NMMB331 - HW1
Jan Oupický

1

We know that a boolean function $g : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is balanced iff $\hat{g}(0) = 0$. Let $g(x) \coloneqq f(x) + f(x+u)$ for some $u \in \mathbb{F}_{2^{2n}}, u \neq 0$. We want to show, that $g(x)$ is balanced:

$$\hat{g}(0) = \sum_{x \in \mathbb{F}_{2^{2n}}} (-1)^{g(x) + \langle x, 0 \rangle} = \sum_{x \in \mathbb{F}_{2^{2n}}} (-1)^{g(x)} = \sum_{x \in \mathbb{F}_{2^{2n}}} (-1)^{f(x) + f(x+u)}$$

Let's see what $f(x)$ and $f(x+u)$ is:

$$f(x) = x_1x_2 + x_3x_4 + \dots x_{2n-1}x_{2n}$$
$$f(x+u) = (x_1+u_1)(x_2+u_2) + (x_3+u_3)(x_4+u_4) + \dots (x_{2n-1}+u_{2n-1})(x_{2n}+u_{2n}) =$$
$$x_1x_2 + x_1u_2 + x_2u_1 + u_1u_2 + \text{same for others}$$

Therefore we can rewrite $f(x+u)$ as $f(x+u) = f(x) + f(u) + \langle x, u' \rangle$ where $u' = (u_2, u_1, u_3, u_4, \dots) \in \mathbb{F}_{2^{2n}}$ and since $u \neq 0$ then $u' \neq 0$. Therefore:

$$\hat{g}(0) = \sum_{x \in \mathbb{F}_{2^{2n}}} (-1)^{f(x)+f(x)+f(u)+\langle x, u' \rangle} = \sum_{x \in \mathbb{F}_{2^{2n}}} (-1)^{f(u)+\langle x, u' \rangle} = (-1)^{f(u)} \sum_{x \in \mathbb{F}_{2^{2n}}} (-1)^{\langle x, u' \rangle}$$

$(-1)^{f(u)}$ is 1 or -1 but the last sum is 0 by annihilator lemma since $u' \neq 0$. Thefore $f(x) + f(x+u)$ is balanced.

Or we can see as above that $g(x)$ is affine and use the rank nullity theorem which says that $\dim(Ker(g)) = 2^n - 1$ and thefore half x map to 0 and the other half must map to 1.

2

a

3

Let's denote $x = \gcd(m,d), y = \gcd(2^m - 1, 2^d - 1)$. We know that $y | 2^m - 1$ and $y | 2^d - 1 \implies 2^m \equiv 1\,(y), 2^n \equiv 1\,(y) \implies ord_{\mathbb{Z}_y}(2) | m, ord_{\mathbb{Z}_y}(2) | d \implies ord_{\mathbb{Z}_y}(2) | \gcd(m,d) = x$. Therefore $2^x \equiv 1\,(y) \iff \gcd(2^m - 1, 2^d - 1) | 2^x - 1$.

Let's denote $x = \gcd(m,d), y = \gcd(2^m - 1, 2^d - 1)$. Assume that $a | 2^m - 1, 2^d - 1 \iff 2^m \equiv 1\,(a), 2^n \equiv 1\,(a) \iff ord_{\mathbb{Z}_a}(2) | m, d \iff ord_{\mathbb{Z}_a}(2) | \gcd(m,d) = x \iff 2^x \equiv 1\,(a)$. There have been equivalences everywhere so we have shown $a | 2^m - 1, 2^d - 1 \iff a | 2^x - 1$. Therefore $2^m - 1, 2^d - 1$ and $2^x - 1$ have the same divisors and ultimately the same greatest one.