NMMB331 - HW2

Jan Oupický

1

Let's assume $L : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then

$$\mathrm{Im}(L^*)^\perp = \{y \in \mathbb{F}_2^n | \forall x \in \mathrm{Im}(L^*) : \langle x, y\rangle = 0\} = \{y \in \mathbb{F}_2^n | \forall x \in \mathbb{F}_2^m : \langle L^*(x), y\rangle = 0\}$$

From lecture we know that $\forall x, y : \langle L^*(x), y\rangle = \langle x, L(y)\rangle \implies$

$$\mathrm{Im}(L^*)^\perp = \{y \in \mathbb{F}_2^n | \forall x \in \mathbb{F}_2^m : \langle x, L(y)\rangle = 0\}$$

We know that for a fixed $v \in \mathbb{F}_2^m$ if v satisfies $\forall x \in \mathbb{F}_2^m : \langle x, v\rangle = 0$ then $v = \underline{0}$. Using this fact we can see that $\mathrm{Im}(L^*)^\perp$ is exactly those $y \in \mathbb{F}_2^n$ such that $L(y) = 0$. That is the definition of $\mathrm{Ker}(L)$.

2

Let G, F be EA-equivalent vectorial boolean functions i.e.:

$$G = A_1 \circ F \circ A_2 + A_3 \text{ where for } i = 1, 2, 3\text{: } A_i(x) = L_i(x) + b \tag{1}$$

and L_i is a linear permutation. As in the lecture, choose u, v and we will show that $|\hat{G}(u, v)|$ corresponds to $|\hat{F}(a, b)|$ for exactly one pair (a, b). Note that we can write:

$$G(x) = L_1 \circ F(L_2(x) + b_2) + b_1 + L_3(x) + b_3$$

Denote $z = L_2(x) + b_2$ then $x = L_2^{-1}(z - b_2) = L_2^{-1}(z) + L_2^{-1}(b_2)$ (L_2 is a linear permutation).

$$\hat{G}(u, v) = \sum_{x \in \mathbb{F}_2^n} \chi(u \cdot G(x) + v \cdot x) = \sum_{x \in \mathbb{F}_2^n} \chi(u \cdot (L_1 \circ F(z) + b_1 + L_3(x) + b_3) + v \cdot x) =$$

$$\chi(u \cdot (b_1 + b_3)) \sum_{z \in \mathbb{F}_2^n} \chi(u \cdot (L_1 \circ F(z) + L_3 \circ L_2^{-1}(z) + L_3 \circ L_2^{-1}(b_2))) + v \cdot (L_2^{-1}(z) + L_2^{-1}(b_2))) =$$

Denote $c = \chi(u \cdot (b_1 + b_3 + L_3 \circ L_2^{-1}(b_2)) + v \cdot L_2^{-1}(b_2))$. By definition $c = \pm 1$. So we can ommit it.

$$|\hat{G}(u,v)| = \sum_{z \in \mathbb{F}_2^n} \chi(u \cdot (L_1 \circ F(z) + L_3 \circ L_2^{-1}(z)) + v \cdot L_2^{-1}(z)) =$$

$$\sum_{z \in \mathbb{F}_2^n} \chi(u \cdot L_1 \circ F(z) + u \cdot L_3 \circ L_2^{-1}(z) + v \cdot L_2^{-1}(z)) =$$

$$\sum_{z \in \mathbb{F}_2^n} \chi(L_1^*(u) \cdot F(z) + (L_3 \circ L_2^{-1})^*(u) \cdot z + (L_2^{-1})^*(v) \cdot z) =$$

$$\sum_{z \in \mathbb{F}_2^n} \chi(L_1^*(u) \cdot F(z) + ((L_3 \circ L_2^{-1})^*(u) + (L_2^{-1})^*(v)) \cdot z) \implies$$

$$|\hat{G}(u,v)| = |\hat{F}(a,b)| \text{ where}$$
$$a = L_1^*(u)$$
$$b = (L_3 \circ L_2^{-1})^*(u) + (L_2^{-1})^*(v)$$

a, b are determined uniquely since L_is (and equivalently L_i^*s) are permutations.

3

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ vectorial boolean function. Denote $f(x) = \sum\limits_{i=0}^{2^n-1} a_i x^i \in \mathbb{F}_{2^n}[x]$ it's polynomial form.

Since we know that F is a boolean function iff $\forall x \in \mathbb{F}_2^n : F(x) = (F(x))^2$ it must hold that in that case $f(x) = (f(x))^2 \in \mathbb{F}_{2^n}$. Let's expand this equality using the properties of $\mathbb{F}_{2^n}$. For $x, y \in \mathbb{F}_{2^n} : (x+y)^2 = x^2 + y^2$ and $x^{2^n} = x$.

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2^n-1} x^{2^n-1}$$

$$(f(x))^2 = \left(\sum_{i=0}^{2^n-1} a_i x^i \right)^2 = \sum_{i=0}^{2^n-1} a_i^2 x^{2i} \implies$$

$$(f(x))^2 = a_0^2 + a_1^2 x^2 + a_2^2 x^4 + \cdots + a_{\frac{2^n-2}{2}}^2 x^{2^n-2} + a_{\frac{2^n-2}{2}+1}^2 x^{2^n} + \cdots + a_{2^n-1}^2 x^{2(2^n-1)}$$

Since $x^{2^n} = x$ the coefficients a_i with $2^n > i > \frac{2^n-2}{2}$ are coefficients at some x^j where j is odd and $j < 2^n$. Therefore rewritten:

$$(f(x))^2 = a_0^2 + a_{\frac{2^n-2}{2}+1}^2 x + a_1^2 x^2 + \cdots + a_{\frac{2^n-2}{2}}^2 x^{2^n-2} + a_{2^n-1}^2 x^{2^n-1}$$

And we need that $f(x) = (f(x))^2$ so we compare coefficients at x^i this gives us $a_0^2 = a_0$ and $a_{2^n-1}^2 = a_{2^n-1}$. The only elements of $\mathbb{F}_{2^n}$ for which this holds are $0, 1$ therefore it must be that $a_0, a_{2^n-1} \in \mathbb{F}_2 \subseteq \mathbb{F}_{2^n}$. We have also conditions on the rest of the coefficients a_i where $1 \le i \le 2^n - 2$. One way to write it is that $1 \le i \le 2^n - 2 : a_i^2 = a_{2i \bmod 2^n-1}$.

Every polynomial with coefficients that fulfill these conditions must correspond to a vectorial boolean function that $\forall x : F(x)^2 = F(x)$ and this means that F can be considered a boolean function since it "outputs"only elements of the subfield $\mathbb{F}_2 \subseteq \mathbb{F}_{2^n}$.