On large Sidon sets

Ingo Czerwinski[(1)], Alexander Pott[(1)]

[(1)] Otto von Guericke University Magdeburg, Germany

A (binary) Sidon set M is a subset of $\mathbb{F}_2^t$ such that the sum of four distinct elements of M is never 0. The goal is to find Sidon sets of large size. In this talk we show that the graphs of almost perfect nonlinear (APN) functions with high linearity can be used to construct large Sidon sets. Thanks to recently constructed APN functions $[[1, 2]]\mathbb{F}_2^8 \to \mathbb{F}_2^8$ with high linearity, we can construct Sidon sets of size 192 in $\mathbb{F}_2^{15}$, where the largest sets so far had size 152. This result will be published in the Journal of Combinatorial Theory (A).

References

[1] Beierle, Christof and Leander, Gregor and Perrin, Léo, Trims and extensions of quadratic APN functions, *Designs, Codes and Cryptography* 2022 pp.1009-1036.

[2] Beierle, Christof and Leander, Gregor, New Instances of Quadratic APN Functions, *IEEE Transactions on Information Theory* 2020 pp. 670-678.