Coding Theory - Homework 3

Kishlaya Jaiswal

October 21, 2019

Exercise 1

Proof. Since f is a boolean function, $f : \mathbb{F}^m \to \mathbb{F}$. Fix $u \in \mathbb{F}^m$, then we have two cases:

- $f(u) = 1$, in which case, we replace 1 by -1 and note that $(-1)^{f(u)} = (-1)^1 = -1 = F(u)$.
- $f(u) = 0$, in which case, we replace 0 by 1 and note that $(-1)^{f(u)} = (-1)^0 = 1 = F(u)$.

Hence, $F(u) = (-1)^{f(u)}$. □

Exercise 2

Proof. F is a row vector whose u^{th} co-ordinate is $F(u)$. Hence

$$(FH)_u = \sum_{v \in \mathbb{F}^m} F_v H_{v,u} = \sum_{v \in \mathbb{F}^m} F(v)(-1)^{v.u} = \sum_{v \in \mathbb{F}^m} (-1)^{u.v + f(v)}$$

Hence, $\tilde{F} = FH$. □

Exercise 3

Proof. We have $H_{u,v} = (-1)^{u.v}$ which is a symmetric Hadamard symmetric matrix of order 2^m. We get,

- $H^t = H$, as H is symmetric
- $H^t H = 2^m I_{2^m}$ as H is Hadamard matrix.

Hence, $H^{-1} = \frac{1}{2^m} H^t = \frac{1}{2^m} H$. Therefore,

$$\tilde{F} = FH \implies F = \frac{1}{2^m} \tilde{F} H \implies F(v) = \frac{1}{2^m} \sum_u \tilde{F}(u) H_{u,v} = \frac{1}{2^m} \sum_u (-1)^{u.v} \tilde{F}(u)$$

□

Exercise 4

Proof. Let $X(u)$ be a row vector whose v^{th} co-ordinate is $f(v) + u.v$.
We observe that,

$$\tilde{F}(u) = \sum_{v \in \mathbb{F}^m} (-1)^{u.v+f(v)} = \sum_{v \in \mathbb{F}^m} (-1)^{X(u)_v} = \sum_{v, X(u)_v = 0} (1) + \sum_{v, X(u)_v = 1} (-1)$$

Hence $\tilde{F}(u) =$ difference between # of zeroes and # of ones in $X(u)$. □

Exercise 5

Proof. Denote by

- α_{00} the number of v for which $f(v) = u.v = 0$
- α_{01} the number of v for which $f(v) = 0$ and $u.v = 1$
- α_{10} the number of v for which $f(v) = 1$ and $u.v = 0$
- α_{11} the number of v for which $f(v) = u.v = 1$

Since this list is exhaustive, we know that $\alpha_{00} + \alpha_{01} + \alpha_{10} + \alpha_{11} = \text{length}(f) = 2^m$.
Next note that, $d(f, u.v) = f - u.v =$ weight of the vector $(f + u.v) = \alpha_{01} + \alpha_{10}$.
As computed above, $\tilde{F}(u)$ is the difference between # of zeroes and # of ones in $X(u) = f + u.v$, so

$$\tilde{F}(u) = \alpha_{00} + \alpha_{11} - \alpha_{01} - \alpha_{10} = \alpha_{00} + \alpha_{11} + \alpha_{01} + \alpha_{10} - 2(\alpha_{01} + \alpha_{10}) = 2^m - 2d(f, u.v)$$

as desired. □

Exercise 6

Proof. We first note that

$$\sum_v (-1)^{u.v+f(v)+1} = -\sum_v (-1)^{u.v+f(v)} = -\tilde{F}(u)$$

Hence, the Walsh transform of $\bar{f} = 1 + f$ is $-\tilde{F}$.
Now let C be the coset of $R(1, m)$ containing f.
Let $x \in C$. Then $x - f \in R(1, m)$. Since $\{\hat{1}, v_0, \ldots v_{m-1}\}$ is a basis for $R(1, m)$, $x = f + c\hat{1} + c_o v_0 + \cdots + c_{m-1} v_{m-1}$.
Here we make a clever observation. When $c_o v_0 + \cdots + c_{m-1} v_{m-1}$ is written in matrix notation as:

$$\begin{pmatrix} c_0 & c_1 & c_2 & \ldots & c_{m-1} \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 & \ldots & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & \ldots & 0 & 0 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 & 1 \end{pmatrix}$$

can be viewed as $(c.v)_{v\in\mathbb{F}^m}$. Hence $c_o v_0 + \cdots + c_{m-1}v_{m-1} = (c.v)_v$.
If $c = 0$ (coefficient of $\hat{1}$ is 0), $x = f + c.v$ and so $wt(x) = d(x, 0) = d(f, c.v) = \frac{1}{2}(2^m - \tilde{F}(c))$ otherwise $c = 1$, $x = \bar{f} + c.v$ and so $wt(x) = d(x, 0) = d(\bar{f}, c.v) = \frac{1}{2}(2^m + \tilde{F}(c))$.
Hence, weight of each word contained in the coset C is

$$\frac{1}{2}(2^m \pm \tilde{F}(u))$$

for $u \in \mathbb{F}^m$. □

Exercise 7

Proof. Let us first consider the number $x(a, b) = 1 + (-1)^a + (-1)^b + (-1)^{a+b+1}$. We shall show that $x(a, b) = \pm 2\ \forall (a, b) \in \mathbb{F}_2^2$.

- $x(0, 0) = 1 + 1 + 1 - 1 = 2$
- $x(0, 1) = 1 + 1 - 1 + 1 = 2$
- $x(1, 0) = 1 - 1 + 1 + 1 = 2$
- $x(1, 1) = 1 - 1 - 1 - 1 = -2$

Let's say $m = 2k$ is an even number. Now to show that $f(v) = v_0v_1 + v_2v_3 + \cdots + v_{2k-2}v_{2k-1}$ is a bent function, we notice the following:

$$\begin{aligned}
\tilde{F}(u) &= \sum_{v\in\mathbb{F}^m} (-1)^{u.v+f(v)} \\
&= \sum_{v} (-1)^{(u_0v_0+\cdots u_mv_m)+(v_0v_1+v_2v_3+\cdots+v_{2k-2}v_{2k-1})} \\
&= \sum_{v} (-1)^{u_0v_0+u_1v_1+v_0v_1} (-1)^{u_2v_2+u_3v_3+v_2v_3} \cdots (-1)^{u_{2k-2}v_{2k-2}+u_{2k-1}v_{2k-1}+v_{2k-2}v_{2k-1}} \\
&= \left(\sum_{(v_0,v_1)\in\mathbb{F}^2} (-1)^{u_0v_0+u_1v_1+v_0v_1} \right) \left(\sum_{(v_2,v_3)\in\mathbb{F}^2} (-1)^{u_2v_2+u_3v_3+v_2v_3} \right) \cdots \\
&\qquad \cdots \left(\sum_{(v_{2k-2},v_{2k-1})\in\mathbb{F}^2} (-1)^{u_{2k-2}v_{2k-2}+u_{2k-1}v_{2k-1}+v_{2k-2}v_{2k-1}} \right)
\end{aligned}$$

But as shown above,

$$\sum_{(v_i,v_j)\in\mathbb{F}^2} (-1)^{u_iv_i+u_jv_j+v_iv_j} = 1 + (-1)^{u_i} + (-1)^{u_j} + (-1)^{u_i+u_j+1} = \pm 2$$

Hence $\tilde{F}(u) = \pm 2^{m/2}$ and so f is a Bent function. □