Symmetries of Codes

Abstract

The project concerns good linear codes with "sufficiently nice" automorphism groups, their constructions under various useful definitions and their applications in cryptography and in theory of computation. We review some relevant coding theory background before we discuss the project. The required background for the project is basic algebra.

1 Some Coding Theory Background

Linear codes enable reliable communication over a noisy channel. The key idea here is that by expanding the information of interest into a codeword, this information can still be recovered even if some symbols of the codeword have been modified. This process is called *error-correction* or *decoding*. Major practical applications are found in satellite communication and in dvd technology, for instance.

Throughout, let K be a finite field and let n be a positive integer. A K-linear code of *length* n is a subspace C of the n-dimensional K-vector space K^n. The code is "good" for the purpose of error-correction if both its *dimension* [1] $\dim_K C$ *and* its *minimum distance* [2] $d_{\min}(C)$ are a "large fraction" of the length. In practice, it is often the case that the field K, the *alphabet*, is *fixed*; a typical choice is $K = \mathbb{F}_2$, the binary field.

The point is that the *Hamming-spheres* [3] $B_H(x,t)$ with $x \in C$ and $t := \lfloor (d_{\min}(C) - 1)/2 \rfloor$ are pairwise disjoint. [4] Define $k := \dim_K C$. Fixing an (injective) *encoding*, i.e., a K-vector space morphism $K^k \longrightarrow K^n$ whose image equals C, a vector $m \in K^k$ describing the information of interest is encoded into the corresponding vector $x \in C$. If an error-vector $e \in K^n$ with $w_H(e) \leq t$ is added to x, then x – and hence m – can

[1] its dimension as a K-vector space

[2] the minimum distance of a linear code of *positive* dimension is the minimum of the *Hamming-distance* between vectors x, y taken over all $x, y \in C$ with $x \neq y$. The Hamming-distance $d_H(x,y)$ between two vectors $x, y \in K^n$ is the *Hamming weight* of the vector $x - y$, i.e., the number of nonzero coordinates among the in total n coordinates of $x - y \in K^n$ (where coordinates are in the standard basis). The Hamming-weight gives a metric on K^n. Since C is linear, $d_{\min}(C)$ equals the minimum of $w_H(x)$ taken over all $x \in C$ with $x \neq 0$.

[3] the set of vectors in K^n at distance at most the given radius from its given centre. Note that its *volume*, i.e., the cardinality of this set, only depends on the radius.

[4] This picture of *sphere-packing* immediately makes it clear that dimension and minimum distance are "mutually opposing": a lower bound on one implies an upper bound on the other.

in principle be decoded uniquely from just $x' := x + e$. Generally, further structural properties of a code are required to enable *efficient* decoding.

With the finite field K *fixed*, a family $\{C_n\}_{n\in\mathcal{I}}$ of K-linear codes C_n of length $n \in \mathcal{I}$, where $\mathcal{I} \subset \mathbb{Z}_{>0}$ and $|\mathcal{I}| = \infty$, is *asymptotically good* if there exist $\delta, \kappa \in \mathbb{R}_{>0}$ such that, for each $n \in \mathcal{I}$, it holds that $(\dim C_n)/n \geq \kappa$ (*information rate*) and $(d_{\min}(C_n))/n \geq \delta$ (*relative minimum distance*). For each finite field K, good codes exist in this sense. This way, the information of interest is encoded over a constant-size alphabet, it is unbounded in length, its expansion into a codeword incurs just a constant multiplicative factor of overhead in length, and, finally, a positive constant fraction of errors is tolerated.

More precisely, let $p, m \in \mathbb{Z}_{>0}$ with p prime and define $q = p^m$. Let $\mathbb{F}_q$ denote the finite field of order q. For each $\delta \in \mathbb{R}$ with $0 < \delta \leq 1 - 1/q$, define

$$H_q(\delta) = \lim_{n\to\infty} \frac{\log_q V_q(n, \lfloor \delta n \rfloor)}{n},$$

where $V_q(n, \cdot)$ denotes the volume of a Hamming-sphere in $\mathbb{F}_q^n$ with radius as given. This limit is well-defined. In fact, for all $\delta \in \mathbb{R}$ with $0 < \delta \leq 1 - 1/q$, it holds that

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta),$$

the *q-entropy function*. Also define $H_q(0) = 0$. It is elementary to show that, for each $\delta \in \mathbb{R}$ with $0 < \delta < 1 - 1/q$ and for each $\epsilon \in \mathbb{R}_{>0}$, there exists a family of $\mathbb{F}_q$-linear codes such that the relative minimum distance is at least δ and the information rate is at least $1 - H_q(\delta) - \epsilon$ (*Asymptotic Gilbert-Varshamov Bound*). As $1 - H_q(\delta) > 0$ if $0 < \delta < 1 - 1/q$, this means particularly that asymptotically good codes exist. For more information, see e.g. [3]. Using methods from algebraic geometry, the bound above can be improved, for instance whenever $q \geq 49$ is a square or $q \geq 7^3$ is a cube. In each case, the improvement holds in a restricted range of δ.

2 The Project

There are many applications of linear codes besides error correction, in particular in cryptography and theory of computation. Often, dimension and minimum distance are the crucial attributes of codes. This project focuses on application of codes in which *additional* properties play a central role as well.

An example from cryptography is *arithmetic secret sharing* (see Ch. 11 in [1]). In the latter case, one considers attributes of "the code itself" *in conjunction* with attributes of certain codes associated with it, such as its *dual* [5] and some of its *powers*. [6] For instance, for the purpose of arithmetic secret sharing, an infinite family of K-linear codes C may

[5] The dual of a K-linear code $C \subset K^n$ is the K-linear code $C^\perp \subset K^n$ defined by the "orthogonal complement" of C, taken with respect to the standard inner product on K^n.

[6] For instance, the *square* $C^{*2} \subset K^n$ of a K-linear code $C \subset K^n$ is the K-linear span of all vectors of the form $(x_1y_1, \ldots, x_ny_n) \in K^n$, with $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in C$.

be called "asymptotically good" if C, its dual $C^{\perp}$ *and* its square C^{*2} are asymptotically good. Interestingly, the only existence proofs so far are algebraic geometric in nature.

Recent developments in cryptography and in theory of computation have brought yet another attribute of a code into (renewed) focus: its *symmetries*. Let S_n denote the symmetric group of permutations on the set of integers $\{1, \ldots, n\}$. This group acts in a natural way on K^n : if $\sigma \in S_n$ and $x := (x_1, \ldots, x_n) \in K^n$, then $\sigma \cdot x := (x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in K^n$. The *automorphism group* $\mathrm{Aut}(C)$ of a K-linear code $C \subset K^n$ is the group of permutations in S_n that map C to itself, i.e., the group consisting of all $\sigma \in S_n$ such that $\sigma \cdot x \in C$ for all $x \in C$.

The code $C \in K^n$ is *cyclic* if $\mathrm{Aut}(C)$ contains the group generated by the cycle $(1\,2 \ldots n) \in S_n$ of order n (the "cyclic shift") as a subgroup. Alternatively, C corresponds to an ideal in the group-algebra $K[G_n]$, where G_n is the cyclic group of order n (see [2, 3]). It is an open problem whether asymptotically good cyclic codes exist. However, under a slight relaxation of the notion they do. This gives rise to interesting applications. One possible direction for the project is to study this relaxation, constructions and applications, as well as certain alternatives. Another possibility concerns good linear codes C such that $\mathrm{Aut}(C)$ contains a subgroup G acting *2-transitively* [7] (or "almost" so). Good codes with this property appear to be rare, but there are very interesting applications. There exists an elementary construction and one that exploits the function field of a Hermitian curve. This presents another possible direction for the project. Several concrete questions will be addressed in the lecture.

Supervisor: Ronald Cramer

References

[1] R. Cramer, I. Damgård, J. Nielsen. *Secure Multiparty Computation and Secret Sharing - An Information Theoretic Appoach*. Book draft (May 11, 2013) available from `http://cs.au.dk/ jbn/mpc-book.pdf`. Final version to be published by Cambridge University Press, 2014.

[2] S. Lang. *Algebra*. Springer GTM. Revised Third Edition, 2002.

[3] J. H. van Lint. *Introduction to Coding Theory*. Springer GTM. Third Edition, 1999.

[7] for each $i, i', j, j' \in \{1, \ldots, n\}$ with $i \neq j$, $i' \neq j'$, there exists $\sigma \in G$ such that $\sigma(i) = i'$ and $\sigma(j) = j'$.