NMMB331 - HW3

Jan Oupický

1

Let $x \in \mathbb{F}_2^n$. Then

$$\frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n} F_g(u)(-1)^{\langle u,x\rangle} = \frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n} g(y)(-1)^{\langle u,y\rangle}(-1)^{\langle u,x\rangle} =$$

$$\frac{1}{2^n}\sum_{y\in\mathbb{F}_2^n} g(y)\sum_{u\in\mathbb{F}_2^n}(-1)^{\langle u,x+y\rangle}$$

There is exactly one y s.t. $x+y=0 \iff x=y$. Using annihilator lemma we get:

$$\frac{1}{2^n}g(x)2^n + 0 = g(x)$$

$\square$

2

First assume $u=0$.

$$F_f(0) = \sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{\langle 0,x\rangle} = \sum_{x\in\mathbb{F}_2^n} f(x) = \sum_{x\in\mathbb{F}_2^n, f(x)=1} 1$$

$$2^{n-1} - \frac{1}{2}W_f(0) = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_2^n}(1-(-1)^{f(x)})\right) = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_2^n, f(x)=1}(1-(-1))\right) =$$

$$\frac{1}{2}\sum_{x\in\mathbb{F}_2^n, f(x)=1} 2 = F_f(0)$$

Now $u \neq 0$:

$$F_f(u) = \sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{\langle u,x\rangle} = \sum_{x\in\mathbb{F}_2^n, f(x)=0} 0(-1)^{\langle u,x\rangle} + \sum_{x\in\mathbb{F}_2^n, f(x)=1} 1(-1)^{\langle u,x\rangle} =$$

$$\sum_{x\in\mathbb{F}_2^n, f(x)=1}(-1)^{\langle u,x\rangle}$$

$$-\frac{1}{2}W_f(u) = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{\langle u,x\rangle} - W_f(u)\right) = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{\langle u,x\rangle} - (-1)^{f(x)+\langle u,x\rangle}\right) =$$

$$\frac{1}{2}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{\langle u,x\rangle}(1-(-1)^{f(x)}\right) = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_2^n, f(x)=0}(-1)^{\langle u,x\rangle}(1-1)\right) +$$

$$\frac{1}{2}\left(\sum_{x\in\mathbb{F}_2^n, f(x)=1}(-1)^{\langle u,x\rangle}(1-(-1))\right) = 0 + F_f(u) = F_f(u)$$

$\square$

3

$$F_{f\oplus g}(u) = \sum_{x\in\mathbb{F}_2^n}(f\oplus g)(x)(-1)^{\langle u,x\rangle} = \sum_{x\in\mathbb{F}_2^n}(f(x)\oplus g(x))(-1)^{\langle u,x\rangle} =$$
$$\sum_{x\in\mathbb{F}_2^n}(f(x)+g(x)-2f(x)g(x))(-1)^{\langle u,x\rangle} =$$
$$\sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{\langle u,x\rangle} + \sum_{x\in\mathbb{F}_2^n} g(x)(-1)^{\langle u,x\rangle} + \sum_{x\in\mathbb{F}_2^n} 2f(x)g(x)(-1)^{\langle u,x\rangle} =$$
$$F_f(u)+F_g(u)+\sum_{x\in\mathbb{F}_2^n}2(fg)(x)(-1)^{\langle u,x\rangle} = F_f(u)+F_g(u)+F_{2fg}(u)$$

□

4

$$\sum_{u\in\mathbb{F}_2^n}(F_f(u))^2 = \sum_{u\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{\langle u,x\rangle}\right)^2 =$$
$$\sum_{u\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n} f(x)f(y)(-1)^{\langle u,x\rangle}(-1)^{\langle u,y\rangle} =$$
$$\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n} f(x)f(y)\sum_{u\in\mathbb{F}_2^n}(-1)^{\langle u,x+y\rangle}$$

Using annihilator lemma there is again only one y s.t. $x+y=0 \iff x=y$:

$$\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n, y=x} f(x)f(y)2^n = \sum_{x\in\mathbb{F}_2^n} f(x)^2 2^n = 2^n\sum_{x\in\mathbb{F}_2^n} f(x) = 2^n w_t(f)$$

5

$$\frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n}(F_f(v))^2(-1)^{\langle u,v\rangle} = \frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n} f(x)f(y)(-1)^{\langle v,x\rangle}(-1)^{\langle v,y\rangle}(-1)^{\langle u,v\rangle} =$$
$$\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n} f(x)f(y)\sum_{v\in\mathbb{F}_2^n}(-1)^{\langle v,x+y\rangle}(-1)^{\langle u,v\rangle} = \frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n} f(x)f(y)\sum_{v\in\mathbb{F}_2^n}(-1)^{\langle v,x+y+u\rangle}$$

Annihilator lemma $x+y+u=0 \iff y=x+u$:

$$\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n, y=x+u} f(x)f(y)2^n = \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n, y=x+u} f(x)f(y) = \sum_{x\in\mathbb{F}_2^n} f(x)f(x+u) = A_f(u)$$

6

First assume we have $u \in \mathbb{F}_2^n$ and $W_f(v) = 0$ for all $v \in \mathbb{F}_2^n : \langle u, v\rangle = 0$. Let's use the inverse fourier transform on the sum $f(x) + f(x+u)$ for $x \in\in \mathbb{F}_2^n$:

$$f(x) + f(x+u) = \frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n} F_f(v)(-1)^{\langle v,x\rangle} + \frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n} F_f(v)(-1)^{\langle v,x+u\rangle} =$$

$$\frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n} F_f(v)((-1)^{\langle v,x\rangle} + (-1)^{\langle v,x\rangle}(-1)^{\langle v,u\rangle}) = \frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n} F_f(v)(-1)^{\langle v,x\rangle}(1 + (-1)^{\langle v,u\rangle})$$

For v s.t. $\langle u, v\rangle = 1$ the summands are 0, so we can only take into account $v : \langle u, v\rangle = 0$

$$f(x) + f(x+u) = \frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n,\langle u,v\rangle=0} 2F_f(v)(-1)^{\langle v,x\rangle}$$

Since we assume $W_f(v) = 0$ for all $v : \langle u, v\rangle = 0$ then for $v \neq 0$ it implies that $F_f(v) = 0$. So we only consider $v = 0$:

$$f(x) + f(x+u) = \frac{1}{2^{n-1}}F_f(0) = \frac{1}{2^{n-1}}(2^{n-1} - \frac{1}{2}W_f(0)) = \frac{1}{2^{n-1}}(2^{n-1} - 0) = 1$$

This proves the implication.

Now consider there exists $u \in \mathbb{F}_2^n : \forall x \in\in \mathbb{F}_2^n : f(x)+f(x+u) = 1$. This means that f is balanced since for every x there must exist $x+u$ s.t. $f(x) \neq f(x+u)$. If f is balanced we have $wt(f) = 2^{n-1}$ and $W_f(0) = 0$. Also $A_f(u) = 0$ because:

$$A_f(u) = \sum_{x\in\in\mathbb{F}_2^n} f(x)f(x+u) = \sum_{x\in\in\mathbb{F}_2^n} f(x)(1 + f(x)) = 0$$

Let's use previous exercices:

$$0 = A_f(u) = \frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n}(F_f(v))^2(-1)^{\langle u,v\rangle} \implies$$

$$0 = \sum_{v\in\mathbb{F}_2^n}(F_f(v))^2(-1)^{\langle u,v\rangle} = \sum_{v\in\mathbb{F}_2^n,\langle v,u\rangle=0}(F_f(v))^2 - \sum_{v\in\mathbb{F}_2^n,\langle v,u\rangle=1}(F_f(v))^2 =$$

$$\sum_{v\in\mathbb{F}_2^n,\langle v,u\rangle=0}(F_f(v))^2 - \left(2^n wt(f) - \sum_{v\in\mathbb{F}_2^n,\langle v,u\rangle=0}(F_f(v))^2\right) =$$

$$\sum_{v\in\mathbb{F}_2^n,\langle v,u\rangle=0} 2(F_f(v))^2 - 2^n 2^{n-1} = 0 \iff 0 = \sum_{v\in\mathbb{F}_2^n,\langle v,u\rangle=0}(F_f(v))^2 - 2^{2n-2} =$$

$$F_f(0)^2 + \sum_{v\in\mathbb{F}_2^n,v\neq0,\langle v,u\rangle=0}(F_f(v))^2 - 2^{2n-2} = (2^{n-1} - \frac{1}{2}W_f(0))^2 + \sum_{v\in\mathbb{F}_2^n,v\neq0,\langle v,u\rangle=0}(F_f(v))^2 - 2^{2n-2}$$

$$W_f(0) = 0:$$

$$0 = 2^{2n-2} + \sum_{v\in\mathbb{F}_2^n,v\neq0,\langle v,u\rangle=0}(F_f(v))^2 - 2^{2n-2} \iff \sum_{v\in\mathbb{F}_2^n,v\neq0,\langle v,u\rangle=0}(W_f(v))^2 = 0$$

Since all summands are positive the only possibility is that $\forall v \neq 0, \langle u, v\rangle = 0$ it holds that $W_f(v) = 0$. The case left is when $v = 0$. We have actually already proved it since f is balanced $\implies W_f(0) = 0$.