Linear and additive codes: theory and applications Abstract

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

Our first application is from theoretical computer science: the **reduction of the construction problem of $\epsilon-$biased arrays (probability spaces, random variables) and $\epsilon-$ dependent arrays to the efficient construction of good codes.** Algebraic-geometric codes provide an asymptotically optimal solution for one variant of the problem. However, as it may not be that easy to efficiently handle AG-codes like those high up in the tower of Artin-Schreier extensions as constructed by Garcia-Stichtenoth it will be a good idea to squeeze the utmost out of classical families related to the projective line and to Hermitian curves. We concentrate on genus 0, and hence on the derivates of Reed-Solomon codes.

Starting point is a **simplified approach to the theory of cyclic codes.** This leads to a generalization in a natural way: **Twisted BCH-codes** generalize cyclic codes from the **linear** to the **additive** (not necessarily linear) case. This family was introduced independently by McEliece, Hattori and G.Solomon (**Reed-Solomon subspace codes**). We sketch a **new approach to the theory of twisted codes.**

One application consists in an explicit construction of families of **quantum codes** in arbitrary characteristic.

The new approach enables us to completely eliminate use of the general theory in some important parametric cases. We obtain **an explicit de-**

scription of a family of additive codes, which via concatenation and lengthening yield a 3-parameter family of linear 2-weight codes.

Another simplification is based on an explicit and rather elementary projection construction due to C.L.Chen. He applied the construction to classical caps (ovals, ovoids) in characteristic 2 . The resulting additive codes with minimum distance 4 have been used in computer memory systems.

Application of Chen projection to Reed-Solomon codes yields a large family

of additive codes, which contains the codes proposed by the Caltech/JPL-people for use in deep-space communication. The original description relied on the theory of Reed-Solomon subspace codes.