On the completeness of Sidon sets obtained from affine conics

Gábor P. Nagy

University of Szeged (Hungary)

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, $x + y \neq z + w$. The subset S is *t-thin Sidon,* if for all $a \in A \backslash \{0\}$, $|S \cap (a + S)| \leqslant t$. In the elementary abelian 2-group $A = \mathbb{F}_2^n$, S is Sidon if and only if it is 2-thin Sidon. For the size of a t-thin Sidon set we have the trivial upper bound

$$|S| \leqslant \sqrt{t} \cdot 2^{n/2} + \frac{1}{2}. \tag{1}$$

Even for the case $t = 2$, that is, for Sidon sets, it is not known how sharp the trivial upper bound is. Except for the value $n = 11$, all known Sidon sets of $\mathbb{F}_2^n$ have size less than or equal to $2^{n/2} + 2$. In $\mathbb{F}_2^{11}$, the largest known Sidon set has size $48 > 2^{n/2} + 2 \approx 47.25$. If n is odd and at least 15, then the largest known Sidon sets have sizes

$$\frac{1}{\sqrt{2}} 2^{n/2} + O(2^{n/4}).$$

Therefore, the gap between the lower and upper bounds on the size of a Sidon set is large, in particular if n is odd. This problem is related to a conjecture by Liu, Mesnager, and Chen from 2017 on the Hamming distance of vectorial Boolean functions to affine functions. If the Liu-Mesnager-Chen Conjecture is true, then for all n, APN functions on $\mathbb{F}_2^n$ would yield a Sidon sets of size $2^{n/2} + 1$ in $\mathbb{F}_2^n$.

A Sidon set is *complete,* if it is not contained in a larger Sidon set. In this talk, we present a class of complete Sidon sets of size $2^{n/2} + 2$ for $n \equiv 0 \pmod 4$.