TUTORIAL XI

1 Homework 6

1. Let $A_q(n,d)$ be the largest k such that a code over alphabet $\{1,\dots,q\}$ of block length n, dimension k and minimum distance d exists (recall that this corresponds to the notation $(n,k,d)_q$). Determine $A_2(3,d)$ for all positive integers d.

   A: *Notice that the value of $A_2(3,d)$ increases when d decrease:*

   - *For $d>3$: no code with block length 3 has distance >3, so forall $d\geq 4$, we have $A_2(3,d)=0$.*
   - *For $d=3$: the repetition code achieve $k=1$, and one can easily that on the 3-dimensional cube, we can take at most 2 point at distance 3 (opposite corners), hence we have $A_2(3,3)=1$.*
   - *For $d=2$: take the pair of codewords c_1,c_2 that achieve the distance 2. They lie in the same face of the cube, and hence the ball of radius 2 cover exactly 6 points, so we have a upper bound of 4 codewords, ie $k\leq 2$. And this bound is achievable with the following codewords for instance: $000,011,110,101$. We hence have $A_2(3,2)=2$.*
   - *For $d=1$: we can just take the whole 8 points, hence $A_2(3,1)=3$.*

2. Suppose C is a $(n,k,d)_\Sigma$-code. Construct using C a code C' that is a $(n-1,k,d-1)_\Sigma$-code.

   A: *Just drop a bit of all the codewords.*

3. Suppose C is a $(n,k,d)_2$-code with d odd. Construct using C a code C' that is a $(n+1,k,d+1)_2$-code.

   A: *The main idea is that is $\mathbf{x}$ and $\mathbf{y}$ achieve the distance d in the first code, create the corresponding codewords $\mathbf{x}@0$ and $\mathbf{y}@1$ in order to have $\Delta(\mathbf{x}@0,\mathbf{y}@1)=d+1$. The distance with the other codewords can only increase. But of course, we may have several such pairs that achieves the distance d in the given code. We then should do this process for any such pair, but what if we have a triplet $\mathbf{u},\mathbf{x},\mathbf{y}$ such that $\Delta(\mathbf{u},\mathbf{x})=\Delta(\mathbf{u},\mathbf{y})=\Delta(\mathbf{x},\mathbf{y})$? We can't assign an extra-bit to $\mathbf{u},\mathbf{x},\mathbf{y}$ to have the new 3 distances at $d+1$. Well, the fact is that this triplet cannot exist since d is odd! We can thus apply the process without any collision.*

   More formally, we consider the graph with vertices corresponding to codewords that achieve distance d with another codeword. We add an edge uv is $\Delta(u,v)=d$. The claim is that this graph doesn't contain any odd cycle since d is odd. This graph is hence bipartite, we can color it with two color. We set the extra-bit of vertices with color 0 to 0, and the extra-bit of vertices with color 1 to 1. For all the other codewords, we arbitrarily set the extra-bit to 0.

2 Weights of Codewords

Let C be an $[n,k,d]$-linear code over $\mathbb{F}_q$. Prove the following.

1. For $q=2$, either all the codewords have even weight or exactly half have even weight and the rest have odd weight.

   A: *Denote by E the set of codewords of C with even weight, and O the set of codewords with odd weight. If $O=\emptyset$, then $E=C$, ie all codewords have even length. Otherwise, there exists $x_0\in O$. Define the map $\rho:E\to O$ such that $\rho(x)=x+x_0$. Indeed, if x has a even weight, then $x+x_0$ must have an odd weight. Moreover, ρ is an involution, ie $\rho\circ\rho=Id$. Thus, ρ is a bijection and $|E|=|O|$. Since $|C|=|E|+|O|$, we have $|E|=|O|=\frac{|C|}{2}$.*

2. For any q, either all the codewords begin with 0 or exactly a fraction $1/q$ of the codewords begin with 0. In general, for a given position $1 \leq i \leq n$, either all codewords contain 0 at the i-th position or each $\alpha \in \mathbb{F}_q$ appears at the i-th position of exactly $1/q$ of the codewords in C.

A: *Again, we partition the set C into subsets $(C_\alpha)_{\alpha \in \mathbb{F}_q}$, where $x \in C_\beta$ if x start with a β. If all the C_α's for $\alpha \neq 0$ are empty, then $C = C_0$ and we are done. Now, if there exists α such that $x_0 \in C_\alpha$, we consider the map $\rho(x) = x + x_0$. We have $\rho^{-1} = \rho^{q-1}$ and thus ρ is a bijection, hence all the C_β's have the same size. In other words, each $\alpha \in \mathbb{F}_q$ appears at the first position of exactly $1/q$ of the codewords in C.*

3. The following inequality holds for the minimum distance d of C.

$$d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}$$

(Hint: Minimum weight is less than or equal to the average non-zero weight.)

A: *From the previous question, we know that in the i-th position (for a fixed $i \in [1, n]$), each $\alpha \in \mathbb{F}_q$ appears in $1/q$ of the codewords. Since there are q^k codewords, There are exactly q^{k-1} codewords with zero in the i-th position. Consider now, the sum of weights of all codewords. For the i-th position the sum of weights will be precisely $q^k - q^{k-1}$ (counting all the non-zero entries). Taking into account all the n positions, we have $\sum_{c \in C} wt(c) = n(q^k - q^{k-1})$. Since minimum distance is the minimum of the weights of non-zero codewords, it must be at most the average weight of a codeword. That is*

$$d \leq \frac{1}{q^{k-1}} \sum_{c \in C} wt(c) = \frac{n(q-1)q^{k-1}}{q^k - 1}$$

3 Reed-Salomon codes

Consider the Reed-Solomon code over a field $\mathbb{F}_q$ and block length $n = q - 1$ defined as

$$RS[n, k]_q = \{(p(1), p(\alpha), \ldots, p(\alpha^{n-1})) \mid p \in \mathbb{F}_q[X] \text{ has degree } \leq k - 1\}$$

where α is a generator of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$

1. Show that for any $k \in [|1; n-1|]$, we have

$$\sum_{i=0}^{n-1} \alpha^{ki} = 0$$

A: *If k is in $[|1; n-1|]$, we have $\alpha^k \neq 1$, hence:*

$$\begin{aligned} \sum_{i=0}^{n-1} \alpha^{ki} &= \sum_{i=0}^{n-1} (\alpha^k)^i \\ &= \frac{1 - (\alpha^k)^n}{1 - \alpha} \\ &= \frac{1 - 1}{1 - \alpha} \\ \sum_{i=0}^{n-1} \alpha^{ki} &= 0 \end{aligned}$$

2. Prove that

$$RS[n,k]_q \subseteq \left\{ (c_0,\dots,c_{n-1}) \in \mathbb{F}_q^n \mid \forall l \in [|1; n-k|], c(\alpha^l) = 0, \text{ where } c(X) = \sum_{i=0}^{n-1} c_i X^i \right\}$$

A: *Let's first prove that for a given polynomial p of degree $k-1$, the following evaluations are zeros:*

$$\sum_{i=0}^{n-1} p(\alpha^i)(\alpha^l)^i \quad \textit{for} \quad l = 1 \dots n-k$$

We set $p(X) = \sum_{j=0}^{k-1} p_j X^j$ and write:

$$\begin{aligned}
\sum_{i=0}^{n-1} p(\alpha^i)(\alpha^l)^i &= \sum_{i=0}^{n-1}\sum_{j=0}^{k-1} p_j \cdot (\alpha^i)^j \alpha^{il} \\
&= \sum_{j=0}^{k-1} p_j \sum_{i=0}^{n-1} (\alpha^{j+l})^i \\
&= \sum_{j=0}^{k-1} p_j \cdot 0 \\
&= 0
\end{aligned}$$

3. Prove that the following matrix is invertible, and compute its inverse.

$$W(\alpha) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \dots & \alpha^{2n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \dots & \alpha^{(n-1)(n-1)} \end{pmatrix}$$

A: $W(\alpha)^{-1} = \frac{1}{n} W(\alpha^{-1})$.

4. Prove that

$$RS[n,k]_q \supseteq \left\{ (c_0,\dots,c_{n-1}) \in \mathbb{F}_q^n \mid \forall l \in [|1; n-k|], c(\alpha^l) = 0, \text{ where } c(X) = \sum_{i=0}^{n-1} c_i X^i \right\}$$

A: *We now want to prove the converse, ie that for a polynomial c of degree n such that $c(\alpha^l) = 0$, there exists a polynomial p of degree $k-1$ such that $(p(1),\dots,p(\alpha^{n-1})) = (c_0,\dots,c_{n-1})$. We just set the system of equations:*

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{k-1} \\ 1 & \alpha^2 & \dots & \alpha^{2k-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \dots & \alpha^{(k-1)(n-1)} \end{pmatrix} \cdot \begin{pmatrix} p_0 \\ \vdots \\ p_{k-1} \end{pmatrix} = \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

We denote by A the pseudo Vandermonde matrix above, which is a submatrix of the following Vandermonde matrix:

$$W(\alpha) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \dots & \alpha^{2n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \dots & \alpha^{(n-1)(n-1)} \end{pmatrix}$$

We can thus write $W(\alpha) = (A|B)$, where B is a $n \times (n-k)$ matrix. We know that $W(\alpha)$ is invertible and moreover, since $\alpha^n = 1$, the inverse of $W(\alpha)$ is just $C = \frac{1}{n}W(\alpha^{-1})$. We thus multiply our system by C:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \cdot \begin{pmatrix} p_0 \\ \vdots \\ p_{k-1} \end{pmatrix} = C \cdot \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

Now, since C is also a Vandermonde matrix, we have

$$C \cdot \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = \frac{1}{n} \begin{pmatrix} c(1) \\ c(\alpha^{-1}) \\ \vdots \\ c(\alpha^{-(n-2)}) \\ c(\alpha^{-(n-1)}) \end{pmatrix} = \frac{1}{n} \begin{pmatrix} c(1) \\ c(\alpha^n) \\ \vdots \\ c(\alpha^2) \\ c(\alpha) \end{pmatrix}$$

The satisfiability equations are satisfied since $c(\alpha^l) = 0$ for $l = 1 \dots (n-k)$ and the unique solution is hence $p_k = c(\alpha^{n-k+1}), p_{k-1} = c(\alpha(n-k+2), \dots p_0 = c(1)$.