Construction of Binary and Ternary Self-Orthogonal Linear Codes

Axel Kohnert

Mathematical Department, University of Bayreuth, D-95440 Bayreuth, Germany

Alfred Wassermann [*]

Mathematical Department, University of Bayreuth, D-95440 Bayreuth, Germany

Abstract

We construct new binary and ternary self-orthogonal linear codes. In order to do this we use an equivalence between the existence of a self-orthogonal linear code over a prime field with a prescribed minimum distance and the existence of a solution of a certain system of Diophantine linear equations. To reduce the size of the system of equations we restrict the search for solutions to solutions with special symmetry given by matrix groups. Using this method we found at least 6 new distance-optimal codes, which are all self-orthogonal.

Key words: self-orthogonal linear code, incidence matrix, group of automorphisms, lattice point enumeration
1991 MSC: 94B05, 94B65

1 Introduction

A self-orthogonal linear $[n, k]$-code is a k-dimensional subspace of the n-dimensional vector space $GF(q)^n$ over the finite field $GF(q)$ with the additional requirement that $C \subseteq C^{\perp}$. Here, we restrict the finite field to $GF(2)$ and $GF(3)$.

The q^k codewords of length n are the elements of the subspace, they are written as row vectors. The Hamming weight $wt(c)$ of a codeword c is defined to be

[*] Corresponding author
Email addresses: axel.kohnert@uni-bayreuth.de (Axel Kohnert), alfred.wassermann@uni-bayreuth.de (Alfred Wassermann).

the number of nonzero entries of c, the minimum distance $dist(C)$ of a code C is the minimum of all weights of the nonzero codewords in C. A $[n,k]-$code of minimum distance d, is called a $[n,k,d]$-code.

For fixed dimension k one is interested in codes with high minimum distance d as these allow the correction of $\lfloor (d-1)/2 \rfloor$ errors. On the other hand one is interested in codes of small redundancy, i.e. in codes of small length n. A linear $[n,k]$-code C is called optimal if there is no linear $[n,k,dist(C)+1]$-code. We could construct self-orthogonal codes whose parameters improve the known bounds for general linear codes in several cases.

In Section 2 we characterize for parameters n,k,d the $[n,k,d]$-codes as solutions of a system of Diophantine linear equations. In Section 3 additional equations are added to this system in order to restrict the search to self-orthogonal codes. Then, in Section 4 we further restrict the search to codes with a prescribed group of automorphisms to reduce the size of the linear system. In Section 5 the problem of solving the system of Diophantine linear equations is transferred to the problem of finding certain vectors in a lattice. Finally, Section 6 contains the results of the computer search.

2 Linear Codes with Prescribed Minimum Distance

If Γ denotes a generator matrix of a q-ary $[n,k]$-code C then the code is given by the set $C = \{v \cdot \Gamma \mid v \in GF(q)^k\}$. If $v \cdot w := \sum_i v_i \cdot w_i$ is the standard inner product and if γ_j indicates the jth column of the generator matrix Γ, then each codeword $v \cdot \Gamma$ can be written as

$$v \cdot \Gamma = (v \cdot \gamma_0, \ldots, v \cdot \gamma_{n-1})$$

It is clear that the codewords $v \cdot \Gamma$ and $\lambda \cdot v \cdot \Gamma$, where $v \in GF(q)^k$ and $\lambda \in GF(q)^*$, are codewords that have the same weight. Let Σ_v be the numbers of columns u of the generator matrix for which $v \cdot u = 0$. Then the codeword $v\Gamma$ has weight d' if and only if $\Sigma_v = n - d'$.

Let Ω be a set of representatives of the set of subspaces of dimension 1, i. e. $\Omega := \{\langle v \rangle \mid v \in GF(q)^k \setminus \{0\}\}$. From now on we will simply use the notation $v \in \Omega$ instead of $\langle v \rangle \in \Omega$. Then Γ is a generator matrix of a $[n,k,d]$-code over $GF(q)$ if and only if

$$max\{\Sigma_v \mid v \in \Omega\} = n - d.$$

This observation leads us to the following theorem which shows the equivalence between the construction of codes with a prescribed minimum distance and solving a system of Diophantine linear equations.

Let $M_{k,q} = (m_{v,w})$ be the $|\Omega| \times |\Omega|$ matrix whose rows resp. columns correspond to the elements of Ω. The entry $m_{v,w}$, corresponding to row v and column w, is defined by

$$m_{v,w} := \begin{cases} 1 \text{ if } v \cdot w = 0 \\ 0 \text{ otherwise.} \end{cases}$$

Theorem 1 *[3] There is a q-ary $[n, k, d']$-code with minimum distance $d' \geq d$ if and only if there is a vector $x \in \mathbb{Z}^{|\Omega|}$ and a vector $y \in \mathbb{Z}^{|\Omega|}$ satisfying $0 \leq x_i \leq n$, respectively $0 \leq y_i \leq n - d$, $0 \leq i < |\Omega|$, and*

$$(M_{k,q}| - I) \cdot \begin{pmatrix} x \\ \hline y \end{pmatrix} = 0 \quad \text{and} \quad \sum_{v \in \Omega} x_v = n, \tag{1}$$

where I is the identity matrix.

$M_{k,q}$ is the point-hyperplane incidence matrix of the finite projective geometry $PG(k-1, q)$. The number $m = (q^k - 1)/(q-1)$ of rows and columns of $M_{k,q}$ is the limiting factor of this approach, since solving the system of Diophantine linear equations is only possible for small values of m. Therefore we apply a well-known method, also described in [2,3], to shrink the matrix $M_{k,q}$ to a much smaller on $M_{k,q}^G$ by prescribing a subgroup G of the general linear group $GL(k, q)$. This approach will be described in Section 4.

3 Self-Orthogonality

For an $[n, k]$-code C the dual code $C^\perp$ is defined as

$$C^\perp = \{w \in GF(q)^n \mid w \cdot c = 0 \text{ for all } c \in C\}.$$

$C^\perp$ is an $[n, n-k]$-code. If $C \subseteq C^\perp$ the code C is called self-orthogonal, if $C = C^\perp$ the code C is called self-dual. That means, a code C is self-orthogonal if and only if

$$v \cdot w = 0 \quad \text{for all } v, w \in C\,.$$

It is known that if Γ is a generator matrix of C and $\gamma^{(0)}, \gamma^{(1)}, \ldots, \gamma^{(k-1)}$ are the rows of Γ then C is self-orthogonal if and only if

$$\gamma^{(i)} \cdot \gamma^{(j)} = \sum_{0 \leq s < n} \gamma_s^{(i)} \cdot \gamma_s^{(j)} = 0 \quad \text{for all } 0 \leq i \leq j < k.$$

These are $\binom{k+1}{2}$ equations over $GF(q)$. As we saw in the previous section, each column of $M_{k,q}$ corresponds to a possible column $v \in \Omega$ of a generator matrix

Γ. With the notation of (1) and $v^{(i)}$ denoting the i-th entry of the column vector v, the additional equations over $GF(q)$ can therefore be written as

$$\sum_{v\in\Omega} x_v(v^{(i)} \cdot v^{(j)}) = 0 \quad \text{for } 0 \le i \le j < k. \tag{2}$$

These equations guarantee, that the row products of a generator matrix Γ built from the columns of Ω are all zero. Combining this with the result from the previous section we get the following theorem.

Theorem 2 *Let $q \in \{2,3\}$. There exists a q-ary self-orthogonal $[n,k,d']$-code with minimum distance $d' \ge d$ if and only if there is a vector $x \in \mathbb{Z}^{|\Omega|}$ and a vector $y \in \mathbb{Z}^{|\Omega|}$, where $0 \le x_i \le n$, respectively $0 \le y_i \le n-d$, $0 \le i < |\Omega|$, satisfying the system of equations*

$$(M_{k,q}| - I) \cdot \begin{pmatrix} x \\ \hline y \end{pmatrix} = 0 \quad \textit{and} \quad P_{k,q} \cdot x \equiv 0 \bmod q \quad \textit{and} \quad \sum_{v\in\Omega} x_v = n,$$

where the $(\binom{k+1}{2} \times |\Omega|)$-matrix $P_{k,q} = (p_{(i,j),v})$ is defined by

$$p_{(i,j),v} \equiv v^{(i)} \cdot v^{(j)} \bmod q,$$

for $0 \le i \le j < k$ and $v \in \Omega$.

In general, for codes over GF(q) with $q \notin \{2,3\}$ self-orthogonality is not preserved by projective equivalence. In that case the existence of a solution vector in the above theorem is a sufficient, but not a necessary condition for the existence of a self-orthogonal code with the prescribed parameters.

The condition "$= 0$" from (2) has to be translated from a condition in $GF(q)$ to a condition over $\mathbb{Z}$. For prime fields the translation is obvious. We remark that the translation is also possible for non-prime fields.

4 Codes with Prescribed Automorphisms

A linear code C with generator matrix Γ has a corresponding multiset $\hat{\Gamma}$ of 1-dimensional subspaces of $GF(q)^k$ by taking the spaces generated by the columns of Γ. We say Γ has $G \le GL(k,q)$ as a group of projective automorphisms if the action of G leaves $\hat{\Gamma}$ invariant. This works as a definition of an automorphism group of the code C, as taking a different generator matrix Γ' gives a conjugated subgroup G' of G as group of projective automorphisms of Γ' [2].

Let G be a subgroup of $GL(k,q)$, let $\omega_0, \dots, \omega_{m-1}$ be the orbits of G on the 1-subspaces of $GF(q)^k$ and let $\Omega_0, \dots, \Omega_{m-1}$ be the orbits of G on the set of $(k-1)$-subspaces with representatives $K_i \in \Omega_i$. Let $M^G_{k,q} = (m^G_{i,j})$ be the $m \times m$ matrix with entries

$$m^G_{i,j} := |\{T \in \omega_j \mid T \subseteq K_i\}|, \quad 0 \le i, j < m\,.$$

Further, let $P^G_{k,q} = (p^G_{(i,j),s})$ be the $\binom{k+1}{2} \times m$ matrix with entries

$$p^G_{(i,j),s} \equiv \sum_{v \in \omega_s} v^{(i)} \cdot v^{(j)} \bmod q, \quad 0 \le i \le j < k, 0 \le s < m.$$

With this notation we can formulate the construction theorem for self-orthogonal linear codes with a prescribed group of automorphisms.

Theorem 3 *Let $q \in \{2,3\}$. There is a q-ary self-orthogonal $[n,k,d']$-code with minimum distance $d' \ge d$ such that a generator matrix of this code has G as a subgroup of the group of automorphisms if and only if there is a vector $x \in \mathbb{Z}^m$ with $x_i \in \{0, \dots, \lfloor n/|\omega_i| \rfloor\}$, $0 \le i < m$, a vector $y \in \mathbb{Z}^m$ with $y_i \in \{0, \dots, n-d\}$, $0 \le i < m$, and a vector $z \in \mathbb{Z}^{\binom{k+1}{2}}$ satisfying*

$$\left(\begin{array}{ccc|c|c} & M^G_{k,q} & & -I & 0 \\ \hline & P^G_{k,q} & & 0 & -q \cdot I \\ \hline |\omega_0| & \dots & |\omega_{m-1}| & 0 & 0 \end{array}\right) \cdot \left(\begin{array}{c} x \\ \hline y \\ \hline z \end{array}\right) = \left(\begin{array}{c} 0 \\ \hline 0 \\ \hline n \end{array}\right), \tag{3}$$

where I is the identity matrix.

Note that in the above system of equations the integer variables z_i, $0 \le i < i\binom{k+1}{2}$ are implicitly bounded by the restrictions on the vector x and y.

As for Theorem 2, in the case of $q \notin \{2,3\}$ the above condition is sufficient but not necessary.

5 Solving Systems of Diophantine Linear Equations

It is well known that finding solutions of the above system of Diophantine linear equations is an NP-hard problem. Here, we try to find solutions with lattice point enumeration [9]. The linear system is transferred into the problem of finding certain small vectors in a lattice. The search for these vectors is done with lattice basis reduction followed by exhaustive enumeration.

The system (3) of equations consists of $3m$ columns and $m + 1 + \binom{k+1}{2}$ rows. The upper bounds on the variables x_i, $0 \le i \le m-1$, are $\lfloor n/|\omega_i| \rfloor$, the upper bounds on the variables y_i, $0 \le i \le m-1$, are $n-d$.

In general, finding solutions for this system can be formulated as the following integer programming problem:

> Let n and m be positive integers and A be an $m \times n$ integer matrix and $c \in \mathbb{Z}^m$. Further, let $r \in \mathbb{N}^n$ be a vector of upper bounds. Does there exist a vector $x \in \mathbb{Z}^n$ such that
>
> $$A \cdot x = c \quad \text{and} \quad 0 \le x \le r\,? \tag{4}$$

Our algorithm to solve the problem (4) for arbitrary values of $r \in \mathbb{N}^n$ consists of two steps. First, we compute a basis consisting of integer vectors $b^{(1)}, b^{(2)}, \ldots, b^{(n-m+1)}$ of the extended homogeneous system, i. e. the negative of the right hand side vector is appended as column 0 to the left hand side matrix A in (4):

$$\underbrace{\left(\begin{array}{c|c} & \\ -c & A \\ & \end{array}\right)}_{=:\,A'} \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = 0\,. \tag{5}$$

Since we can assume that the extended matrix A' has full row-rank m, the kernel of the system (5) has dimension $n-m+1$.

We can assume that there are no obviously fixed variables and no obvious contradictions, i. e. we can at least assume that $0 < r_i \in \mathbb{N}$ for $1 \le i \le n$. The basis of the lattice consists of the columns of the following $(m+n+1) \times (n+1)$-matrix (see [10]):

$$\left(\begin{array}{c|cccc} -N \cdot d & & N \cdot A & & \\ \hline -r_{\max} & 2s_1 & 0 & \cdots & 0 \\ -r_{\max} & 0 & 2s_2 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ -r_{\max} & 0 & \cdots & \cdots & 2s_n \\ \hline r_{\max} & 0 & \cdots & \cdots & 0 \end{array}\right)$$

where $N \in \mathbb{N}$ is a large constant and

$$r_{\max} = \operatorname{lcm}\{r_1, \ldots, r_n\} \quad \text{and} \quad s_i = \frac{r_{\max}}{r_i}\,, \quad 1 \le i \le n\,.$$

If N is large enough, see [1], the reduced basis will consist of $n-m+1$ vectors with only zeroes in the first m rows and m vectors which contain at least one nonzero entry in the first m rows. The latter vectors can be removed from the basis. From the remaining $n-m+1$ vectors we can delete the first m rows which contain only zeroes. This gives a basis $b^{(1)}, b^{(2)}, \ldots, b^{(n-m+1)} \in \mathbb{Z}^{n+1}$ of the kernel of (5). In the second step of the algorithm all integer linear combinations of the basis vectors $b^{(1)}, b^{(2)}, \ldots, b^{(n-m+1)} \in \mathbb{Z}^{n+1}$ which correspond to solutions of the problem (4) are enumerated. Since we are only interested in non-homogeneous solutions of (5) we can demand that $x_0 = 1$ in (5).

Theorem 4 *Let*

$$v = u_1 \cdot b^{(1)} + u_2 \cdot b^{(2)} + \ldots + u_{n-m+1} \cdot b^{(n-m+1)}$$

be an integer linear combination of the basis vectors with $v_0 = r_{\max}$*. Then* v *is a solution of the system (4) if and only if*

$$v \in \mathbb{Z}^{n+1} \text{ where } -r_{\max} \leq v_i \leq r_{\max},\ 1 \leq i \leq n\ .$$

The exhaustive enumeration is done with the backtracking algorithm of Ritter [8], see also [2,9,10] for a detailed description. After finding the first solution of (4) the enumeration is stopped.

6 Results

In this section we present the parameters of all linear codes we constructed with the proposed method and which are improvements of the bounds (for general linear codes) in [6]. We restricted ourself to the binary and ternary case.

We are not aware of tables of bounds for self-orthogonal codes. A complete list of the best parameters of the codes we could construct, together with generator matrices and the group of automorphisms used, are available at [4].

Parameters of new optimal codes:

$[177, 10, 84]_2$ $[38, 7, 21]_3$ $[191, 6, 126]_3$

$[202, 6, 132]_3$ $[219, 6, 144]_3$ $[60, 7, 36]_3$

Parameters of codes which are improvements to the bounds in [6] but which are not optimal codes:

$[175, 10, 82]_2$ $[140, 11, 64]_2$ $[61, 7, 36]_3$

$[188, 7, 120]_3$ $[243, 7, 156]_3$

The computation was done on a 2GHz PC with 1GB main memory. To construct the systems of equations we directly use the definitions given in section (4). The time needed to do this is small compared to the time needed to solve the corresponding system of Diophantine equations. The computation times depend heavily on the number of orbits and the number $n - d$ which is the upper bound of parts of the variables. Also the number $\binom{k}{2}$ of equations to ensure self-orthogonal solutions comes into play. All this is shown in the following table which gives detailed information for the 6 optimal codes:

code	# orbits	time	$n - d$	$\binom{k}{2}$
$[177, 10, 84]_2$	51	$< 3h$	93	45
$[38, 7, 21]_3$	101	$< 100s$	17	21
$[60, 7, 36]_3$	67	$< 100s$	24	21
$[202, 6, 132]_3$	44	$< 10s$	70	15
$[219, 6, 144]_3$	38	$< 10s$	75	15
$[191, 6, 126]_3$	44	$< 10s$	65	15

One further problem is to choose a group such that the reduction is large enough to get a system which can be handled by the algorithm, but on the other hand which is also a group of automorphisms of a self-orthogonal code with high minimum distance. We experimented with several subgroups of $GL(k, q)$. For more details see [5] where we described the situation in the more general case of arbitrary linear codes with prescribed automorphisms. In the case of self-orthogonal codes we noticed that the cyclic groups (i.e. only one generator) were especially good. So for example in the case of $q = 2$ and $k = 9$ all the distance-optimal self-orthogonal codes were found by using cyclic groups.

In most cases it was possible to find self-orthogonal codes, which meet the minimum weight of the best known linear codes. Of course this is possible only in the case of even weight (in the binary case) and weight d with $d \equiv 0$ mod 3 (in the ternary case). This situation is shown in the following table for the case $q = 2$ and $k = 9$. It lists the length n and minimum distance d of all self-orthogonal codes which could be constructed with the above method and whose minimum distance is as least as high as the best known codes in [6]. An entry $30 - 33$ means that codes of length $30, 31, 32$, and 33 could be constructed.

n	d	n	d	n	d	n	d	n	d
$21-25$	8	$70-74$	32	$118-121$	56	$175-176$	84	$222-223$	108
$30-33$	12	$80-81$	36	$127-128$	60	$182-184$	88	226	110
$38-42$	16	84	38	$135-138$	64	$189, 191$	92	$228-233$	112
45	18	$86-90$	40	142	66	194	94	$238-240$	116
$47-50$	20	93	42	$144-145$	68	$196-201$	96	243	118
53	22	$95-97$	44	148	70	205	98	$245-248$	120
$55-58$	24	100	46	$150-154$	72	$207-209$	100	250	122
$63-65$	28	$102-106$	48	$159-160$	76	212	102	252	124
68	30	$111-113$	52	$166-170$	80	$214-216$	104	256	128

Acknowledgements

The authors thank the anonymous referee for pointing out some errors and giving helpful remarks which improved the paper considerably.

References

[1] K. Aardal, C. A. J. Hurkens and A. K. Lenstra: *Solving a linear Diophantine equation with lower and upper bounds on the variables.* In: R. E. Bixby, E. A. Boyd and R.Z. Ríos-Mercado (eds.): *Integer Programming and Combinatorial Optimization, 6th International IPCO Conference*, Springer, pp. 229–242, 1998.

[2] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann: *Error-correcting linear codes*, Springer, 2006.

[3] M. Braun: *Construction of linear codes with large minimum distance*, IEEE Transactions on Information Theory, Vol. 50, No. 8, pp. 1687–1691, August 2004.

[4] A. Kohnert: *Linear codes*, Online Server
http://linearcodes.uni-bayreuth.de.

[5] M. Braun, A. Kohnert and A. Wassermann: *Optimal linear codes from matrix groups*, IEEE Transactions on Information Theory, Vol. 51, No. 12, pp. 4247–4251, January 2005.

[6] A. Brouwer: *Linear code bounds*, Online Server
http://www.win.tue.nl/~aeb/voorlincod.html.

[7] J. H. Griesmer: *A bound for error-correcting codes*, IBM J. Res. Develop., Vol. 4, pp. 532–542, 1960.

[8] H. Ritter: *Breaking knapsack cryptosystems by max-norm enumeration*, In: J. Pribyl (ed.), Proceedings of the 1st International Conference on the Theory and Applications of Cryptology, PRAGOCRYPT'96, Prague, Czech Republic, pp. 480–492, CTU Publishing House, 1996.

[9] A. Wassermann: *Finding simple t-designs with enumeration techniques*, Journal of Combinatorial Designs 6, pp. 79–90, 1998.

[10] A. Wassermann: *Attacking the market split problem with lattice point enumeration*, Journal of Combinatorial Optimization 6, pp. 5–16, 2002.