X}|}\sum_{x'} W(y|x')$. Thus $X$ and $Y$ are not independent, so $C(W) \geq I(X:Y) > 0$.*

2. Show that if $C$ corrects $E$, then $\exists D : N \to C$ s.t. $\forall x \in C, \forall y \in N, (x,y) \in E \Rightarrow D(y) = x$.

   ***A:*** *Let us define $D$ in the following way:*

$$D(y) := \begin{cases} x & \text{if } x \in C \text{ such that } (x,y) \in E, \\ x_0 & \text{fixed otherwise.} \end{cases}$$

   *First $D$ is well defined. Indeed if $x, x' \in C$ such that $(x,y), (x',y) \in E$, then since $C$ corrects $E$, we have that $x = x'$. Then $D$ verifies the statement: let $x \in C$ and $y \in N$ such that $(x,y) \in E$, then by definition of $D$ we have that $D(y) = x$.*

## 2 Parity check matrix

Let $C$ be a $[n,k,d]_2$-linear code and $G \in \mathbb{F}_2^{k\times n}$ be a generator matrix. That is, $C = \{xG, x \in \mathbb{F}_2^k\}$. We call a parity check matrix of the code $C$ a matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ such that for all $c \in \mathbb{F}_2^n$ we have $cH^T = 0$ if and only if $c \in C$. The objective of this exercise is to show how to construct a parity check matrix from a generator matrix.

1. Show that $H$ is a parity check matrix if and only if $GH^T = 0$ and $\text{rank}(H) = n - k$.

   ***A:*** *If $H$ is a parity check matrix, then $xGH^T = 0$ for all $x$, so $GH^T = 0$. Moreover, we know that Ker$(H^T) = C$ is of dimension $k$, so $H$ is of rank $n-k$.*

   *Reciprocally, if $GH^T = 0$, then $cH^T = 0$ for all $c \in C$. So $C \subset$ Ker$(H^T)$, but $C$ is of dimension $k$ and Ker$(C)$ is also of dimension $k$, so we have an equality $C =$ Ker$(H^T)$, and $H$ is a parity check matrix of $C$.*

2. Show that, from $G$ we can construct a generator matrix $G'$ of the form $G' = [I_k|P]$ for some $P \in \mathbb{F}_2^{k\times(n-k)}$. (If $n$ is not optimal, we may have to permute the coefficients of the vectors).

   ***A:*** *This is Gaussian elimination (with a permutation of the columns of $G$ if some column is all zero — this is equivalent to permuting the coefficients of the vectors $x$).*

3. Construct a parity check matrix from $G'$.

***A:*** *The matrix $H = [-P^T | I_{n-k}]$ satisfies $GH^T = -P + P = 0$ and is of rank $n-k$. So, $H$ is a parity check matrix.*

4. Construct a parity check matrix of the code given by the generator matrix $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ in $\mathbb{F}_2$.

***A:*** *From question 2, we have an equivalent representation of $G$ as $G' = [I_k | P] = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$*
*So, the matrix $H$ is $H = [-P^T | I_{n-k}] = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$*

## 3 Hamming bound

1. Let $0 \leq p \leq \frac{1}{2}$. Give a formula for $\mathrm{Vol}_2(r, n) = |B_2(0, r)|$ the size of the ball in $\mathbb{F}_2^n$ of radius $r = p \cdot n$ where the distance considered is the Hamming weight.
2. Prove the following bound: for any $(n, k, d)_2$ code $C \subseteq (\Sigma)^n$ with $|\Sigma| = 2$,
$$k \leq n - \log_2 \left( \mathrm{Vol}_2 \left( \frac{d-1}{2}, n \right) \right)$$
3. Define the 2-ary entropy function: $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ defined for $x \in [0, 1]$. Prove that for large enough $n$, we have: $\mathrm{Vol}_2(pn, n) \leq 2^{nH_2(p)}$.

   **Remark.** Using Stirling's approximation, we can show that: $\mathrm{Vol}_2(pn, n) \geq 2^{nH_2(p) - o(n)}$ (exercise!).

## 4 Gilbert-Varshamov bound

1. Let $1 <= d <= n$. Show that there exists a $(n, k, d')_2$-code for some $d' \geq d$, such that
$$k \geq n - \log_2 \left( \mathrm{Vol}_2 \left( d-1, n \right) \right)$$

***A:*** *Greedy algorithm: start with empty $C$ and then as long as it is possible, add a codeword c such that $d(c, C) \geq d$.*
*At the end of the procedure, you have a code such that $\{0,1\}^n \subseteq \bigcup_{c \in C} B_2(c, d-1)$.*
*This gives $2^n \leq \sum_{c \in C} \mathrm{Vol}_2(d-1, n) = |C| \cdot \mathrm{Vol}_2(d-1, n)$.*

## 5 Linear Codes Achieving the Gilbert-Varshamov Bound

The purpose of this exercise is to use the probabilistic method to show that a random linear code lies on the Gilbert-Varshamov bound, with high probability.

1. Given a non-zero vector $\mathbf{m} \in \mathbb{F}_2^k$ and a uniformly random $k \times n$ matrix $\mathbf{G}$ over $\mathbb{F}_2$, show that the vector $\mathbf{mG}$ is uniformly distributed over $\mathbb{F}_2^n$.

*A: As $\mathbf{m} = (m_1, \ldots, m_k)$ is non zero, at least one of the $m_i$ is non zero. Assume without loss of generality that $m_1$ is non zero. Let $\mathbf{x} = (x_1, \ldots, x_n) = \mathbf{mG}$. We have, for all $1 \le i \le n$:*

$$\mathbf{x}_i = \sum_{j=1}^{k} m_j g_{j,i} = m_1 g_{1,i} + c_i$$

*As the $g_{i,j}$ are uniform and independent, the $m_1 g_{1,i}$ are also uniform and independent (because $m_1$ is non zero and then $g \mapsto g m_1$ is a bijection).*

*We write $u_i = m_1 g_{1,i}$ and $\mathbf{u} = (u_1, \ldots, u_n)$.*
*We have that $\mathbf{u}$ is uniform in $\mathbb{F}_q^n$ and then $\mathbf{x} = (\mathbf{u} + (c_1, c_2, \ldots, c_n))$ is also uniform.*

2. Let $k = (1 - H_2(\delta) - \varepsilon)n$, with $\delta = d/n$. Show that there exists a $k \times n$ matrix $\mathbf{G}$ such that

$$\forall \mathbf{m} \in \mathbb{F}_2^k \setminus \{\mathbf{0}\}, |\mathbf{mG}| \ge d$$

*A: Take a uniformly random $k \times n$ matrix $\mathbf{G}$ over $\mathbb{F}_q$. Then thanks to question 1, we have that for any $\mathbf{m} \neq 0$, $\mathbf{mG}$ is a uniformely distributed over $\mathbb{F}_q^n$. In particular:*

$$\mathbf{P}(|\mathbf{mG}| < d) = \frac{\mathrm{Vol}_q(d-1, n)}{q^n}$$

*Using the bound from Exercise 3, this probability is upper bounded by $q^{n(H_q(\delta)-1)}$.*
*By union bound, we have:*

$$\begin{aligned}\mathbf{P}(\exists \mathbf{m} \in \mathbb{F}_q^k \setminus \{0\},\ |\mathbf{mG}| < d) &\le q^k q^{n(H_q(\delta)-1)} \\ &= q^{n(1-H_q(\delta)-\varepsilon)+n(H_q(\delta)-1)} \\ &= q^{-\varepsilon n}\end{aligned}$$

*We have $2^{-\varepsilon n} < 1$ because $q \ge 2$ and $\varepsilon n > 0$.*

*Hence, $\mathbf{P}(\exists \mathbf{m} \in \mathbb{F}_2^k \setminus \{0\},\ |\mathbf{mG}| < d) < 1$. Thus, it means that there exists $\mathbf{G}$ such that for all $\mathbf{m} \neq 0$ we have $|\mathbf{mG}| \ge d$.*

3. Show that $\mathbf{G}$ has full rank (i.e., it has dimension at least $k = (1 - H_2(\delta) - \varepsilon)n$)

*A: We know that for all $\mathbf{m} \in \mathbb{F}_2^k \setminus \{0\}$, we have $|\mathbf{mG}| \ge d$. In particular $\mathbf{mG} \neq 0$. Hence Ker$(\mathbf{G}) = \{0\}$, thus $\mathbf{G}$ has full rank by the rank-nullity theorem.*