Extension of Good Linear Codes

Axel Kohnert
Ischia June 2006

Bayreuth University Germany
axel.kohnert@uni-bayreuth.de
http://linearcodes.uni-bayreuth.de
A linear \([n, k; q]\) code \(C\) is a \(k\)–dimensional subspace \(< GF(q)^n\).

The codewords are the vectors of the subspace \(C\).

All codewords are of length \(n\), the letters are from the alphabet \(GF(q)\).
A generator matrix $\Gamma$ of a linear $[n, k; q]$ code $C$ is a $k \times n$ matrix where each row is a basis element of the code $C$.

$$C = \{v\Gamma : v \in GF(q)^k\}$$

Encoding is easy, just multiplication by the generator matrix.
Minimum Distance

Error correction capability of $C$ is measured by the minimum distance $d$. Computation of the minimum distance is easy for a linear code, it is the minimum weight of all codewords.
Minimum Weight Generator

We are interested in the codewords \( \{c_1, \ldots, c_s\} \) of minimum weight.

The vectors \( \{v_1, \ldots, v_s\} \in GF(q)^k \) with:

\[
v_i \Gamma = c_i
\]

are called the minimum weight generator.
Good Codes

We speak of a good code, if it is a linear code which has the highest known minimum distance $d$, for fixed $n, k, q$.

There are tables available for the highest known minimum distance.
Best Codes

typical situation, same $d$ for several $n$
We try to build new good (or even better) codes having minimum distance $d + 1$ and larger length $n + l$ using known good codes of length $n$ and minimum distance $d$. We only look at the minimum weight codewords as all other nonzero codewords are of weight $\geq d + 1$. 

\textit{l—Extension}
We try to find \( l \) new columns, which we add to the generator matrix.

For each vector \( v \) in the minimum weight generator there must be at least one new column \( \gamma \) such that \( \langle v, \gamma \rangle \neq 0 \).

This crucial property can be formulated using an intersection matrix.
Intersection Matrix

\[ \gamma \in GF(q)^k \]

\[ \downarrow \]

\[ M = \begin{bmatrix} M_{\nu,\gamma} \end{bmatrix} \quad \leftarrow \nu \in \text{Minimum weight generator} \]

\[ M_{\nu,\gamma} = \begin{cases} 0 & \langle \nu, \gamma \rangle = 0 \\ 1 & \langle \nu, \gamma \rangle \neq 0 \end{cases} \]
We try to find $l$ columns of the intersection matrix, such that their sum is a vector with no zero entries. This is equivalent to a solution of the following Diophantine system of inequalities/equation:
Diophantine System of Equations

We are interested in a $0/1$ solution $x = (x_1, \ldots, x_{q^k-1})$ of the system

\[
\begin{array}{c|c|c|c}
M & x & \geq 1 & \geq 1 \\
1 \ldots 1 & \vdots & \vdots & \\
1 \ldots 1 & & = l \\
\end{array}
\]

**Theorem:** There is $[n + l, k; q]$ code with minimum distance $> d \iff$ there is a solution of the above Diophantine system.
The matrix $M$ is part (selection of rows) of the incidence matrix of the finite projective geometry $PG(k - 1, q)$.

The property of being an $l$–extension can be formulated in the language of finite projective geometry.
For example we found a new $[n = 82, k = 8, d = 49; q = 3]$ code, which is $2$—extension of a previously computed good $[80, 8, 48; 3]$ code with 1320 codewords of minimum weight. Among all possible pairs we found a covering pair.

This new code can 2 times be extended using $1$—extension, giving also new $[83, 8, 50; 3]$ and $[84, 8, 51; 3]$ codes. For the last one we apply again $2$—extension and afterwards $1$—extension and get new $[86, 8, 53; 3]$ and $[87, 9, 54; 3]$ codes.
Other newly found codes using \$l\$–extension are:

\[ [130, 8, 79; 3] \]

\[ [187, 6, 135; 4], [197, 6, 142; 4], [212, 6, 153; 4], [227, 6, 165; 4], [232, 6, 169; 4], [242, 6, 177; 4], [247, 6, 181; 4] \]

\[ [191, 7, 134; 4], [192, 7, 135; 4] \]

here we do not list the derived codes. All these codes are improvements of Brouwers table.
Thank you very much for your attention.

- A. Wassermann: Talk at Combinatorics 2004
- list of new codes including generator matrix and weight enumerator:
  http://linearcodes.uni-bayreuth.de
- A. E. Brouwer has a list of good codes:
  http://www.win.tue.nl/~aeb/