Sidon sets in $\mathbb{F}_2^n$ and the vectorial nonlinearity

Gábor P. Nagy
Budapest University of Technology and Economics
and University of Szeged (Hungary)

The study of the nonlinear properties of vectorial Boolean functions is fundamental for the evaluation of the resistance of the block cipher against the main attacks, such as the differential attack and the linear attack. The main metrics of the nonlinear properties are the *differential uniformity* δ_f (the lower is the less linear), the *nonlinearity* $\mathrm{NL}_1(f)$, and the *vectorial nonlinearity* $\mathrm{NL}_{\boldsymbol{v}}(f)$. The vectorial nonlinearity of $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is defined as the Hamming distance of f to the set of affine $\mathbb{F}_2^n \to \mathbb{F}_2^m$ maps. These measures are linked by the lower bounds

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq \mathrm{NL}_1(f), \qquad \mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{\delta_f} \cdot 2^{n/2} - \frac{1}{2}.$$

that hold for all $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Liu, Mesnager and Chen (2017) conjectured the upper bound

$$\mathrm{NL}_{\boldsymbol{v}}(f) \leq \left(1 - 2^{-m}\right)\left(2^n - 2^{\frac{n}{2}}\right).$$

The computation of the vectorial nonlinearity $\mathrm{NL}_{\boldsymbol{v}}(f)$ is generally difficult. Our goal is to better understand the vectorial nonlinearity by applying the theory of Sidon sets of $\mathbb{F}_2^n$. The subset S of the abelian group A is a *Sidon set* in A, if for any $x, y, z, w \in S$ of which at least three are different, $x + y \neq z + w$. We will use old and new results on Sidon sets to improve the estimates for the vectorial nonlinearity of APN functions.

References

1. L. Babai and V. T. Sós. Sidon sets in groups and induced subgraphs of Cayley graphs. In: European J. Combin. 6.2 (1985), pp. 101–114.

2. J. Liu, S. Mesnager, and L. Chen. On the nonlinearity of S-boxes and linear codes. In: Cryptogr. Commun. 9.3 (2017), pp. 345–361.

3. C. Carlet and S. Mesnager. On those multiplicative subgroups of $\mathbb{F}_{2^n}^*$ which are Sidon sets and/or sum-free sets. In: J. Algebraic Combin. 55.1 (2022), pp. 43–59.

4. G. P. Nagy. Thin Sidon sets and the nonlinearity of vectorial Boolean functions. arXiv preprint arXiv:2212.05887 (2022).