Fourier For Fun

Ziquan Yang

August 20, 2014

1 Problem

Let $C = \{c = (c_i) \in F_2^{N-1} | \sum_{i=0}^{N-2} c_i \alpha^{ij} = 0, \forall j \not\equiv 0 (mod 3)\}$. Count the number of codewords of weight 3 in C.

2 Prof. Calderbank's solution

Consider $\{0, i, j\}$ to be the support of a codeword of weight 3 in C. In particular α and α^5 are both zeros of the codeword. Denote $x = \alpha^i$ and $y = \alpha^j$ we have

$$\begin{aligned} 1 + x + y &= 0 \\ 1 + x^5 + y^5 &= 0 \\ 1 + x^5 + (1+x)^5 &= 0 \\ x^4 + x &= 0 \end{aligned}$$

Observe that x and y are symmetric, the above calculation shows $x, y \in \mathbb{F}_4$. It is easy to check that this is indeed a codeword. Any other codeword must be a cyclic shift of this codeword, so there are exactly $(N-1)/3$ codewords in C.

3 Fourier Transform Solution

Consider the spectrum of a codeword, we know that $V_j = 0, \forall j \not\equiv 0 (mod 3)$. And we know the linear complexity of the spectrum is at least 3, otherwise the vector will be a zero vector. Now suppose we have a spectrum of linear complexity exactly 3, and let $\Lambda(x) = 1 + \sum_{j=1}^{3} \Lambda_j x^j$ be the connection polynomial. Note that we clearly have $V_j \neq 0, \forall j \equiv 3$ since otherwise the vector will be zero. Apply the definition of connection polynomial to V_1 and V_2 we get $-\Lambda_1 V_0 = 0$ and $-\Lambda_2 V_0 = 0$ implying $\Lambda_1 = 0$ and $\Lambda_2 = 0$. Thus we know $\Lambda_3 = \Lambda_3 V_0$ and $\Lambda_6 = \Lambda_3^2 V_0$. Now apply the conjugacy constraint on the spectrum, we get $(\Lambda_3 V_0)^2 = \Lambda_3^2 V_0$. Since we clearly have $\Lambda_3 \neq 0$ and $V_0 \neq 0$, this shows $V_0 = 1$. Now we see the spectrum must be

$$V_j = \begin{cases} \Lambda_3^{j/3}, & j \equiv 0, \quad \text{mod } 3 \\ 0, & \text{otherwise} \end{cases}$$

Taking $N = 16$ as a example, we see the spectrum must be

$$100\Lambda_3 00\Lambda_3^2 00\Lambda_3^3 00\Lambda_3^4 00$$

Conjugacy constraint is automatically satisfied as long as $(\Lambda_3^4)^2 = \Lambda_3^3$, i.e. $V_{12}^2 = V_9$. This shows $\Lambda_3^5 = 1$. The spectrum is uniquely determined by such Λ_3 and conversely each fifth root of unity will give a spectrum that corresponds to a codeword. Thus there are 5 codewords with weight 3 in C. More generally, consider $N = 2^{2m}$. Let $j \equiv 0, \mod 3$ be such that $2j\%N < j$. The conjugacy constraint will give $\Lambda_3^{(N-1)/3} = 1$. Thus there are exactly $3^{(N-1)/3}$ codewords of weight 3. Additionally, we can apply inverse Fourier transform to see that the codewords look exactly like what has been show in the former method.