Homework 3: Monday, 14 October, 2019

Throughout the discussion, m is an even number and $\mathbb{F}$ denotes the field of order 2.

1. For a Boolean function f on $\mathbb{F}^m$ let F be a real vector obtained by replacing 1 by -1 and 0 by 1. Show that $F(u) = (-1)^{f(u)}$.

2. Let $\tilde{F}$ be a real vector given by

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

   Show that as row vectors, we have: $\tilde{F} = FH$ where H is a symmetric Hadamard matrix of order 2^m given by $H_{u,v} = (-1)^{u.v}$.

3. Show that $F = \frac{1}{2^m}\tilde{F}H$ or $F(v) = \frac{1}{2^m}\sum_{u \in \mathbb{F}^m}(-1)^{u.v}\tilde{F}(u)$.

4. Show that $\tilde{F}(u)$ is equal to the difference between the number of 0s and the number of 1s in the binary vector $f + \sum_i u_i v_i$.

5. Show that this implies that

$$\tilde{F}(u) = 2^m - 2d\left(f, \sum_i u_i v_i\right)$$

   or equivalently: $d\left(f, \sum_i u_i v_i\right) = \frac{1}{2}(2^m - \tilde{F}(u))$.

6. Use all the previous results to prove that the weight distribution of the coset of $R(1, m)$ that contains the word f is:

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

   for $u \in \mathbb{F}^m$.

7. Let m be even. A Boolean function f is a Bent function if the coefficients of $\tilde{F}$ are all $\pm 2^{m/2}$. Show that $f(v_0, v_1, v_2, v_3) = v_0 v_1 + v_2 v_3$ is a Bent function.