Value distributions of perfect nonlinear functions

Lukas Kölsch

University of South Florida

(joint work with Sasha Polujan)

Perfect nonlinear functions

Definition

Let $F \colon G \to H$ be a function between finite abelian groups G, H. We say F is perfect nonlinear if

$$|\{x \in G \colon F(x+a) - F(x) = b\}| = \frac{|G|}{|H|}$$

for all $a \in G \setminus \{0\}$ and $b \in H$.

F is also called *bent* - these are the functions that are "as far away" from homomorphisms as possible.

Perfect nonlinear functions - Connections

Cryptography: add non-linearity - studied in symmetric cryptography

Combinatorics: Constructions of designs, (partial) difference sets, ...

Theorem (Dillon)

A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is perfect nonlinear if and only if it is the characteristic function of a difference set. The difference set has parameters $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$.

Coding theory: Many constructions. Connections to designs via the Assmus-Mattson theorem. Rank-metric codes.

Finite Geometry: Perfect nonlinear functions with $G = H = \mathbb{F}_p^n$ (planar functions) can be used to construct (non-desarguesian) projective planes.

Question

We investigate value distributions. What are the possible image set sizes and preimage set sizes of perfect nonlinear functions?

Previous results for Boolean functions (e.g. Nyberg, 1995), planar functions (e.g. Kyureghyan, Pott, 2008; Weng, Zeng, 2012; Coulter, Senger, 2013)

Goal

Develop a general framework for value distributions of perfect nonlinear functions that includes previous results as special cases, and gives new insights.

A preliminary result

Proposition (KP)

Let $F\colon G \to H$ be a perfect nonlinear function. Then the following holds

$$\sum_{\beta \in H} |F^{-1}(\beta)|^2 = |G| + \frac{|G|}{|H|}(|G|-1).$$

Proof.

We have $\sum_{\beta \in H} |F^{-1}(\beta)|^2 = |\{(x,y) \in G \times G \colon F(x) = F(y)\}|$.

$$|\{(x,y) \in G \times G \colon F(x) = F(y)\}| = |\{(x,a) \in G \times G \colon F(x) = F(x+a)\}|.$$

$F(x) = F(x+a)$ holds for a fixed value $a \neq 0$ for exactly $|G|/|H|$ values of x. □

A derived equation

Proposition (KP)

Let $F\colon G \to H$ be a perfect nonlinear function. Then the following holds

$$\sum_{\beta \in H} |F^{-1}(\beta)|^2 = |G| + \frac{|G|}{|H|}(|G|-1).$$

Let $X_1, \ldots, X_{|H|} \in \mathbb{N}_0$ be the preimage set sizes of F.

$$\sum_{i=1}^{|H|} X_i^2 = |G| + \frac{|G|}{|H|}(|G|-1), \tag{1}$$

$$\sum_{i=1}^{|H|} X_i = |G|. \tag{2}$$

For some small values of $|H|$ already strong conditions!

Bounds on preimage set sizes

Theorem (KP)

Let $F\colon G \to H$ be a perfect nonlinear function. Then for all $\beta \in H$:

$$\frac{|G|}{|H|} - \sqrt{|G|} + \frac{\sqrt{|G|}}{|H|} \leq |F^{-1}(\beta)| \leq \frac{|G|}{|H|} + \sqrt{|G|} - \frac{\sqrt{|G|}}{|H|}.$$

1. If $|F^{-1}(\alpha)| = \frac{|G|}{|H|} - \sqrt{|G|} + \frac{\sqrt{|G|}}{|H|}$ then $|F^{-1}(\beta)| = \frac{|G|}{|H|} + \frac{\sqrt{|G|}}{|H|}$ for each $\beta \neq \alpha$.

2. If $|F^{-1}(\alpha)| = \frac{|G|}{|H|} + \sqrt{|G|} - \frac{\sqrt{|G|}}{|H|}$ then $|F^{-1}(\beta)| = \frac{|G|}{|H|} - \frac{\sqrt{|G|}}{|H|}$ for each $\beta \neq \alpha$.

We call the two boundary cases *almost balanced*.

Almost balanced functions

It turns out almost all classic constructions of perfect nonlinear function are almost balanced!

For the classical setting $G = \mathbb{F}_p^n$, $H = \mathbb{F}_p^m$, we have the following result:

Theorem (KP)

Almost balanced perfect nonlinear functions $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ of both types exist for all $m \leq n/2$, where $n \in \mathbb{N}$ is an arbitrary even number and p is an arbitrary prime number.

Proof.

Primary constructions (Maiorana-McFarland, monomials) yield almost balanced functions, and the direct sum secondary construction preserves the almost balanced condition and can be used to cover all remaining cases. □

Question

Are almost balanced perfect nonlinear functions rare or not? Are all perfect nonlinear functions $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ with n even and $m \leq n/2$ (equivalent to) an almost balanced perfect nonlinear function?

$p = 2$, $m = 1$: Every perfect nonlinear function is almost balanced (folklore)

Question

Are almost balanced perfect nonlinear functions rare or not? Are all perfect nonlinear functions $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ with n even and $m \leq n/2$ (equivalent to) an almost balanced perfect nonlinear function?

$p = 2$, $m = 1$: Every perfect nonlinear function is almost balanced (folklore)

$p = 2$, $m = 2$: Every perfect nonlinear function is almost balanced (KP, 2023+)

Question

Are almost balanced perfect nonlinear functions rare or not? Are all perfect nonlinear functions $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ with n even and $m \leq n/2$ (equivalent to) an almost balanced perfect nonlinear function?

$p = 2$, $m = 1$: Every perfect nonlinear function is almost balanced (folklore)

$p = 2$, $m = 2$: Every perfect nonlinear function is almost balanced (KP, 2023+)

Higher values of m?

Theorem (KP)

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ *be a perfect nonlinear function. Then, the preimage set sizes are* $X_i = 2^{n-m} + 2^{n/2-m}(2T_i - 1)$ *for all* $i \in \{1, \ldots, 2^m\}$ *where the* T_i *are integers satisfying the two equations*

$$\sum_{i=1}^{2^m} T_i^2 = 2^{2m-2}$$
$$\sum_{i=1}^{2^m} T_i = 2^{m-1}.$$

(Actually a more general result exists for odd primes).

Proof uses discrete Fourier transform.

The discrete Fourier transform

Definition

Let $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$. The Fourier transform $\mathcal{F}$ of F is

$$\mathcal{F}_F(b) = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{\langle b, F(x) \rangle_m}, \quad \text{where } \zeta_p = e^{2\pi i/p} \quad \text{and } i^2 = -1.$$

Theorem

If F is perfect nonlinear then $|\mathcal{F}_F(b)| = p^{n/2}$ for all non-zero b.

We have

$$\sum_{b\in\mathbb{F}_{2^m}} \mathcal{F}_F(b) = \sum_{x\in\mathbb{F}_{2^n}} \sum_{b\in\mathbb{F}_{2^m}} (-1)^{\langle b,F(x)\rangle_m} = 2^m \cdot |\{x \in \mathbb{F}_{2^n} \colon F(x) = 0\}|.$$

Counting another way, we also have

$$\sum_{b\in\mathbb{F}_{2^m}} \mathcal{F}_F(b) = 2^n + \sum_{b\in\mathbb{F}_{2^m}^*} \mathcal{F}(b) = 2^n + 2^{n/2}\left(k - (2^m - 1 - k)\right),$$

where $k = |\{b \in \mathbb{F}_{2^m}^* \colon \mathcal{F}_F(b) = 2^{n/2}\}|$. So

$$|\{x \in \mathbb{F}_{2^n} \colon F(x) = 0\}| = 2^{n-m} - 2^{n/2} + 2^{n/2-m}\left(2k+1\right).$$

The preimage of 0 is "not special", so we get the same result for all preimages.

Theorem (KP)

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a perfect nonlinear function. Then, the preimage set sizes are $X_i = 2^{n-m} + 2^{n/2-m}(2T_i - 1)$ for all $i \in \{1, \dots, 2^m\}$ where the T_i are integers satisfying the two equations

$$\sum_{i=1}^{2^m} T_i^2 = 2^{2m-2}$$
$$\sum_{i=1}^{2^m} T_i = 2^{m-1}.$$

Proof.

Major ingredients:

Fourier transform ideas from the previous slides.

The 2 integer equations (1) and (2) from earlier. □

In particular, the new equations *only* rely on m, not on n!

$m = 3$

Theorem (KP)

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^3$ be a perfect nonlinear function. Then there are only four possible preimage distributions which are the 2 almost balanced distributions, and the distributions with preimage set sizes $X_i = 2^{n-3} + 2^{n/2-3}(2T_i - 1)$ where

$$T_1 = -2, T_2 = T_3 = T_4 = 2, T_5 = \cdots = T_8 = 0, \textit{ or}$$

$$T_1 = 3, T_2 = T_3 = T_4 = -1, T_5 = \cdots = T_8 = 1.$$

For $n = 6$, we are able to find examples with all 4 possible value distributions.

Proof: Derive extra conditions using the discrete Fourier transform, then solve the 2 equations from earlier with a computer.

$m = 4$

Theorem (KP)

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^4$ be a perfect nonlinear function. Then there are exactly 14 possible preimage distributions.

For $n = 8$, we are able to find examples with all 14 possible value distributions.

Proof: Derive even more extra conditions using the discrete Fourier transform, then solve the 2 equations from earlier with a better computer.

Results in the other direction

Knowing preimage set sizes can sometimes force a function to be perfect nonlinear:

Theorem (KP)

Let $F \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a plateaued function. If F is almost balanced then F is perfect nonlinear.

Further connections between the Fourier transform and image sets

Almost balanced perfect nonlinear functions always have specific Fourier transforms.

Theorem (KP)

Let $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be an almost balanced perfect nonlinear function. Then

$$\mathcal{F}_F(b) = p^{n/2} \text{ or } \mathcal{F}_F(b) = -p^{n/2}$$

for any $b \neq 0$.

Summarizing..

Only a few preimage set distributions can occur.

Many constructions yield *almost balanced* functions.

These have some special properties!

But also other perfect nonlinear functions exist where things are less clear.

Open problems

For $G = \mathbb{F}_2^n$, $H = \mathbb{F}_2^m$, $m \geq 3$, there are perfect nonlinear functions F that are not almost balanced. However, is it true that all perfect nonlinear functions are *equivalent to* an almost balanced functions, i.e. is there an additive function L such that $F + L$ is almost balanced?

Preliminary computer experiments seem to confirm this at least for $m = 3, 4$ - general case unclear though.

Thank you for your attention!

The talk is based on a paper available on the arXiv:

Kölsch, L., Polujan, A.: Value distributions of perfect nonlinear functions