ON DUAL EXTREMAL MAXIMAL SELF-ORTHOGONAL CODES OF TYPE I-IV

ANNAKA MEYER

Lehrstuhl D für Mathematik
RWTH Aachen University
Templergraben 64, 52062 Aachen, Germany

(Communicated by Steven Dougherty)

Abstract. For a Type $T \in \{I, II, III, IV\}$ of codes over finite fields and length $N$ where there exists no self-dual Type $T$ code of length $N$, upper bounds on the minimum weight of the dual code of a self-orthogonal Type $T$ code of length $N$ are given, allowing the notion of dual extremal codes. It is proven that for $T \in \{II, III, IV\}$ the Hamming weight enumerator of a dual extremal maximal self-orthogonal Type $T$ code of a given length is unique.

1. Introduction

Let $F$ be a finite field. A linear code is a subspace $C \leq F^N$. The dual code of $C$ is

$$C^\perp = \{v \in F^N | \sum_{i=1}^{N} v_i c_i^J = 0 \text{ for all } c \in C\},$$

where $J$ is the identity or a field automorphism of order 2. If $C \subseteq C^\perp$ then $C$ is called self-orthogonal and if $C = C^\perp$ then $C$ is called self-dual.

A famous result by Gleason and Pierce states that if a certain divisibility condition on the Hamming weights $\text{wt}(c) := |\{i \in \{1, \ldots, N\} | c_i \neq 0\}|$ is imposed on the codewords $c \in C$ then there are basically four Types of codes:

**Theorem 1.** (Gleason-Pierce Theorem) (cf. [12]) Let $C = C^\perp \leq F_q^N$ such that $\text{wt}(c) \in m\mathbb{Z}$ for all $c \in C$ and some $m > 1$. Then one of the following holds.

(I) $q = 2$ and $m = 2$ (self-dual binary codes),

(II) $q = 2$ and $m = 4$ (doubly-even self-dual binary codes),

(III) $q = 3$ and $m = 3$ (self-dual ternary codes),

(IV) $q = 4$, $m = 2$ and $J \neq \text{id}$ (Hermitian self-dual quaternary codes),

(o) $q = 4$, $m = 2$ (certain Euclidean self-dual codes),

(d) $q$ is arbitrary, $m = 2$ and $C$ is permutation equivalent to an orthogonal sum $\bigoplus_{i=1}^{N/2} (1,a)$ of self-dual codes of length 2 where either $q$ is even and $a = 1$ or $q \equiv 1 \pmod{4}$ and $a^2 = -1$ or $J$ has order 2 and $aa^J = -1$.

The first four of the above are named self-dual Type I, II, III and IV codes, respectively. For $T \in \{I, II, III, IV\}$, the respective integer $m$ from Theorem 1 will be denoted by $m_T$ throughout this paper.

Many authors simply call “Type $T$” the codes from Theorem 1, i.e. Type $T$ implies self-dual. However, since we are interested in the lengths $N$ where there

2000 Mathematics Subject Classification: 11T71.

Key words and phrases: Linear code, self-orthogonal code, weight distribution, extremality.
exists no self-dual code of the respective Type, we are going to broaden the term Type \( T \) as follows.

**Definition 1.** For \( T \in \{I, II, III, IV\} \), a Type \( T \) code is a self-orthogonal linear code, over the field \( F_2 \) for \( T \in \{I, II\} \), over the field \( F_3 \) for \( T = III \) and over \( F_4 \) for \( T = IV \), respectively, such that the Hamming weight of each codeword is a multiple of \( m_T \).

Note that the divisibility condition on the Hamming weights in Definition 1 is an additional constraint only for \( T = II \). Although in this sense Type II codes are also Type I codes, for clarity’s sake let us call Type I only those codes which are *not* doubly-even (as the majority of authors does for self-dual codes).

The Hamming weight enumerator

\[
we(C)(x, y) := \sum_{c \in C} x^{N - wt(c)} y^{wt(c)} \in \mathbb{C}[x, y],
\]

a homogeneous polynomial of degree \( N \), counts the number of codewords of each weight. Gleason showed that for a Type \( T \in \{I, IV\} \), the weight enumerators of self-dual Type \( T \) codes lie in a polynomial ring \( \mathbb{C}[f_T, g_T] \), where \( f_T \) and \( g_T \) themselves are linear combinations of products of weight enumerators of self-dual Type \( T \) codes ([4], see Theorem 8 in this paper).

This very powerful result provides an overview of the possible weight distributions of such codes, and in particular allows to derive the upper bounds on the minimum weight, \( d(C) := \min_{0 \neq c \in C} wt(c) \), cited in Theorem 3. The closer the minimum weight comes to this bound, the better the error-correcting capability of the code. A self-dual code is called *extremal* if its minimum weight reaches the respective upper bound.

Moreover, it follows immediately from Gleason’s Theorem that the length of a self-dual Type \( T \) code is always a multiple of \( o_T := \min(\deg(f_T), \deg(g_T)) = \gcd(\deg(f_T), \deg(g_T)) \).

In this paper, we consider the case where \( N \) is not a multiple of \( o_T \). By the above, there exists no self-dual Type \( T \) code of length \( N \), but one may still consider maximal self-orthogonal Type \( T \) codes, which we will simply call maximal Type \( T \) codes.

**Definition 2.** A code \( C \) is called maximal Type \( T \) if it is Type \( T \) and there exists no Type \( T \) code which properly contains \( C \).

The main theorem below gives upper bounds on the dual minimum weight \( d(C^\perp) \) of a maximal Type \( T \) code \( C \) (and thus on the dual minimum weight of any Type \( T \) code), which gives rise to the notion of dual extremal maximal Type \( T \) codes.

**Theorem 2.** Let \( T \in \{I, \ldots, IV\} \) and let \( C \) be a maximal Type \( T \) code. Then \( d(C^\perp) \leq d_{\max}(T, N) \), where \( d_{\max}(T, N) \) is given in Table 1 below.

The bounds are, basically, developed in two ways, depending on the parameters of \( C \). If the code length \( N \), writing \( n \cdot o_T \leq N \leq (n + 1) \cdot o_T \) with some integer \( n \), is closer to \( (n + 1) \cdot o_T \), then one may extend \( C^\perp \) to a self-dual Type \( T \) code of length \( (n + 1) \cdot o_T \) (cf. Section 2), and then use the well-known bounds on the minimum weight of self-dual Type \( T \) codes and design theory to upper bound \( d(C^\perp) \) (cf. Section 3.2). If \( N \) is closer to \( n \cdot o_T \) then it is more appropriate to use the structure of the complex vector space \( F_T^{(k)} \) spanned by the dual Hamming weight enumerators of maximal Type \( T \) codes of length equivalent to \( k \ (mod \ o_T) \),
in Section 4. The case $T = II$ and $N \equiv 4 \pmod{8}$ is exceptional here, since the extension and shortening procedure introduced in this paper fail to construct a self-dual code from a maximal Type II code of length $N \equiv 4 \pmod{8}$. However, one obtains upper bounds on $d(C^\perp)$ using the shadow of a self-dual Type I code of length $N$ and a result by Bachoc and Gaborit in [1] (cf. Section 3.4). Here it proves particularly useful to consider the dual distance $d(C^\perp)$ instead of $d(C)$.

The structure of $I_T^{(k)}$ is investigated in Section 4. Clearly $I_T^{(k)}$ is a module for $\mathbb{C}[f_T,g_T]$, since the orthogonal sum of a self-dual and a maximal self-orthogonal code is again a maximal self-orthogonal code. As a $\mathbb{C}[f_T,g_T]$-module, $I_T^{(k)}$ is finitely generated and free ([6, Ch. 10]).

Based on the latter observation, one obtains results on the weight distribution similar to those in the case of self-dual Type $T$ codes. In particular, it is shown in Section 4 that for $T \in \{II,III,IV\}$ the Hamming weight enumerator of a dual extremal maximal Type $T$ code is uniquely determined.

**Table 1. Value of $d_{\text{max}}(T,N)$**

| $T$ | $m_T$ | $\sigma_T$ | $N$ | $d_{\text{max}}(T,N)$ |
|-----|-------|------------|-----|----------------------|
| I   | 2     | 2          | $N \not\equiv 21 \pmod{24}$ | $\min\{4 + 4\lceil \frac{N+1}{24} \rceil, 2 + 2\lceil \frac{N+1}{8} \rceil\}$ |
|     |       |            | 21 (mod 24)        | $6 + 4\lceil \frac{N+1}{24} \rceil$ |
|     |       |            | 1, 9 or 17 (mod 24) | $1 + \lceil \frac{N}{24} \rceil + 3\lceil \frac{N+7}{24} \rceil$ |
|     |       |            | 2 (mod 24)         | $\frac{N+8}{6}$ |
|     |       |            | 3, 11 or 19 (mod 24)| $1 + 2\lceil \frac{N}{24} \rceil + \lceil \frac{N+5}{24} \rceil + \lceil \frac{N+13}{24} \rceil$ |
|     |       |            | 4 (mod 24)         | $\frac{N+8}{6}$ |
|     |       |            | 5 (mod 24)         | $1 + 4\lceil \frac{N}{24} \rceil$ |
|     |       |            | 6 (mod 24)         | $2 + 4\lceil \frac{N}{24} \rceil$ |
|     |       |            | 7, 13, 14 or 15 (mod 24) | $3 + 4\lceil \frac{N}{24} \rceil$ |
|     |       |            | 10 or 18 (mod 24)  | $1 + \lceil \frac{N}{8} \rceil + \lceil \frac{N+8}{24} \rceil$ |
|     |       |            | 12 (mod 24)        | $\frac{N}{6}$ |
|     |       |            | 20 (mod 24)        | $\frac{N+4}{6}$ |
|     |       |            | 21 (mod 24)        | $5 + 4\lceil \frac{N}{24} \rceil$ |
|     |       |            | 22 (mod 24)        | $6 + 4\lceil \frac{N}{24} \rceil$ |
|     |       |            | 23 (mod 24)        | $7 + 4\lceil \frac{N}{24} \rceil$ |
| II  | 4     | 8          | $N \equiv 21 \pmod{24}$ | $\frac{N+1}{6}$ |
|     |       |            | 1, 5 or 9 (mod 12) | $3 + 3\lceil \frac{N}{12} \rceil$ |
|     |       |            | 2 (mod 12)         | $1 + 3\lceil \frac{N}{12} \rceil$ |
|     |       |            | 3, 6 or 7 (mod 12) | $2 + 3\lceil \frac{N}{12} \rceil$ |
|     |       |            | 10 (mod 12)        | $4 + 3\lceil \frac{N}{12} \rceil$ |
|     |       |            | 11 (mod 12)        | $5 + 3\lceil \frac{N}{12} \rceil$ |
| III | 3     | 4          | 1 or 3 (mod 6)     | $1 + 2\lceil \frac{N}{6} \rceil$ |
|     |       |            | 5 (mod 6)          | $3 + 2\lceil \frac{N}{6} \rceil$ |
| IV  | 2     | 2          | $N \equiv 21 \pmod{24}$ | $\frac{N+1}{6}$ |
2. Constructing self-dual codes from maximal self-orthogonal codes

Let $C$ be a maximal Type $T$ code, for some $T \in \{I, \ldots, IV\}$, and length $N = k + n \cdot o_T$, with $1 \leq k \leq o_T - 1$. In what follows, two methods are presented to construct a self-dual Type $T$ code from $C$. The first method, an extension of $C^\perp$, applies when $k \geq \frac{o_T}{2}$, unless $T = \Pi$ and $N \equiv 4 \pmod{8}$. The thus extended self-dual code $\text{ext}(C)$ will have length $(n+1) \cdot o_T$. For Type I codes, this is nothing but the well-known procedure of adding an overall parity check (cf. [8, Ch. 1]). The second method, a shortening of $C$, applies when $t \leq \frac{o_T}{2}$ (again unless $T = \Pi$ and $N \equiv 4 \pmod{8}$), and results in a self-dual code of length $n \cdot o_T$. This method is a generalization of the puncturing process for Type I codes (see, again, [8, Ch. 1]).

An important preparation is the following basic result on the dimension of maximal self-orthogonal codes. By the theory of Witt groups (see [11, Ch.1,2]), the isomorphism type of the quadratic module $C^\perp/C$ is independent from the choice of $C$ (see e.g. [6, Ch. ]). In particular we have the following.

**Lemma 1.** Let $D_T(N)$ be the dimension of a maximal Type $T$ code $C$ of length $N = k + n \cdot o_T$, with $1 \leq k \leq o_T - 1$, and let $D'_T(N) = N - D_T(N)$ be the dimension of $C^\perp$. Then $D_T(N)$ (and hence $D'_T(N)$) is well-defined, i.e. independent from the choice of $C$.

For the extension and shortening procedures, the values of $D_T(N)$ and $D'_T(N)$ are particularly important.

**Lemma 2.** Let $N = k + n \cdot o_T$, where $n$ and $k$ are integers and $1 \leq k \leq o_T - 1$.

(i) If $k \geq \frac{o_T}{2}$ then $D'_T(N) - D_T(N) = o_T - k$ and $D'_T(N) = \frac{(n+1) \cdot o_T}{2}$, except in the case when $T = \Pi$ and $k = 4$.

(ii) If $k \leq \frac{o_T}{2}$ then $D'_T(N) - D_T(N) = k$ and $D_T(N) = \frac{n \cdot o_T}{2}$, except in the case when $T = \Pi$ and $k = 4$.

(iii) If $k = 4$ then $D'_T(N) = \frac{n \cdot o_T}{2} + 1$.

**Proof.** For $n = 0$, the claim of the lemma is easily verified. Now if $C$ is a maximal Type $T$ code of length $N$ and $C'$ is a self-dual code of length $o_T$, then $C \oplus C'$ is a maximal Type $T$ code of length $N + o_T$ and dimension $D_T(N) + \frac{r}{2}$. Hence

$$D'_T((n+1) \cdot o_T) = D'_T(n \cdot o_T) + \frac{o_T}{2}.$$ 

The rest is induction on $N$, using the relation $D_T(N) = N - D'_T(N)$. \qed

2.1. Extension. This is a special way of gluing codes together (cf. [8, Ch.3, Sect. 11.11.1]). Assume that $k \geq \frac{o_T}{2}$, but not $T = \Pi$ and $k = 4$. We construct a linear map $f : C^\perp \to F^{o_T - k}$ with kernel $C$ such that $(f(c'), f(c'')) = -(c', c'')$ for all $c', c'' \in C^\perp$. Then $\text{ext}(C) := \{(c', f(c')) \mid c' \in C^\perp\}$ is a Type $T$ code of length $(n+1) \cdot o_T$, which is even self-dual since according to Lemma 2,

$$\dim(\text{ext}(C)) = \dim(C^\perp) = \frac{(n+1) \cdot o_T}{2}.$$ 

The map $f$ will be explicitly given in Table 2, since the weight distribution of the code $\text{ext}(C)$ is the primary interest here. However, we shall mention that the existence of $f$ has the following theoretical background (see [11, Ch.1]): Let $\beta(N)$ denote the (Euclidian or Hermitian) scalar product on $F^N$ which defines orthogonality in the context of the respective Type $T$. If $C \leq F^N$ is a $T$ code then one obtains
another well-defined scalar product
\[ \beta^{(N)} / C : C^⊥ / C \times C^⊥ / C \to \mathbb{F}, \quad (c' + C, c'' + C) \mapsto \beta^{(N)}(c', c''). \]

If \( C \) is maximal self-orthogonal then the space \( (C^⊥ / C, -\beta^{(N)} / C) \) is isometric to \( (\mathbb{F}^{α_T-k}, \beta^{(α_T-k)}) \) (that the two spaces have the same dimension is already in Lemma 1, the rest is, again, a result of the theory of Witt groups). Hence the orthogonal sum
\[ (C^⊥ / C, \beta^{(N)} / C) \oplus (\mathbb{F}^{α_T-k}, \beta^{(α_T-k)}) \]
contains a self-dual code \( \tilde{C} \). Now for \( c' \in C^⊥, f(c') \) is the unique element of \( \mathbb{F}^{α_T-k} \) such that \( (c' + C, f(c')) \in \tilde{C} \), i.e. \( \text{ext}(C) = \{(c', f(c')) \mid (c' + C, f(c')) \in \tilde{C}\} \).

**Table 2. Extension**

| \( T \) | \( α_T \) | \( k \) | \( \mathcal{B} \) | \( f(\mathcal{B}) \) |
|---|---|---|---|---|
| I | 2 | 1 | \( (v), \mathcal{G}(v) = (1) \) | \( f(v) = (1) \) |
| II | 8 | 5 | \( (u, v, w), \mathcal{G}(u, v, w) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \mathcal{Q}(u, v, w) = \begin{pmatrix} \frac{1}{7} & \frac{1}{7} & \frac{1}{7} \end{pmatrix} \) | \( f(u) = (1 \ 1 \ 0), f(v) = (0 \ 1 \ 1), f(w) = (1 \ 1 \ 1) \) |
| II | 8 | 6 | \( (u, v), \mathcal{G}(u, v) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathcal{Q}(u, v) = \begin{pmatrix} \frac{3}{4} & \frac{3}{4} \end{pmatrix} \) | \( f(u) = (1 \ 0), f(v) = (0 \ 1) \) |
| II | 8 | 7 | \( (v), \mathcal{G}(v) = (1), \mathcal{Q}(v) = \begin{pmatrix} \frac{1}{2} \end{pmatrix} \) | \( f(v) = (1) \) |
| III | 4 | 2 | \( (u, v), \mathcal{G}(u, v) = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \) | \( f(u) = (1 \ 1), f(v) = (1 \ 2) \) |
| III | 4 | 3 | \( (v), \mathcal{G}(v) = (2) \) | \( f(v) = (1) \) |
| IV | 2 | 1 | \( (v), \mathcal{G}(v) = (1) \) | \( f(v) = (1) \) |

Table 2 shows explicitly how to extend a maximal Type \( T \) code. There \( \mathcal{B} \) denotes an ordered set of vectors in \( \mathbb{F}^N \) such that \( \{b + C \mid b \in \mathcal{B}\} \) is a basis for \( C^⊥ / C \), and \( \mathcal{G} \) is the Gram matrix of \( \beta^{(N)} / C \) with respect to \( \mathcal{B} \). If \( T = \text{II} \) then, additionally, the table gives the values of the quadratic form
\[ Q : C^⊥ / C \to \mathbb{Q} / \mathbb{Z}, \quad c' + C \mapsto \frac{1}{4} \text{wt}(c') + \mathbb{Z}. \]

Note that, writing \( N = k + n \cdot α_T \) as above, up to isometry \( \mathcal{G} \) and \( Q \) do not depend on \( n \) - for \( \mathcal{G} \), this has already been mentioned, and there is an analogous result for quadratic forms (cf. [11, Ch.2]).
One observes that a word in \( C^\perp \) is extended to a word with the least possible Hamming weight which is a multiple of \( m_T \). Technically speaking, the extension procedure has the following effect on the Hamming weight enumerator.

**Remark 1.** Let \( C \) be a maximal Type \( T \) code of length \( N = n \cdot \alpha_T + k \), where \( \frac{2T}{n} \leq k \leq n - 1 \), and let \( \text{ext}(C) \) be the self-dual Type \( T \) code of length \( (n + 1) \cdot \alpha_T \) obtained by extension of \( C \) as described above. If \( \text{we}(C^\perp) = x^N + \sum_{i=d(C^\perp)}^{N} a_i x^{N-i} y^i \) then

\[
\text{we}(\text{ext}(C)) = x^{N+\alpha_T-k} + \sum_{i=d(C^\perp)}^{N+\alpha_T-k} b_i x^{N+\alpha_T-k-i} y^i,
\]

where

\[
b_i = \begin{cases} 
  a_i + a_{i-1} + \cdots + a_{i-m(T)+1}, & i \equiv 0 \pmod{m_T} \\
  0 & \text{otherwise}.
\end{cases}
\]

In particular, there exists an integer \( t \), depending on the length of \( C \), such that \( d(C^\perp) \leq t \cdot m_T \leq d(\text{ext}(C)) \). This will be used in Section 3 to derive upper bounds on \( d(C^\perp) \).

### 2.2. Shortening.

Assume that \( k \leq \frac{2T}{n} \), but not \( T = \Pi \) and \( k = 4 \). Moreover, assume that \( D_T(N) \geq k \). This only excludes the case \( N = k = 1 \), for \( T \in \{I, \ldots, IV\} \), or \( T \in \{II, III\} \) and \( k = N = 2 \). In these cases, the zero code of length 0 is appropriate as the shortened code.

Otherwise, since \( D_T(N) \geq k \), after some suitable permutation of the coordinates the map

\[
\pi : C \to \mathbb{F}^k, \quad (c_1, \ldots, c_N) \mapsto (c_{N-k+1}, \ldots, c_N)
\]

which maps a codeword to its last \( k \) components is surjective. There are possibly lots of suitable coordinate permutations, which may result in different shortened codes (cf. Example 1). However, in the context of this paper it suffices to consider just any of these, keeping in mind that the obtained shortened code depends on this choice.

Since \( D_T(N) - D_T(N) = k \) due to Lemma 2, there exists a subset \( \mathcal{B} = \{v_1, \ldots, v_k\} \subset \mathbb{F}^N \) with \( \langle C, v_1, \ldots, v_k \rangle = C^\perp \). The \( v_i \) may be chosen to satisfy

\[(v_i, v_j) = (\pi(v_i), \pi(v_j))\]

for all \( i, j \in \{1, \ldots, k\} \), possibly after adding suitable elements of \( C \), due to the surjectivity of \( \pi \). Now we define a map \( f : C^\perp \to \mathbb{F}^{\alpha_T-k} \) (given explicitly in Table 3) as in the case where \( k \geq \frac{2T}{n} \), to obtain a self-orthogonal code \( E := \{(c', f(c'))\} \) of length \( (n + 1) \cdot \alpha_T \) and dimension \( D_T(N) \). In general, the code \( E \) is not self-dual. However, the code \( D \) formed by the last \( \alpha_T \) coordinates of the vectors \( (v_i, f(v_i)) \), \( i \in \{1, \ldots, k\} \) is self-orthogonal. Define

\[
C_{(k)} := \{(c_1, \ldots, c_{n-\alpha_T}) \mid (c_1, \ldots, c_{(n+1)-\alpha_T}) \in E, (c_{n-\alpha_T+1}, \ldots, c_{(n+1)-\alpha_T}) \in D\}.
\]

This procedure is called *subtraction* of \( D \) from \( E \) (cf. [8]). The code \( C_{(k)} \) is clearly self-orthogonal. Its length is \( n \cdot \alpha_T \) and, by Lemma 2, its dimension is

\[
\dim(\ker(\pi)) + \dim(C^\perp/C) = \dim(C) - k + k = \dim(C) = \frac{n \cdot \alpha_T}{2}.
\]

Hence \( C_{(k)} \) is a self-dual Type \( T \) code. From Table 3 one easily tells that there exists an integer \( t \), depending on the length of \( C \), such that \( d(C^\perp) - k \leq t \cdot m_T \leq d(C_{(k)}) \). It is not possible, though, to foretell the effect of the shortening procedure on the weight distribution of \( C \). Example 1 presents two ways of shortening a code, such that the shortened codes have different weight enumerators.
| $T$ | $\omega$ | $K$ | $D$ | $f(\beta)$ | $G(\omega)$ | $Q(\omega)$ | $f(\omega)$ |
|-----|-----|-----|-----|--------|--------|--------|--------|
| I  | 2 1 | 1  | (1 1 0 0 0 0 0) | $f(\beta) = (1)$ | $G(\omega) = (1)$ | $Q(\omega) = (1 0 0)$ | $f(\omega) = (1 1 0 0 0 0 0)$ |
| II | 8 1 | 1  | (1 1 0 0 0 0 0) | $f(\beta) = (1)$ | $G(\omega) = (1)$ | $Q(\omega) = (1 0 0)$ | $f(\omega) = (1 1 0 0 0 0 0)$ |
| III| 8 2 | 1  | (1 1 0 0 0 0 0) | $f(\beta) = (1)$ | $G(\omega) = (1)$ | $Q(\omega) = (1 0 0)$ | $f(\omega) = (1 1 0 0 0 0 0)$ |
| IV | 4 1 | 1  | (1 1 0 0 0 0 0) | $f(\beta) = (1)$ | $G(\omega) = (1)$ | $Q(\omega) = (1 0 0)$ | $f(\omega) = (1 1 0 0 0 0 0)$ |
Example 1. Let $C$ be the maximal self-orthogonal ternary $[13, 6, 3]$ code such that $C^\perp$ has generator matrix

$$B := \begin{pmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 0 & 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \\
2 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 1
\end{pmatrix}$$

The first six rows of $B$ form a generator matrix of $C$. One verifies that $C$ is a direct sum of the self-dual tetracode $t_4$ of length 4 and the maximal self-orthogonal $[9, 4, 3]$ code $e^{3+3}$ (see [6] for more details). A generator matrix of a shortening $C_{(1)}$ of $C$ is obtained by deleting the penultimate row and last column of $B$. Using Magma, one verifies that

$$\text{we}(C_{(1)}) = x^{12} + 8x^9y^3 + 240x^6y^6 + 464x^3y^9 + 16y^{12}.$$ 

Let $C'$ be the code obtained from $C$ by a cyclic left coordinate shift. A generator matrix for a shortening $C'_{(1)}$ of $C'$ is obtained from $B$ by deleting the first row and column. One observes that $C'_{(1)}$ has a direct summand $t_4$, while $C_{(1)}$ has not; hence their weight enumerators must be distinct. In fact,

$$\text{we}(C'_{(1)}) = x^{12} + 24x^9y^3 + 192x^6y^6 + 512x^3y^9.$$ 

In conclusion, the weight distribution of the extended code only depends on the weight distribution of the original code, while shortening does not even respect permutation equivalence. In Section 5, it will be shown that no way of shortening can be found such that

1. shortening is well-defined on the weight enumerator level and, in this sense,
2. the “shortening” of weight enumerators extends to a homomorphism $U^{(k)}_T \rightarrow \mathbb{C}[f_T, g_T]$ of $\mathbb{C}[f_T, g_T]$-modules (cf. Section 1), such that
3. a polynomial $x^N + a_Ny^d x^{N-d} + \cdots + a_Ny^N$ is “shortened” to a polynomial of the form $x^{N-s} + b_{N-s}y^{d-s} + \cdots + b_{N-s}y^{N-s}$, where $s$ is the number of positions shortened, i.e. shortening allows to derive upper bounds on the minimum distance even on the polynomial level.

3. Bounds on the dual distance of codes of Type I – IV

In the previous section, two procedures have been described to obtain a self-dual Type $T$ code $D$ from a maximal Type $T$ code $C$. Now the connection between $d(C)$ and $d(D)$ is studied, to obtain an upper bound for $d(C^\perp)$ from upper bounds that are known for $d(D)$.

For self-orthogonal codes of length $N = k + n \cdot o_T$, where $n$ and $k$ are integers with $k \in \{\frac{N}{2}, \ldots, o_T - 1\}$ (cf. Section 3.2), the extension procedure is applied, and the obtained bounds (cf. Theorem 6) are sharp for small $N$. An important tool in developing these bounds is a result by Assmus and Mattson (cf. Theorem 5), which says that the words of minimum weight in an extremal self-dual code (cf. Definition 3) hold a $t$-design, where $t$ depends on the Type and length of the code.

When $k \in \{1, \ldots, \frac{N}{2} - 1\}$ (cf. Section 3.3), the shortening procedure applies, but the thus obtained bounds on $d(C^\perp)$ are not satisfactory, not even for small $N$. In Section 5, a different approach is pursued, using the algebraic structure of the space.
spanned by the Hamming weight enumerators of maximal self-orthogonal codes, to obtain the sharp upper bounds from Theorem 2.

In the exceptional case $T = II$ and $N \equiv 4 \pmod{8}$, sharp upper bounds on $d(C^\perp)$ are derived in Section 3.4.

### 3.1. Some known results on extremal self-dual codes.

Recall that the Hamming weight enumerators of self-dual Type $T$ codes, for $T \in \{I, \ldots, IV\}$, lie in a polynomial ring $\mathbb{C}[f_T, g_T]$, where $f_T, g_T$ are themselves linear combinations of products of weight enumerators of self-dual Type $T$ codes (cf. Section 1). This has been used by several authors to derive upper bounds on the minimum distance of these codes, as follows.

**Theorem 3.** (cf. [8, Ch.3, Th.28]) Let $C$ be a self-dual Type $T$ code of length $N$, where $T \in \{I, II, III, IV\}$. Then $d(C) \leq m_T + m_T \lfloor \frac{N}{\deg(g_T)} \rfloor$.

For Type I codes, this bound can be improved using the concept of the shadow of a code (cf. Section 3.4). The following is due to Rains ([10]).

**Theorem 4.** Let $C$ be a self-dual Type I code of length $N$. Then $d(C) \leq 4 + 4 \lfloor \frac{N}{24} \rfloor$, except if $N \equiv 22 \pmod{24}$, in which case $d(C) \leq 6 + 4 \lfloor \frac{N}{24} \rfloor$.

These very powerful results allow a notion of extremality for self-dual codes of Type I-IV.

**Definition 3.** For $T \in \{II, III, IV\}$, a self-dual Type $T$ code is called extremal if its minimum weight equals the bound given in Theorem 3. A self-dual Type I code is called extremal if its minimum weight equals the bound given in Theorem 4.

In either case, we denote the minimum weight of an extremal self-dual code of Type $T$ and length $N$ by $d_{\text{max}}(T, N)$. The set of all words of minimum weight in an extremal self-dual code of Type II – IV has a particularly nice structure. Note that $s$-extremal codes in the sense of [1] also yield designs.

**Theorem 5.** [Assmus-Mattson, see [5, Th. 9.3.10]] Let $T \in \{II, III, IV\}$ and let $C$ be an extremal self-dual Type $T$ code of length $N > 0$. Then the words of minimum weight in $C$ hold a $t(T, N)$-design according to the following table.

|   | II | III | IV |
|---|----|-----|----|
| $N \pmod{\deg(g_T)}$ | 0  | 8   | 16 |
| $t(T, N)$               | 5  | 3   | 1  |

In an extremal self-dual Type I code whose length is not a multiple of 24, the words of minimum weight in general do not hold a design. There are even extremal self-dual Type I codes where the supports of the words of minimum weight are contained in a proper subset of $\{1, \ldots, N\}$. Hence we define $t(I, N) = 0$ for $N \not\equiv 0 \pmod{24}$. If $N$ is a multiple of 24 then an extremal self-dual Type I code is also Type II, and of course extremal in the sense of Type II. In this case the words of minimum weight form a 5-design. Correspondingly, we define $t(I, N) = 5$ if $N \equiv 0 \pmod{24}$.

### 3.2. Bounds in the extension case.
Theorem 6. Let $T \in \{I, \ldots, IV\}$ and let $C$ be a Type $T$ code of length $N \equiv k \pmod{\sigma_T}$, where $k \geq \frac{\sigma_T}{2}$, and let $d_{\text{max}}(T, N + \sigma_T - k)$, $t(T, N + \sigma_T - k)$ be as in the previous section. Then
\[
d(C^\perp) \leq d_{\text{max}}(T, N) := d_{\text{max}}(T, N + \sigma_T - k) - \min(t(T, N + \sigma_T - k), \sigma_T - k).
\]

Proof. Assume that $d(C^\perp) > d_{\text{max}}(T, N)$. Let $\delta := \min(t(T, N + \sigma_T - k), \sigma_T - k)$, and consider the self-dual extended code $\text{ext}(C)$. Due to our assumption, $d(C^\perp) > d(\text{ext}(C)) - \delta$. Hence the words of minimum weight in $\text{ext}(C)$ have less than $\delta$ nonzero entries in their last $\sigma_T - k$ coordinates. On the other hand, $\text{ext}(C)$ is extremal, since always $\delta \leq m_T$. Hence its words of minimum weight form a $t(T, N + \sigma_T - k)$-design and thus for an arbitrary $\delta$-subset $M$ of the last $\sigma_T - k$ coordinates, there exists a word of minimum weight in $\text{ext}(C)$ whose support contains $M$. This is a contradiction. Hence the claim of the theorem follows. \hfill \Box

This motivates us to call dual extremal a maximal Type $T$ code of length $N$ (where $N$ is as in the beginning of this section) if its dual distance equals $d_{\text{max}}(T, N)$.

Lemma 3. With the notation from Theorem 6, assume that $\sigma_T - k \leq t(T, N + \sigma_T - k)$. Then $\text{ext}$ establishes a correspondence between the set of all dual extremal maximal Type $T$ codes of length $N$ and the set of all extremal self-dual Type $T$ codes of length $N + \sigma_T - k$. In this case, $\text{ext}$ inverts the puncturing process on these two sets, i.e. one obtains the dual of a maximal Type $T$ code $C$, with $d(C^\perp) = d_{\text{max}}(T, N)$, by deleting the last $\sigma_T - k$ coordinates in an extremal self-dual code of length $N + \sigma_T - k$.

Proof. If $D$ is an extremal self-dual code of length $N + \sigma_T - k$, then $D$ contains a word of minimum weight whose support contains the last $\sigma_T - k$ coordinate positions. Hence deleting the last $\sigma_T - k$ coordinates in $D$ yields the dual of a maximal Type $T$ code $C$, with $d(C^\perp) = d(D) - \delta = d_{\text{max}}(T, N)$. \hfill \Box

Example 2. (i) There is in general no correspondence between the dual extremal maximal Type III codes of length $N \equiv 6 \pmod{12}$ and the extremal self-dual Type III codes of length $N + 2$ (in this case, with the notation from Theorem 6, $\sigma_T - k = 2$ and $t(T, N + 2) = 1$). For instance, the extremal self-dual ternary [20,10,6] code $D$ with generator matrix $(I_{10} \mid H)$, where
\[
H = \begin{pmatrix}
1 & 1 & 1 & 2 & 2 & 0 & 1 & 2 & 2 \\
1 & 1 & 1 & 2 & 2 & 0 & 2 & 0 & 1 \\
1 & 2 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \\
1 & 2 & 1 & 0 & 2 & 0 & 2 & 1 & 2 \\
2 & 0 & 1 & 2 & 0 & 2 & 1 & 2 & 2 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 2 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 0 \\
1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 2 \\
0 & 1 & 0 & 2 & 1 & 1 & 1 & 2 & 1
\end{pmatrix},
\]

(cf. [7,9]) cannot be obtained by extending a dual extremal Type III code of length 18. This is due to the fact that $D$ contains codewords of weight 6 whose penultimate and ultimate entries are both nonzero, so any word in a ternary code of length 18 that extends to these must have minimum weight $4 < 5 = d_{\text{max}}(\text{III,18})$. Although the words of weight 6 in $D$ do not form a
Similarly, there is in general no correspondence between the dual extremal Type II codes and the extremal self-dual Type II codes of length \( n = 13 \) or \( n = 14 \) (mod 24). Hence extension of an extremal self-dual Type III code never leads to a permutation equivalent of \( D \), i.e. here ext does not even establish a correspondence between the permutation equivalence classes of the respective codes.

(ii) Similarly, there is in general no correspondence between the dual extremal Type II codes of length \( n \equiv 13 \) or \( n \equiv 14 \) (mod 24) and the extremal self-dual Type II codes of length \( n + 3 \) or \( n + 2 \), respectively.

(iii) In all the other cases (i.e. except when \( T = \text{III} \) and \( n \equiv 6 \) (mod 12) or \( T = \text{II} \) and \( n \equiv 13 \) or \( n \equiv 14 \) (mod 24)), ext establishes a bijection between the set of all dual extremal codes of length \( n \) and the set of all extremal self-dual codes of length \( n + \sigma_T - k \), due to Theorem 6. The inverse map consists in puncturing (and then changing to the dual code), i.e. in an extremal self-dual code, the last \( \sigma_T - k \) coordinates can be omitted to obtain the dual of a dual extremal code. Puncturing 1,2 or 3 coordinates in the extremal extended Golay code \( g_{24} = g_{12} \), for instance, leads to a dual extremal \([23,12,7]\) or \([22,12,6]\) or \([21,12,5]\) code, respectively.

3.3. Bounds in the shortening case. As announced above, in this case one obtains only very weak bounds, using the fact that the minimum distance of the shortened code is always less than or equal to the minimum distance of the original code. The reason is that, contrarily to the extension case, shortening means a lot of information loss. The following preliminary result is improved in Section 4.

Remark 2. Let \( C \) be a Type \( T \) code of length \( n \), where \( T \in \{I, \ldots, IV\} \) and assume that \( n \equiv k \) (mod \( \sigma_T \)), where \( k \in \{1, \ldots, \frac{\sigma_T}{2} - 1\} \). Then \( d(C^\perp) = d_{\text{max}}(T, n-k)+k \).

3.4. Bounds from shadows. In this section, an upper bound on the dual distance of a maximal Type II code of length \( n \equiv 4 \) (mod 8) is given, using the concept of the shadow (cf. [2]). For a self-dual Type I code \( D \) of length \( n \), the shadow \( S(D) \) is the set of all vectors \( v \in F_2^n \) such that

\[
2 \sum_{i=1}^N v_i d_i \equiv \text{wt}(d) \pmod{4}
\]

for all \( d \in D \). Equivalently, if \( C := \{d \in D \mid \text{wt}(d) \equiv 0 \pmod{4}\} \) is the doubly-even subcode of \( D \), then \( S(D) = C^\perp - D \). Note that \( \dim(C) = \dim(D) - 1 \), i.e. \( C \) is a maximal Type II code. The following has been shown in [1] (see also [3]).

Theorem 7. Let \( D \) be a self-dual Type I. Let \( d(S(D)) := \min\{\text{wt}(s) \mid s \in S(D)\} \). Then \( 2d(D)+d(S(D)) \leq 4 + \frac{N}{2} \), unless \( n \equiv 22 \) (mod 24), when \( 2d(D)+d(S(D)) \leq 6 + \frac{N}{2} \).

Assume that \( n \) is even, but no multiple of 8, i.e. there exists a self-dual Type I code, but no self-dual Type II code of length \( n \). Let \( C \) be a maximal Type II code of length \( n \), and let \( D \) be a self-dual Type I code which contains \( C \), i.e. \( C \) is the doubly-even subcode of \( D \), and \( S(D) = C^\perp - D \). Then, due to Theorem 7,

\[
d(C^\perp) = \min\{d(S(D)), d(D)\} \leq \frac{1}{3} (2d(S(D)) + d(D)) \leq \frac{N+8}{6}.
\]

Based on this observation, one easily concludes the proof of Theorem 2 in the case \( T = \text{II} \) and \( n \equiv 4 \) (mod 8), and in the case \( T = \text{II} \) and \( n \equiv 2 \) (mod 24).
4. The weight distribution of a dual extremal code of Type II-IV is unique

Using the structure of the ring $\mathbb{C}[f_T, g_T]$, it is not hard to see that the weight enumerator of an extremal self-dual code of Type $T \in \{\text{II, III, IV}\}$ is uniquely determined (cf. [8, Ch. 3]). For $T = \text{I}$, this is false if one (as we do) considers as extremal those codes whose minimum distance reaches the newer bound given by Rains (cf. Theorem 4). Hence in this section, unless Type I is explicitly included, let $T$ be one of the Types II, III or IV.

For lengths where there exists no self-dual Type $T$ code, this section uses the structure of the complex vector space $I_T^{(k)}$ spanned by the Hamming weight enumerator of maximal Type $T$ codes of length congruent to $k \pmod{\sigma_T}$ as a $\mathbb{C}[f_T, g_T]$-module (free and finitely generated, cf. Section 4.1) to prove an analogous result for maximal Type $T$ codes. It follows from the fact that $I_T^{(k)}$ has the Weierstrass property that for every integer $N \equiv k \pmod{\sigma_T}$ there exists a unique homogeneous polynomial $p \in I_T^{(k)}$ of the form

$$x^N + \delta((I_T^{(k)})^N)y^{\delta((I_T^{(k)})^N)}x^{N-\delta((I_T^{(k)})^N)} + \cdots + a_Ny^N,$$

where $\delta$ depends basically on the dimension of $(I_T^{(k)})_N$. On the one hand, in the case $k \geq \frac{N}{2}$, where Theorem 2 has been proven in the previous section, it turns out that the dual weight enumerator of a dual extremal maximal Type $T$ code of length $N$ is the unique element of $(I_T^{(k)})_N$ of the above form.

On the other hand, the least non-vanishing term in $p$ provides an upper bound for the minimum weight of a maximal Type $T$ code $C$ of length $N$, and the weight enumerator of a code meeting that bound is of course unique. This bound is easy to calculate for small values of $N$. For $k < \frac{N}{2}$ and lengths $N$ exceeding a certain range, one obtains upper bounds on $d(C^\perp)$ exploiting the fact that as $d(C^\perp)$ grows sufficiently large, one may shorten $C$ to an extremal self-dual code of almost the same length. But extremal self-dual codes do not exist for sufficiently large $N$. The exact spectrum, i.e. the meaning of “sufficiently large”, is in [8, Ch. 9.3]. In conclusion, one thus obtains upper bounds on $d(C^\perp)$ also when $k < \frac{N}{2}$, which completes the proof of Theorem 2.

4.1. Gleason’s Theorem and maximal Type $T$ codes.

**Theorem 8.** [Gleason’s Theorem] If $C$ is a self-dual Type $T$ code, where $T \in \{\text{I}, \ldots, \text{IV}\}$, then $\text{we}(C) \in \mathbb{C}[f_T, g_T]$, where $f_T$ and $g_T$ are themselves linear combinations of products of weight enumerators of self-dual Type $T$ codes, according to Table 4.

| Type | $f_T$ | $g_T$ |
|------|-------|-------|
| I    | $x^2 + y^2$ | $x^2y^2(x^2 - y^2)^2$ |
| II   | $x^8 + 14x^4y^4 + y^8$ | $x^4y^4(x^4 - y^4)^4$ |
| III  | $4x^4 + 8xy^3$ | $y^3(x^3 - y^3)^3$ |
| IV   | $x^2 + 3y^2$ | $y^2(x^2 - y^2)^2$ |
The direct sum of a self-dual Type $T$ code and a maximal Type $T$ code is again a maximal Type $T$ code, and the weight enumerator of a direct sum is the product of the weight enumerators of the summands. Hence, if $I_T^{(k)}$ is as above, then we have the following remark.

**Remark 3.** $I_T^{(k)}$ is a module for $\mathbb{C}[f_T, g_T]$.

It has been shown in [6, Ch. 10] that for $T \in \{I, \ldots, IV\}$, the module $I_T^{(k)}$ is free and generated by finitely many weight enumerators of maximal Type $T$ codes (see Table 5 in this paper).

### 4.2. The Weierstrass property

For a subspace $W \subseteq \mathbb{C}[x, y]$ and an integer $N$, let $W_N$ be the subspace of $W$ formed by the homogeneous elements of degree $N$.

**Definition 4.** Let $W \subseteq \mathbb{C}[x, y]$ be a subspace and let

$$J := \{ j \in \mathbb{N} \mid \text{coef}(p, y^j x^i) = 0 \text{ for all } p \in W \text{ and all } i \in \mathbb{N} \}.$$ 

The space $W$ is said to have the *Weierstrass property* if, for every $N \in \mathbb{N}$, every element of $W_N$ is uniquely determined by its first $\dim(W_N)$ coefficients which do not belong to $J$, i.e. by the coefficients in $x^N, x^{N-1}y, \ldots, x^{N-(\delta(W_N)-1)}y^{\delta(W_N)-1}$, where

$$\delta(W_N) = \min\{n \in \mathbb{N} \mid |\{0, \ldots, n-1\} - J| = \dim(W_N)\}.$$ 

It is well-known that the spaces $\mathbb{C}[f_T, g_T]$, for $T \in \{I, \ldots, IV\}$, have the Weierstrass property (cf. [8, Ch. 3]). This allows to define extremality of self-dual Type $T$ codes. In what follows this concept is described for a general space $W$, which is assumed to have the Weierstrass property: For every positive integer $N$ there is an injective linear map

$$W_N \rightarrow \mathbb{C}^{\delta(W_N)}, \quad \sum_{i=0}^{N} a_i y^i x^{N-i} \mapsto (a_0, \ldots, a_{\delta(W_N)}).$$

This gives rise to a notion of extremality, as follows.

**Definition 5.** Assume that the space $W \subseteq \mathbb{C}[x, y]$ has the Weierstrass property. Then for every positive integer $N$ the space $W_N$ contains a unique element of the form

$$x^N + a_{\delta(W_N)} y^{\delta(W_N)} x^{N-\delta(W_N)} + a_{\delta(W_N)+1} y^{\delta(W_N)+1} x^{N-(\delta(W_N)+1)} + \cdots + a_N y^N,$$

i.e. where the sequence formed by the first $\delta(W_N)$ coefficients is $(1, 0, \ldots, 0)$. This element is called the *extremal* element of $W_N$.

Recall that for Hamming weight enumerators of maximal Type $T$ codes, for $T \in \{I, \ldots, IV\}$ and $k \geq \frac{3T}{2}$, a notion of extremality has been introduced in Section 3.2, using the fact that a Type $T$ code of length $N$ satisfies $d(C^\perp) \leq d_{\max}(T, N)$. In the subsequent section it is shown that for $T \in \{I, II, III, IV\}$ the latter notion of extremality coincides with the one defined via the Weierstrass property.
4.3. Proof of the uniqueness of the extremal weight enumerator. In this section it is proven that the spaces \( I_T^{(k)} \) spanned by the dual Hamming weight enumerators of maximal Type \( T \) codes of length \( N \equiv k \mod o_T \) have the Weierstrass property, for \( T \in \{I, \ldots, IV\} \) and \( k \in \{1, \ldots, o_T - 1\} \). In particular, the space \((I_T^{(k)})_N\) contains a unique extremal polynomial of the form

\[
x^N + a_{\delta(I_T^{(k)})}y^{\delta(I_T^{(k)})}x^{N-\delta(I_T^{(k)})} + \cdots + a_N y^N,
\]

i.e. where the sequence formed by the first \( \delta((I_T^{(k)})_N) \) coefficients is \((1,0,\ldots,0)\). Note that the coefficient \( a_{\delta(I_T^{(k)})} \) may be zero. Now if \( k \geq \frac{o_T}{2} \) and \( T \in \{II, III, IV\} \) then the weight enumerator of a dual extremal Type \( T \) code is the extremal element in \((I_T^{(k)})_N\), since always \( d_{\max}(T,N) \leq \delta((I_T^{(k)})_N) \) (cf. Remark 4). In particular, this completes the proof of the uniqueness of the extremal weight enumerator for \( k \geq \frac{o_T}{2} \).

It remains to show that the spaces \( I_T^{(k)} \) have the Weierstrass property. To this aim a triangular basis of \((I_T^{(k)})_N\) is constructed below. The construction starts with an appropriate basis for \( \mathbb{C}[f_T,g_T] \). It is equivalent with the fact that the space \( \mathbb{C}[f_T,g_T] \) has the Weierstrass property (cf. Section 4.2) that

**Corollary 1.** For every integer \( n \) which is a multiple of \( o_T \), the complex vector space \((\mathbb{C}[f_T,g_T])_n\) has a basis \((p_0,\ldots,p_s)\) which is of triangular shape, i.e. \( p_i \) is a multiple of \( y^{m+1} \), for \( i \in \{0,\ldots,s\} \).

Table 5 shows that for every \( k \in \{1,\ldots,o_T - 1\} \), the \( \mathbb{C}[f_T,g_T] \)-module \( I_T^{(k)} \) has a basis \((q_1,\ldots,q_{t_T,k})\) which is triangular as well: If \( i \) is the largest integer such that \( q_j \) is a multiple of \( y^i \), then \( q_{j+1} \) is a multiple of \( y^{i+1} \), for \( j \in \{1,\ldots,t_{T,k} - 1\} \).

Moreover, one observes that in most cases there are some regular “gaps” in the weight distribution of the \( q_j \), i.e. the set \( J_T^{(k)} := \{i \in \mathbb{Z} \mid \text{coef}(q_j(1,y),y^{i+m+1}z) = 0 \text{ for all } j \in \{1,\ldots,t_{T,k}\} \text{ and all } z \in \mathbb{Z}\} \) is non-empty. Since all the weights of an element of \( \mathbb{C}[f_T,g_T] \) are multiples of \( m_T \), it even holds that \( \text{coef}(p(1,y),y^i) = 0 \) for all \( i \in J_T^{(k)} \) and all \( p \in I_T^{(k)} \).

One observes from Table 5 that, metaphorically speaking, if one ignores the columns belonging to the coefficients of \( q_j(1,y) \) at \( y^i \), for \( i \in J_T^{(k)} \), then the triangle formed by the basis vectors \( q_j \) is even isosceles. In particular,

\[
t_{T,k} = \{i \in \{0,\ldots,o_T - 1 \mid i \notin J_T^{(k)} \}\}.
\]

Now one forms a triangular basis of \((I_T^{(k)})_N\), where \( N \equiv k \mod o_T \), as follows. For \( j \in \{1,\ldots,t\} \), let \( \eta_j := \deg(q_j) \). Then \( N - \eta_j \) is a multiple of \( o_T \). Choose a basis \( B_j = \{p_{0,j},\ldots,p_{s,j}\} \) of \((\mathbb{C}[f_T,g_T])_{N-\eta_j}\) as in Corollary 1. Then

\[
\mathcal{C} := \bigcup_{j=1}^{t_{T,k}} \{q_j b \mid b \in B_j\}
\]

is a basis of \((I_T^{(k)})_N\) which, if \( \mathcal{C} = \{c_1,\ldots,c_u\} \) is ordered appropriately, has the property that if \( i \) is the largest integer such that \( c_j \) is a multiple of \( y^i \), then \( c_{j+1} \) is a multiple of \( y^{i+1} \). As an immediate consequence,

**Corollary 2.** The spaces \( I_T^{(k)} \), for \( T \in \{I,\ldots,IV\} \) and \( k \in \{1,\ldots,o_T - 1\} \), have the Weierstrass property.
Table 5. Triangular bases for the spaces $I^{(k)}_T$

| $T'$ | $6$ | Basis for $I^{(k)}_T$ | Coefficients                                                                 |
|------|-----|----------------------|-------------------------------------------------------------------------------|
| I    | 1   | $\text{we}(1_{j})$  | $1 + y$                                                                        |
| I    | 1   | $\text{we}(1_{j})$  | $y + 3y^2 - 4y^3 - 4y^4 + 3y^5 + y^6|_9$                                    |
| I    | 1   | $\text{we}(1_{j})$  | $y + 1y^2 - 23y^3 - 176y^4 + 198y^5 - 23y^6|_{12}$                           |
| I    | 1   | $\text{we}(1_{j})$  | $y + 11y^2 + 19y^3 + y^4|_{17}$                                               |
| I    | 2   | $\text{we}(d_2)$    | $1 + 2y + y^2|_2$                                                             |
| I    | 2   | $\text{we}(d_2)$    | $y - 2y^2 + 2y^3 - 2y^4 + 2y^5 - 2y^6|_{10}$                                |
| I    | 2   | $\text{we}(d_2)$    | $y^2 - 3y^3 - 8y^4 + y^5 - 5y^6 + 10y^7 - 5y^8 + y^9|_{10}$                   |
| I    | 2   | $\text{we}(d_2)$    | $y^3 - 7y^4 - 5y^5 - 7y^6 + y^7 - 5y^8 + 11y^9|_{11, \text{sym}}$             |
| I    | 3   | $\text{we}(d_3)$    | $y^4 + 5y^5 + 6y^6 + 30y^7 - 7y^8 - 11y^9 - 48y^{10} + 96y^{11}$             |
| I    | 3   | $\text{we}(d_3)$    | $y + 10y^2 + 12y^3 + 168y^4|_{13, \text{sym}}$                              |
| II   | 4   | $\text{we}(d_4)$    | $1 + 6y^2 + y^3|_1$                                                            |
| II   | 4   | $\text{we}(d_4)$    | $y^2 + 4y^3 - 12y^4 - 4y^5 + 22y^6|_{12, \text{sym}}$                       |
| II   | 5   | $\text{we}(d_5)$    | $1 + y + 6y^2 + 6y^3 + y^4 + y^5|_6$                                          |
| II   | 5   | $\text{we}(d_5)$    | $y + 3y^2 - 9y^3 + 5y^4 - 6y^5 + 6y^6|_{11, \text{sym}}$                    |
| II   | 5   | $\text{we}(d_5)$    | $y^2 - 2y^3 + 7y^4 - 9y^5 - 3y^6 + 5y^7 - 13y^8 + 13y^9|_{11, \text{sym}}$  |
| II   | 5   | $\text{we}(d_5)$    | $y^3 + y^4 - y^5 - y^6 - 3y^7 - 3y^8 + 3y^9 + 3y^{10}|_{11, \text{sym}}$   |
| II   | 6   | $\text{we}(d_6)$    | $1 + 3y^2 + 8y^3 + 3y^4 + y^5|_{16}$                                          |
| II   | 6   | $\text{we}(d_6)$    | $y^2 - 2y^3 + y^4 - 2y^5 + 4y^6|_{14, \text{sym}}$                          |
| II   | 6   | $\text{we}(d_6)$    | $y^3 + 2y^4 - 2y^5 - 6y^6 + 6y^7 + 6y^8|_{11, \text{sym}}$                  |
| II   | 7   | $\text{we}(d_7)$    | $1 + 5y^2 + 7y^3 + y^4|_2$                                                     |
| II   | 7   | $\text{we}(d_7)$    | $y^3 + 5y^4 - 8y^5 - 16y^6 + 18y^7|_{12, \text{sym}}$                       |
| III  | 1   | $\text{we}(1_{j})$  | $1 + y$                                                                        |
| III  | 1   | $\text{we}(1_{j})$  | $y + 10y^2 - 38y^3 - 26y^4 - 44y^5 - 8y^6|_{10}$                            |
| III  | 2   | $\text{we}(d_2)$    | $1 + y^2 + 4y^3 + y^4|_2$                                                     |
| III  | 2   | $\text{we}(d_2)$    | $y - 2y^2 + y^3 - 4y^4 + 2y^5 + y^6|_{10}$                                   |
| III  | 2   | $\text{we}(d_2)$    | $y^2 - 2y^3 + 2y^4 - 2y^5 - 2y^6|_{11}$                                      |
| III  | 3   | $\text{we}(d_3)$    | $1 + 6y^2 + 2y^3 + 7y^4 - 6y^5 + 9y^6 + 3y^7 - 4y^8|_{11}$                   |
| III  | 3   | $\text{we}(d_3)$    | $y^2 + 3y^3 - 6y^4 + 9y^5 + 3y^6 - 4y^7|_{11}$                               |
| IV   | 1   | $\text{we}(1_{j})$  | $1 + 3y^2|_1$                                                                 |
| IV   | 1   | $\text{we}(1_{j})$  | $y + 2y^2 - 4y^3 - 2y^4 + 3y^5|_5$                                           |
As announced above, the last necessary result, which is easy to verify by induction
on \( N \), e.g., to prove the uniqueness of the extremal weight enumerator of a maximal
Type \( T \) code is

**Remark 4.** \( d_{\text{max}}(T, N) \leq \delta((I_T^{(k)})_N). \)

In Table 5, all polynomials are given, evaluated at \( x = 1 \), to shorten notation. A
small index indicates the total degree. If a polynomial \( p \) is symmetric, i.e. \( p(x, y) =
 p(y, x) \), then its redundant coefficients are omitted, which is indicated by an index
\( \text{sym} \). For instance, \( [y + 3y^2 - 9y^3 + 5y^4 - 6y^5 + 6y^6]_{\text{sym}} \) denotes the polynomial
\[
\begin{align*}
x^{12}y + 3x^{11}y^2 - 9x^{10}y^3 + 5x^9y^4 - 6x^8y^5 + 6x^7y^6 \\
+ 6x^6y^7 - 6x^5y^8 + 5x^4y^9 - 9x^3y^{10} + 3x^2y^{11} + xy^{12}.
\end{align*}
\]

In addition, Table 5 describes how these polynomials can be obtained from weight
enumerators of maximal Type \( T \) codes. For the notation of these codes, the reader
is referred to [6].

5. Extremal polynomials and extremal codes

Let \( T \in \{I, \ldots, IV\} \) and let \( k, N \) be integers with \( 1 \leq k \leq o_T - 1 \) and \( N \equiv k \pmod{o_T} \). Recall from Section 4 that there exists a unique extremal element \( p \in (U_T^{(k)})_N \),
of the form
\[
p(x, y) = x^{-N} + a_{(I_T^{(k)})_N}y^\delta((I_T^{(k)})_N)x^{-N-\delta((I_T^{(k)})_N)} + \cdots + a_Ny^N.
\]

Of course \( p \) is not necessarily the weight enumerator of a code. However, it is
interesting to observe that for small lengths \( N \), say up to 4000, the position of the
least non-vanishing coefficient in \( p \), i.e.
\[
d(p) := \min\{i \in \{\delta((I_T^{(k)})_N), \ldots, N\} \mid a_i \neq 0\}
\]
satisfies the upper bound on the dual minimum distance of a putative maximal
Type \( T \) code of length \( N \). This could probably be proven for arbitrary \( N \) using the
B¨ urmann-Lagrange formula. In this section, though, it is shown that the extension
procedure introduced in Section 2 can, to some extent, be useful to this aim, too.
Regrettably, the shortening process fails to provide any upper bounds on \( d(p) \). It
is shown in Theorem 9 that this is not a weakness of this particular shortening
procedure, but that there exists no shortening procedure at all which is useful to
this aim.

5.1. A \( \mathbb{C}[f_T, g_T] \)-module homomorphism induced by code extension. Assume
that \( N = k + n \cdot o_T \), where \( k \geq \frac{2T}{T-1} \) (here we exclude the exceptional case
\( T = 2 \) and \( k = 4 \)). Let \( C \) be a maximal Type \( T \) code of length \( N \). It is easy to
observe that if \( D \) is a self-dual Type \( T \) code, then \( \text{ext}(D \oplus C) = D \oplus \text{ext}(C) \). This
suggests to define a \( \mathbb{C}[f_T, g_T] \)-module homomorphism
\[
\alpha : I_T^{(k)} \rightarrow \mathbb{C}[f_T, g_T], \quad \text{we}(C_i) \mapsto \text{we}(\text{ext}(C_i)),
\]
where the \( \text{we}(C_i) \) form a \( \mathbb{C}[f_T, g_T] \)-basis for \( I_T^{(k)} \). Recall that the weight distribution
of the extended code \( \text{ext}(C) \), of length \( N + o_T - k \), can easily be read off from the
weight distribution of \( C \) (cf. Remark 1). Hence

**Remark 5.** If \( C \) is a maximal Type \( T \) code then \( \alpha(\text{we}(C)) = \text{we}(\text{ext}(C)) \), i.e. the
map \( \alpha \) extends the effect of the extension procedure on the weight enumerator to a
homomorphism of \( \mathbb{C}[f_T, g_T] \)-modules.
This allows to upper bound the generalized minimum distance of polynomials in $I_T^{(k)}$.

**Definition 6.** Let $p \in \mathbb{C}[x, y]$ be a homogeneous polynomial of degree $N$, of the form

$$p(x, y) = x^N + a_d y^d x^{N-d} + \cdots + a_N y^N.$$  

Then the integer $d := d(p)$ is called the generalized minimum distance of $p$.

**Corollary 3.** If $k \geq \frac{d_T}{2}$ and $p \in I_T^{(k)}$ is homogeneous of degree $N$, such that $d(p)$ is defined, then $d(p) \leq d(\alpha(p)) \leq d_{\max}(T, N + \sigma_T - k)$.

As mentioned above, explicit calculations (the author used Magma) show that under the assumptions of Corollary 3, even $d(p) \leq d_{\max}(T, N)$ for small lengths $N$. The author conjectures that this holds for arbitrary $N$, but at the present state of our knowledge, this question has to remain open for future research.

5.2. $\mathbb{C}[f_T, g_T]$-module homomorphisms induced by shortening - A nonexistence result. In this section, assume that $T \in \{\text{II, III}\}$ and $N = k + \sigma_T$, where $k \in \{1, \ldots, \frac{d_T}{2} - 1\}$. We prove the nonexistence of a shortening procedure that is well-defined on the weight enumerator level and gives rise to a $\mathbb{C}[f_T, g_T]$-module homomorphism which allows to upper bound $d(p)$, for $p \in I_T^{(k)}$.

**Theorem 9.** There exists no $\mathbb{C}[f_T, g_T]$-module homomorphism $\alpha : I_T^{(k)} \rightarrow \mathbb{C}[f_T, g_T]$ such that

(1) if $C$ is a maximal Type $T$ code of length $N$, then $\alpha(C)$ is a self-dual Type $T$ code of length $N - k$ and

(2) $d(\alpha(p)) \geq d(p) - k$ for all $p \in I_T^{(k)}$ where $d(p)$ is defined.

**Proof.** We give the proof in the case $T = \text{III}$ and $k = 1$ (the other cases, i.e. $T = \text{II}$ and $k \in \{1, 2, 3\}$, are similar). The $\mathbb{C}[f_T, g_T]$-module $I_T^{(1)}$ has a basis $(\text{we}(i_1), \text{we}(e_3^{++}))$, according to Table 5 (see also [6, Ch. 10]). Assume that $\alpha$ is a $\mathbb{C}[f_{\text{III}}, g_{\text{III}}]$-module homomorphism that satisfies the first condition of the theorem. Then $\alpha(\text{we}(i_1)) = 1$ and $\alpha(\text{we}(e_3^{++})) = \text{we}(t_4)^2$. Let $p$ be the extremal element of $I_T^{(1)}$, then $d(p) = 7 = d_{\max}(\text{III}, 25)$. But $d(\alpha(p)) = 3 < 7 - 1 = 6$, which contradicts the second condition. This shows the assertion. \qed

**References**

[1] C. Bachoc and P. Gaborit, Designs and self-dual codes with long shadows, J. Combin. Theory, 105 (2004), 15–34.

[2] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory, 36 (1990), 1319–1333.

[3] P. Gaborit, A bound for certain s-extremal lattices and codes, Arch. Math. (Basel), 89 (2007), 143–151.

[4] A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in “Actes, Congr. Int. Math.” (ed. P. Gauthier-Villars), 3 (1971), 211–215.

[5] W. C. Huffman and V. Pless, “Fundamentals of Error-Correcting Codes,” Cambridge University Press, Cambridge, 2003.

[6] G. Nebe, E. M. Rains and N. J. A. Sloane, “Self-Dual Codes and Invariant Theory,” Springer, Berlin, 2006.

[7] M. Ozeki, On intersection properties of extremal ternary codes, J. Math. Industry, 1 (2009), 105–121.

[8] V. Pless, W. C. Huffman and R. A. Brualdi (eds.), “Handbook of Coding Theory,” North-Holland, Amsterdam, 1998.
[9] V. Pless, N. J. A. Sloane and H. N. Ward, *Ternary codes of minimum weight 6, and the classification of length 20*, IEEE Trans. Inform. Theory, 26 (1980), 305–316.

[10] E. M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory, 44 (1998), 134–139.

[11] W. Scharlau, *Quadratic and Hermitian forms*, in “Grundlehren der Mathematischen Wissenschaften,” Springer-Verlag, 1985.

[12] N. J. A. Sloane, *Gleason’s Theorem on self-dual codes and its generalizations*, preprint, arXiv:math/0612535

Received February 2010; revised September 2010.

E-mail address: annika.meyer@math.rwth-aachen.de