

# NMMB331 - HW1

Jan Oupický

## 1

We know that a boolean function  $g : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$  is balanced iff  $\hat{g}(0) = 0$ . Let  $g(x) := f(x) + f(x + u)$  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:

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

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

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

## 2

We are going to be using the same steps as in the proof for  $r = 2^{m-1}$  and  $\text{Supp}_f = \bigcup_{i=1}^r V_i \setminus \{0\}$ . Now we have  $r = 2^{m-1} + 1$  and  $0 \in \text{Supp}_f$ .

We want to prove that  $\forall a \in \mathbb{F}_2^n : \hat{f}(a) = \pm 2^m$ . We can rewrite as follows:

$$\hat{f}(a) = \sum_{x \in \mathbb{F}_2^n} \mu(f(x) + \langle a, x \rangle) = \sum_{x \in \mathbb{F}_2^n} \mu(f(x)) \mu(\langle a, x \rangle) = - \sum_{x \in \text{Supp}_f} \mu(\langle a, x \rangle) + \sum_{x \notin \text{Supp}_f} \mu(\langle a, x \rangle)$$

First let's assume that  $\forall i \in \{1, \dots, r\} : a \notin V_i^\perp$ . That means that using annihilator lemma we calculate the first sum as follows:

$$\begin{aligned} - \sum_{x \in \text{Supp}_f} \mu(\langle a, x \rangle) &= -(\mu(\langle a, 0 \rangle) + \sum_{x \in \text{Supp}_f \setminus \{0\}} \mu(\langle a, x \rangle)) = -(1 + \sum_{i=1}^{2^{m-1}+1} \sum_{x \in V_i \setminus \{0\}} \mu(\langle a, x \rangle)) = \\ &= -(1 + \sum_{i=1}^{2^{m-1}+1} \left( \sum_{x \in V_i} \mu(\langle a, x \rangle) - \mu(\langle a, 0 \rangle) \right)) = -(1 + \sum_{i=1}^{2^{m-1}+1} (0 - 1)) = -(1 - (2^{m-1} + 1)) = 2^{m-1} \end{aligned}$$

Now for the second sum we need to calculate  $|H_a \cap \overline{\text{Supp}_f}|, |\overline{H_a} \cap \overline{\text{Supp}_f}|$  where  $H_a = \{x \in \mathbb{F}_2^n : \langle a, x \rangle = 0\}$ . Then

$$\begin{aligned} \sum_{x \notin \text{Supp}_f} \mu(\langle a, x \rangle) &= \sum_{x \in \overline{\text{Supp}_f}} \mu(\langle a, x \rangle) = \sum_{x \in (\text{Supp}_f \cap H_a)} \mu(\langle a, x \rangle) + \sum_{x \in (\overline{\text{Supp}_f} \cap \overline{H_a})} \mu(\langle a, x \rangle) = \\ &= \sum_{x \in (\text{Supp}_f \cap H_a)} 1 + \sum_{x \in (\overline{\text{Supp}_f} \cap \overline{H_a})} -1 = |H_a \cap \overline{\text{Supp}_f}| - |\overline{H_a} \cap \overline{\text{Supp}_f}| \end{aligned}$$

First:

$$\begin{aligned} |H_a| &= 2^{n-1} = 2^{2m-1} \\ |\text{Supp}_f| &= \left| \left( \bigcup_{i=1}^{2^{m-1}+1} V_i \setminus \{0\} \right) \cup \{0\} \right| = (2^{m-1} + 1)(2^m - 1) + 1 = 2^{2m-1} + 2^{m-1} \end{aligned}$$

The first holds because  $H_a$  because its the kernel of the scalar product which is a linear map with image of dimension 1  $\implies$  dimension of the kernel is  $n - 1$ .

The latter one is because we have  $2^{m-1} + 1$  vector spaces  $V_i$  of dimension  $m$  and the only thing which they have in common is one element (0) so we subtract from each and then add it at the end.

Now we have to compute  $|H_a \cap \text{Supp}_f|$ . We can rewrite it as follows:

$$\begin{aligned} |H_a \cap \text{Supp}_f| &= |H_a \cap \left( \left( \bigcup_{i=1}^{2^{m-1}+1} V_i \setminus \{0\} \right) \cup \{0\} \right)| = |H_a \cap \{0\}| + |H_a \cap (V_1 \setminus \{0\})| + \dots \\ &\quad \dots |H_a \cap (V_r \setminus \{0\})| \end{aligned}$$

$|H_a \cap (V_i \setminus \{0\})|$  means for how many elements of  $x \in (V_i \setminus \{0\})$  holds  $\langle a, x \rangle = 0$ . Similarly as before it holds for half of elements of  $V_i$  (including 0) so its  $2^{m-1} - 1$  (half and subtracted 0) since  $\forall i : a \notin V_i^\perp$ . Therefore:

$$|H_a \cap \text{Supp}_f| = (2^{m-1} + 1)(2^{m-1} - 1) + 1 = 2^{2m-2}$$

Since  $(H_a \cap \text{Supp}_f) \cup (H_a \cap \overline{\text{Supp}_f}) = H_a \cap \mathbb{F}_2^n = H_a$  (and similarly for the other one) we can calculate the rest:

$$\begin{aligned} |H_a \cap \overline{\text{Supp}_f}| &= |H_a| - |H_a \cap \text{Supp}_f| = 2^{2m-1} - 2^{2m-2} = 2^{2m-2} \\ |\overline{H_a} \cap \overline{\text{Supp}_f}| &= |\overline{\text{Supp}_f}| - |H_a \cap \overline{\text{Supp}_f}| = 2^{2m-1} - 2^{m-1} - 2^{2m-2} = 2^{2m-2} - 2^{m-1} \implies \\ \sum_{x \notin \text{Supp}_f} \mu(\langle a, x \rangle) &= 2^{2m-2} - (2^{2m-2} - 2^{m-1}) = 2^{m-1} \implies \hat{f}(a) = 2^{m-1} + 2^{m-1} = 2^m \end{aligned}$$

Now let's assume  $a = 0$ , then as in the other proof:

$$\hat{f}(0) = 2^{2m} - 2|\text{Supp}_f| = 2^{2m} - 2(2^{2m-1} + 2^{m-1}) = 2^{2m} - 2^{2m} - 2^m = -2^m$$

Now let's assume that there exists  $k \in \{1, \dots, r\} : a \in V_k^\perp$ . We claim that then  $\forall i \in \{1, \dots, r\} \setminus \{k\} : a \notin V_i^\perp$ . If that were true, we would have  $i \neq j : a \in V_i^\perp, a \in V_j^\perp$  which would mean that for every  $x \in V_i, y \in V_j \implies \langle a, x \rangle = 0 = \langle a, y \rangle \implies \langle a, x+y \rangle = 0$  but  $V_i + V_j = \mathbb{F}_2^n$  which means that  $\forall z \in \mathbb{F}_2^n : \langle a, z \rangle = 0$  which is a contradiction for  $a \neq 0$ .

Now we will proceed as before expect we will handle  $V_k$  separately. WLOG  $k = 1$ .

$$\begin{aligned}
& - \sum_{x \in \text{Supp}_f} \mu(\langle a, x \rangle) = - \left( \sum_{x \in V_1} \mu(\langle a, x \rangle) + \sum_{i=2}^{2^{m-1}+1} \left( \sum_{x \in V_i \setminus \{0\}} \mu(\langle a, x \rangle) - \mu(\langle a, 0 \rangle) \right) \right) = \\
& -(|V_1| + \sum_{i=1}^{2^{m-1}} \left( \sum_{x \in V_{i+1} \setminus \{0\}} \mu(\langle a, x \rangle) - \mu(\langle a, 0 \rangle) \right)) = -(2^m - 2^{m-1}) = -2^{m-1}
\end{aligned}$$

And similarly for the other sum. We will again calculate the set cardinalities:

$$\begin{aligned}
|H_a \cap \text{Supp}_f| &= |H_a \cap V_1| + |H_a \cap (\text{Supp}_f \setminus V_k)| = 2^m + 2^{m-1}(2^{m-1} - 1) = 2^{2m-2} + 2^{m-1} \\
|H_a \cap \overline{\text{Supp}_f}| &= |H_a| - |H_a \cap \text{Supp}_f| = 2^{2m-1} - (2^{2m-2} + 2^{m-1}) = 2^{2m-2} - 2^{m-1} \\
|\overline{H_a} \cap \overline{\text{Supp}_f}| &= |\overline{\text{Supp}_f}| - |H_a \cap \overline{\text{Supp}_f}| = 2^{2m-1} - 2^{m-1} - (2^{2m-2} - 2^{m-1}) = 2^{2m-2} \implies \\
& \sum_{x \notin \text{Supp}_f} \mu(\langle a, x \rangle) = 2^{2m-2} - 2^{m-1} - 2^{2m-2} = -2^{m-1} \implies \\
& \hat{f}(a) = -2^{m-1} - 2^{m-1} = -2^m
\end{aligned}$$

The proof is now complete.

### 3

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