PETR LISONEK, Simon Fraser University
Maximally non-associative quasigroups

A quasigroup $(Q, \cdot)$ is an algebraic structure whose multiplication table is a Latin square. We say that $(x, y, z) \in Q^3$ is an associative triple if $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Quasigroups with few associative triples were proposed for various applications in cryptography. Let $a(Q)$ denote the number of associative triples in Q. It is easy to show that $a(Q) \geq |Q|$. In 2012 Grošek and Horák conjectured that $a(Q) = |Q|$ never occurs. Let us call Q maximally non-associative if $a(Q) = |Q|$. The first example of a maximally non-associative quasigroup (of order 9) was found by Drápal and Valent (J. Combin. Des. 2018). In this work we use nearfields and their associated sharply two-transitive groups to construct maximally non-associative quasigroups. We conjecture that any nearfield that is not a field produces examples. We report results of an extensive and successful computer search. When q is an odd prime power, we show that a non-constructive existence result for maximally non-associative quasigroups of order q^2 can be obtained if certain character sums can be suitably bounded. This is joint work with Aleš Drápal (Charles University, Prague).