Skew Hadamard difference sets from commutative semifields and symplectic spreads

Qing Xiang

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716, USA
xiang@math.udel.edu

Let G be a finite group of order v (written multiplicatively). A k-element subset D of G is called a (v, k, λ) *difference set* if the list of "differences" xy^{-1}, $x, y \in D$, $x \neq y$, represents each nonidentity element of G exactly λ times. Let q be a prime power congruent to 3 modulo 4. The set of nonzero squares of GF(q) is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$ difference set in $(\mathrm{GF}(q), +)$. This construction dates back to 1933, and it is due to Paley. The difference sets coming from this construction are usually called *Paley difference sets*.

A difference set D in a finite group G is called *skew Hadamard* if G is the disjoint union of D, $D^{(-1)}$, and $\{1\}$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$. The Paley difference sets provide a family of examples of skew Hadamard difference sets. For more than 70 years, these are the only known examples in abelian groups. It was conjectured that no further examples in abelian groups can be found. This conjecture was disproved by Ding and Yuan in 2005. Subsequently, we found another construction using certain permutation polynomials from the Ree-Tits slice symplectic spreads in $\mathrm{PG}(3, 3^{2h+1})$. In this talk, we will discuss these developments and raise several questions about skew Hadamard difference sets.