Weil Sums of Binomials and Helleseth's Conjecture

Daniel J. Katz
Department of Mathematics
California State University, Northridge, USA

We are interested in Weil sums of binomials of the form

$$W_{k,d}(a) = \sum_{x \in k} \psi(x^d + ax),$$

where k is a finite field of characteristic p, ψ is the canonical additive character of k, and the exponent d is relatively prime to $|k^*|$ and nondegenerate, that is, not a power of p modulo $|k^*|$. Fix q and d and consider the set of values obtained as a runs through k^*. The value set is of interest in many areas of pure and applied math: counting zeroes of polynomials over finite fields, cryptography, remote sensing, and communications networks. At least three distinct values must appear, and we discuss recent results about the case where precisely three appear.

One conjecture about three-valued Weil sums that has been attacked repeatedly in the past two decades was posed by Helleseth in 1976. The conjecture states that it is impossible for $W_{k,d}$ to be three-valued if k is obtained from the prime field $\mathbf{F}_p$ via a tower of quadratic extensions, that is, if $[k : \mathbf{F}_p]$ is a power of 2. We sketch the history of the proof of the conjecture when $p = 2$, beginning with the foundations laid by Calderbank-McGuire-Poonen-Rubinstein (1996), the critical insight of Feng (2012), and our final step which completed the proof. We show how an additional insight proves the conjecture when $p = 3$. Then we discuss partial results, obtained jointly with Yves Aubry and Philippe Langevin, for $p \geq 5$.