Eric Rains
UC Davis

Bounds on self-dual codes and lattices

ABSTRACT

A number of particularly interesting low-dimensional codes and lattices have the extra property of being equal to (or, for lattices, similar to) their duals; as a result, it is natural to wonder to what extent self-duality constrains the minimum distance of such a code or lattice. The first significant result in this direction was that of Mallows and Sloane, who showed that a *doubly-even* self-dual binary code of length n has minimum distance at most 4[n/24] + 4, and with Odlyzko, obtained an analogous result for lattices. Without the extra evenness assumption, they obtained a much weaker bound; in fact, as I will show, this gap between singly-even and doubly-even codes is illusory: the bound 4[n/24] + 4 holds for essentially all self-dual binary codes. For asymptotic bounds, the best result for doubly-even binary codes is that of Krasikov and Litsyn, who showed d <= D n+o(n) where $D = (1-5^{-1/4})/2$ 0.165629. I'll discuss a different proof of their bound, applicable to other types of codes and lattices, in particular showing that for any positive constant c, there are only finitely many self-dual binary codes satisfying d >= D n-c $n^{1/2}$.