An analogue of the Pless symmetry codes

Gabriele Nebe and Darwin Villar

Lehrstuhl D für Mathematik, RWTH Aachen University
52056 Aachen, Germany
nebe@math.rwth-aachen.de

Abstract. A series of monomial representations of $SL_2(p)$ is used to construct a new series of self-dual ternary codes of length $2(p+1)$ for all primes $p \equiv 5 \pmod{8}$. In particular we find a new extremal self-dual ternary code of length 60.

Keywords: extremal self-dual code, automorphism group, monomial representations

MSC: primary: 94B05

1 Introduction.

In 1969 Vera Pless [7] discovered a family of self-dual ternary codes $P(p)$ of length $2(p+1)$ for primes $p$ with $p \equiv -1 \pmod{6}$. Together with the extended quadratic residue codes $XQR(q)$ of length $q+1$ ($q$ prime, $q \equiv \pm 1 \pmod{12}$) they define a series of self-dual ternary codes of high minimum distance (see [4, Chapter 16, §8]). For $p = 5$, the Pless code $P(5)$ coincides with the Golay code $g_{12}$ which is also the extended quadratic residue code $XQR(11)$ of length 12.

Using invariant theory of finite groups, A. Gleason [2] has shown that the minimum distance of a self-dual ternary code of length $4n$ cannot exceed $3\lfloor \frac{3n}{2} \rfloor + 3$. Self-dual codes that achieve equality are called extremal. Both constructions, the Pless symmetry codes and the extended quadratic residue codes yield extremal ternary self-dual codes for small values of $p$.

This short note gives an interpretation of the Pless codes using monomial representations of the group $SL_2(p)$. This construction allows to read off a large subgroup of the automorphism group of the Pless codes (which was already described in [7]). A different but related series of monomial representations of $SL_2(p)$ is investigated to construct a new series of self-dual ternary codes $V(p)$ of length $2(p+1)$ for all primes $p \equiv 5 \pmod{8}$. The automorphism group of $V(p)$ contains the group $SL_2(p)$. For $p = 5$ we again find $V(5) \cong g_{12}$ the Golay code of length 12, but for larger primes these codes are new. In particular the code $V(29)$ is an extremal ternary code of length 60, so we now know three extremal ternary codes of length 60: $XQR(59)$, $P(29)$ and $V(29)$. 

1
2 Codes and monomial groups.

Let $K$ be a field, $n \in \mathbb{N}$. Then the monomial group $\text{Mon}_n(K^*) \leq \text{GL}_n(K)$ is the group of monomial $n \times n$-matrices over $K$, where a matrix is called monomial, if it contains exactly one non-zero entry in each row and each column. So $\text{Mon}_n(K^*) \cong K^* \wr S_n \cong (K^* )^n : S_n$ is the semidirect product of the subgroup $(K^* )^n$ of diagonal matrices in $\text{GL}_n(K)$ with the group of permutation matrices. For any subgroup $S \leq K^*$ we define $\text{Mon}_n(S) := S^n \wr S_n$ to be the subgroup of monomial matrices having all non-zero entries in $S$. There is a natural epimorphism $\pi : \text{Mon}_n(S) \to S_n$ mapping any monomial matrix to the associated permutation.

By MacWilliam’s extension theorem ([3], see also [8]) any $K$-linear weight preserving isomorphism between two subspaces of $K^n$ is the restriction of a monomial transformation in $\text{Mon}_n(K^*)$. This justifies the following commonly used notion of equivalence of codes, which also motivates the investigation of monomial representations of finite groups to find good codes with large automorphism group.

**Definition 1.** A $K$-code $C$ of length $n$ is a subspace of $K^n$. Two codes $C$ and $C'$ of length $n$ are called monomially equivalent, if there is some $g \in \text{Mon}_n(K^*)$ such that $Cg = C'$. The monomial automorphism group of $C$ is $\text{Aut}(C) := \{ g \in \text{Mon}_n(K^*) | Cg = C \}$.

3 Endomorphism rings of monomial representations.

The theory exposed in this section is well known, a nice explicit formulation is contained in [5, Section I (1)]. Let $G$ be some group. A linear $K$-representation $\Delta$ of degree $n$ is a group homomorphism $\Delta : G \to \text{GL}_n(K)$. The representation is called monomial, if its image $\Delta(G)$ is conjugate in $\text{GL}_n(K)$ to some subgroup of $\text{Mon}_n(K^*)$. We call the monomial representation transitive, if $\pi(\Delta(G))$ is a transitive subgroup of $S_n$. In this case the set $\{ h \in G | 1 \pi(\Delta(h)) = 1 \} =: H$ is a subgroup of index $n$ in $G$ and $\Delta$ is obtained by inducing up a degree 1 representation of $H$ as follows:

Let $H$ be a subgroup of $G$ of index $n := [G : H]$. Choose $g_1, \ldots, g_m \in G$ such that

$$G = \bigcup_{\ell=1}^{m} H g_\ell H$$

and put $H_\ell := H \cap g_\ell^{-1} H g_\ell$. Choose some right transversal $h_{\ell,j}$ of $H_\ell$ in $H$, so that $h_{\ell,1} = 1$ and $H = \bigcup_{j=1}^{k_\ell} H h_{\ell,j}$. Then

$$G = \bigcup_{\ell=1}^{m} \bigcup_{j=1}^{k_\ell} H g_\ell h_{\ell,j}$$
and the right transversal \( \{ gh \ell, j \mid \ell = 1, \ldots, m, k = 1, \ldots, k_\ell \} \) is a set of cardinality \( n \) which we will use as an index set of our \( n \times n \)-matrices.

For a group homomorphism \( \lambda : H \to K^* \) the associated monomial representation of \( G \) is \( \Delta := \lambda^G_H : G \to \text{Mon}_n(\lambda(H)) \) defined by

\[
(\lambda^G_H(g))_{gh \ell, j, g' h' \ell', j'} = \begin{cases} 
0 & \text{if } gh \ell, j g(g' h'_{\ell', j'})^{-1} \not\in H \\
\lambda(gh \ell, j g(g' h'_{\ell', j'})^{-1}) & \text{if } gh \ell, j g(g' h'_{\ell', j'})^{-1} \in H
\end{cases}.
\]

The representation \( \lambda \) restricts in two obvious ways to a representation of \( H_\ell \):

\[
\lambda_\ell : H_\ell \to K^*, h \mapsto \lambda(h) \text{ and } \lambda^{0\ell}_\ell : H_\ell \to K^*, h \mapsto \lambda(hg_\ell h_\ell^{-1}).
\]

Let \( \mathcal{I} := \{ \ell \in \{1, \ldots, m\} \mid \lambda_\ell = \lambda^{0\ell}_\ell \} \) and reorder the double coset representatives so that \( \mathcal{I} = \{1, \ldots, d\} \). Then the endomorphism ring

\[
\text{End}(\Delta) := \{ X \in K^{n \times n} \mid X \Delta(g) = \Delta(g)X \text{ for all } g \in G \}
\]

has dimension \( d \) and the Schur basis of \( \text{End}(\Delta) \) is \( (B_1 = I_n, B_2, \ldots, B_d) \) where \( (B_\ell)_{gh \ell, j} = 1 \) and \( (B_\ell)_{gh \ell, j} \neq 0 \) if and only if \( \ell = k \). As \( \Delta(h_{\ell,k})B_\ell = B_\ell \Delta(h_{\ell,k}) \) we conclude

\[
\lambda(h_{\ell,k})(B_\ell)_{gh \ell, j} = \Delta(h_{\ell,k})g_{\ell, g} h_{\ell, j} = \lambda(h_{\ell,k})\lambda(h_{\ell,j}^{-1})
\]

so \( (B_\ell)_{gh \ell, j} = \lambda(h_{\ell,j})^{-1} \) for all \( j \). More generally we get

**Lemma 2.** \( (B_\ell)_{gk h_{k,i}, gk' h'_{k',i'}} = 0 \) if \( g k h_{k,i} h_{k,i}^{-1} h_{k,i}^{-1} \not\in H g H \). Otherwise write \( g k h_{k,i} h_{k,i}^{-1} h_{k,i}^{-1} g k^{-1} = h g h_{\ell,j} \) for some \( h \in H \). Then \( (B_\ell)_{gk h_{k,i}, gk' h'_{k',i'}} = \lambda(h)^{-1} \lambda(h_{\ell,j}^{-1}) \).

**Proof.** To see this we choose \( g = (g k h_{k,i})^{-1} \in G \). Then \( \Delta(g) g k h_{k,i} = 1 \) and hence

\[
(\Delta(g) B_\ell)_{gk h_{k,i}, gk h_{\ell,j}} = \Delta(g)_{gk h_{k,i}} (B_\ell)_{gh \ell, j} = \lambda(h_{\ell,j})^{-1}.
\]

On the other hand

\[
(B_\ell \Delta(g))_{gk h_{k,i}, gh \ell, j} = (B_\ell)_{gk h_{k,i}, gk h_{k,i} h_{k,i}^{-1} h_{k,i}^{-1} (g k h_{\ell,j})^{-1}} \Delta(g)_{gk h_{k,i} h_{k,i}^{-1} h_{k,i}^{-1}, gh \ell, j}
\]

for the unique \((k', i')\) such that

\[
h := g k h_{k,i} (g k h_{k,i})^{-1} (g k h_{\ell,j})^{-1} \in H
\]

and then \( \Delta(g)_{gk h_{k,i} h_{k,i}^{-1} h_{k,i}^{-1}, gh \ell, j} = \lambda(h) \). As \( \Delta(g) B_\ell = B_\ell \Delta(g) \) we compute

\[
\lambda(h_{\ell,j})^{-1} = (B_\ell)_{gk h_{k,i}, gk' h'_{k',i'}} \lambda(h).
\]

□

3
4 Generalized Pless codes.

In this section we reinterpret the construction of the famous Pless symmetry codes \( P(p) \) discovered by Vera Pless [7], [6]. Explicit generator matrices for the Pless codes may be obtained from the endomorphism ring of a monomial representation. Let \( p \) be an odd prime and

\[
\text{SL}_2(p) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_p^{2\times2} \mid ad - bc = 1 \}
\]

the group of \( 2 \times 2 \)-matrices over the finite field \( \mathbb{F}_p \) with determinant 1. Let

\[
B := \{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \text{SL}_2(p) \} = \langle h_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \zeta := \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \rangle.
\]

Then \( B \) is a subgroup of \( \text{SL}_2(p) \) or index \( p + 1 \), isomorphic to the semidirect product \( C_p : C_{p-1} \), with center \( Z(B) = Z(\text{SL}_2(p)) = \langle \zeta^{(p-1)/2} \rangle = \{ \pm I_2 \} \). Let

\[
\lambda : B \to K^*, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto 1, \zeta \mapsto -1
\]

Then \( \lambda(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}) = \left( \frac{a}{p} \right) \) is just the Legendre symbol of the upper left entry. Let

\[
\Delta := \lambda^{\text{SL}_2(p)} : \text{SL}_2(p) \to \text{Mon}_{p+1}(K^*)
\]

be the monomial representation induced by \( \lambda \). The following facts about this representation are well known, and easily computed from the general description in the previous section.

**Remark 3.**

1. (Gauß-Bruhat decomposition) \( \text{SL}_2(p) = B \cup BwB \) where \( w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \).
2. \( B \cap wBw^{-1} = \langle \zeta \rangle \).
3. A right transversal of \( B \) in \( \text{SL}_2(p) \) is given by \( [1, wh_x : x \in \mathbb{F}_p] \) where \( h_x := \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in B. \)
The Schur basis of $\text{End}(\Delta)$ is $(I_{p+1}, P)$, where $P_{1,1} = 0$, $P_{1,x} = 1$ for all $x$. Then $P_{wh_x,1} = \left( \frac{-1}{p} \right)$ and 

$$
P_{wh_x,wh_y} = \begin{cases} 
\left( \frac{x-y}{p} \right) & x \neq y \\
0 & x = y.
\end{cases}
$$

(5) $P^2 = \left( \frac{-1}{p} \right) p$ and $PP^\text{tr} = p$.

To construct monomial representations of degree $2(p+1)$ we consider the group 

$$
\mathcal{G}(p) := \left\{ \left( \begin{array}{cc} \Delta(g) & 0 \\
0 & \Delta(g) \end{array} \right) \mid g \in \text{SL}_2(p) \right\} \leq \text{Mon}_{2(p+1)}(K^*)
$$

where $j = -\left( \frac{-1}{p} \right) = \begin{cases} 
1 & p \equiv 3 \pmod{4} \\
-1 & p \equiv 1 \pmod{4}.
\end{cases}$

Remark 4. (1) $\mathcal{G}(p) \cong \begin{cases} 
C_4 \times \text{PSL}_2(p) & p \equiv 1 \pmod{4} \\
C_2 \times \text{SL}_2(p) & p \equiv 3 \pmod{4}
\end{cases}$

(2) $\text{End}(\mathcal{G}(p)) = \left\{ \left( \begin{array}{cc} A & B \\
jB & A \end{array} \right) \mid A, B \in \text{End}(\Delta) \right\}$ is generated by 

$$
I_{2(p+1)}, X := \left( \begin{array}{cc} P & 0 \\
0 & P \end{array} \right), Y := \left( \begin{array}{cc} 0 & I_{p+1} \\
jI_{p+1} & 0 \end{array} \right), XY = \left( \begin{array}{cc} 0 & P \\
jP & 0 \end{array} \right)
$$

with $X^2 = -jp$, $Y^2 = j$, $XY = YX$, $(XY)^2 = -p$.

Definition 5. Let $K = \mathbb{F}_q$ be the finite field with $q$ elements and assume that there is some $a \in K^*$ such that $a^2 = -p$. Then we put $P_q(p) := aI_{2(p+1)} + XY \in \text{End}(\mathcal{G}(p))$ and define the generalized Pless code $P_q(p) \leq K^{2(p+1)}$ to be the code spanned by the rows of $P_q(p)$.

Theorem 6. Let $a \in \mathbb{F}_q^*$ such that $a^2 = -p$. The code $P_q(p)$ has generator matrix $(aI_{p+1}P)$ and is a self-dual code in $\mathbb{F}_q^{2(p+1)}$. $d(P_q(p)) \leq (p + 7)/2$ if $q$ is odd and $d(P_q(p)) \leq 4$ if $q$ is even.

The group $\mathcal{G}(p)$ is a subgroup of $\text{Aut}(P_q(p))$.

Proof. By construction the group $\mathcal{G}(p)$ is a subgroup of $\text{Aut}(P_q(p))$. As $PP^\text{tr} = pI_{p+1} = -a^2I_{p+1}$ the code $P_q(p)$ is self-dual with respect to the standard inner product.
The upper bound on the minimum distance is obtained by adding the first two rows of the generator matrix \((aI_{p+1} - 1)\). The sum has weight 4 if \(q\) is even. If \(q\) is odd then the first row of \(P\) is \((0, 1^p)\) and the second row of \(P\) is \((-1, 0, v)\) where \(v \in \{±1\}^{p−1}\) has exactly \((p−1)/2\) ones and \((p−1)/2\) minus ones. \(□\)

**Remark 7.** For \(K = \mathbb{F}_3\) and \(p ≡ −1 \pmod{3}\) we may choose \(a = 1\) and the generator matrix of \(P_3(p)\) is the one for the Pless symmetry code \(P(p)\) as given in [7].

With Magma [1] we compute the following invariants of first few Pless codes:

<table>
<thead>
<tr>
<th>(p)</th>
<th>(2(p+1))</th>
<th>5</th>
<th>11</th>
<th>17</th>
<th>23</th>
<th>29</th>
<th>41</th>
<th>47</th>
</tr>
</thead>
<tbody>
<tr>
<td>(d(P_3(p)))</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>18</td>
<td>21</td>
<td>24</td>
<td>28</td>
<td>36</td>
</tr>
<tr>
<td>(\text{Aut}(P_3(p)))</td>
<td>(G(11, 2))</td>
<td>(G(17, 2))</td>
<td>(G(23, 2))</td>
<td>(G(29, 2))</td>
<td>(G(41))</td>
<td>(G(47))</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For \(q = 5, 7,\) and 11 we computed \(d(P_q(p))\) with Magma:

<table>
<thead>
<tr>
<th>((p, q))</th>
<th>((11, 5))</th>
<th>((19, 5))</th>
<th>((29, 5))</th>
<th>((31, 5))</th>
<th>((3, 7))</th>
<th>((5, 7))</th>
<th>((11, 7))</th>
<th>((17, 7))</th>
<th>((19, 7))</th>
<th>((7, 11))</th>
<th>((13, 11))</th>
<th>((17, 11))</th>
<th>((19, 11))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2(p+1))</td>
<td>12</td>
<td>40</td>
<td>60</td>
<td>64</td>
<td>8</td>
<td>12</td>
<td>28</td>
<td>36</td>
<td>40</td>
<td>16</td>
<td>28</td>
<td>36</td>
<td>40</td>
</tr>
<tr>
<td>(d(P_q(p)))</td>
<td>9</td>
<td>13</td>
<td>18</td>
<td>18</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>12</td>
<td>13</td>
<td>7</td>
<td>10</td>
<td>12</td>
<td>13</td>
</tr>
</tbody>
</table>

5 A new series of self-dual codes invariant under \(\text{SL}_2(p)\).

Applying the same strategy as in the previous section we now construct a monomial representation of \(\text{SL}_2(p)\) of degree \(2(p+1)\) where \(p\) is a prime so that \(p−1 ≡ 4 \pmod{8}\). We assume that \(\text{char}(K) ≠ 2\).

Then the subgroup \(B^{(2)} := \left\{ \begin{pmatrix} a^2 & 0 \\ b & a^{−2} \end{pmatrix} \mid a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\} \leq \text{SL}_2(p)\) of index \(2(p+1)\) in \(\text{SL}_2(p)\) has a unique linear representation \(γ : B^{(2)} \to K^*\) with \(γ(B^{(2)}) = \{±1\}\), so \(γ\left( \begin{pmatrix} a^2 & 0 \\ b & a^{−2} \end{pmatrix} \right) = \left( \frac{a}{p} \right)\). Then \(Δ' := γ_{\text{SL}_2(p)}\) is a faithful monomial representation of degree \(2(p+1)\).

To obtain explicit matrices we choose \(w := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\) as above. By assumption \(2 \in \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2\), put \(\epsilon := \text{diag}(2, 2^{−1})\). Then \(B = B^{(2)} \cup B^{(2)}\epsilon\) and

\[
\text{SL}_2(p) = B \cup BwB = B^{(2)} \cup B^{(2)}wB^{(2)} \cup B^{(2)}\epsilon \cup B^{(2)}\epsilon wB^{(2)}
\]
and a right transversal is given by \([1, wh_x, \epsilon, \epsilon wh_x : x \in \mathbb{F}_p]\) where \(h_x := \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in B^{(2)}\).

**Lemma 8.** \(\text{End}(\Delta')\) has a Schur basis \((B_1, B_w, B_\epsilon, B_{\epsilon w} = B_\epsilon B_w)\) where \(B_\epsilon = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\) and \(B_w = \begin{pmatrix} X & Y \\ -Y^t & X^t \end{pmatrix}\) with

\[
X = \begin{pmatrix} 0 & 1 & \ldots & 1 \\ & & -1 \\ & \vdots & & R_X \\ -1 & & & \end{pmatrix},
Y = \begin{pmatrix} 0 & 0 & \ldots & 0 \\ & & \vdots & R_Y \\ & & & 0 \end{pmatrix}
\]

where rows and columns of \(R_X\) and \(R_Y\) are indexed by the elements \(\{0, \ldots, p-1\}\) of \(\mathbb{F}_p\) and

\[
(R_X)_{a,b} = \begin{cases} 0 & b - a \not\in (\mathbb{F}_p)^2 \\ \left(\frac{a}{p}\right) & b - a = c^2 \in (\mathbb{F}_p)^2 \end{cases},
(R_Y)_{a,b} = \begin{cases} 0 & 2(b - a) \not\in (\mathbb{F}_p)^2 \\ \left(\frac{b}{p}\right) & 2(b - a) = c^2 \in (\mathbb{F}_p)^2 \end{cases}
\]

**Proof.** Explicit computations with the general formulas in Lemma 2. For instance \((B_w)_{wh_x,wh_y} \neq 0\) if and only if

\[
wh_x-pw^{-1} = \begin{pmatrix} 1 & y-x \\ 0 & 1 \end{pmatrix} \in B^{(2)}_w B^{(2)}.
\]

This is equivalent to \(y - x = a^2\) for some \(a \in \mathbb{F}_p\) and then

\[
wh_x-yw^{-1} = \begin{pmatrix} a^2 & 0 \\ 1 & a^{-2} \end{pmatrix} w \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}
\]

and hence \((B_w)_{wh_x,wh_y} = \left(\frac{a}{p}\right).\)

**Remark 9.** Note that \((-1) = c^2\) is a square but not a 4th power, so \(\left(\frac{a}{p}\right) = -1\) and hence \(X\) is skew symmetric and \(B^{tr}_w = -B_w, B^{tr}_{\epsilon w} = -B_{\epsilon w}\). We compute that \(B^2_w = B^2_{\epsilon w} = -p\) and \(B^2_{\epsilon} = -1\) so \(\text{End}(\Delta') \cong \left(\frac{-2}{K}\right)\) is isomorphic to a quaternion algebra over \(K\). We also compute that \((B_w + B_{\epsilon w})^2 = -2p.\)
Definition 10. Let \( p \) be a prime \( p \equiv 8 \mod 5 \), \( K = \mathbb{F}_q \) so that there is some \( a \in K^* \) such that \( a^2 = -tp \) for \( t = 1 \) or \( t = 2 \). We then put

\[
V_t(p) := \begin{cases} 
  aI_{2(p+1)} + B_w & t = 1 \\
  aI_{2(p+1)} + B_w + B_{cw} & t = 2 
\end{cases}
\]

and let \( V_q(p) \) be the linear code spanned by the rows of \( V_t(p) \).

Theorem 11. \( V_q(p) \) is a self-dual code in \( \mathbb{F}_q^{2(p+1)} \). Its monomial automorphism group contains the group \( \text{SL}_2(p) \).

Proof. By construction the code \( V_q(p) \) is invariant under \( \text{SL}_2(p) \). To see that \( V_q(p) \) is self-orthogonal we check that

\[
V_1(p)V_1(p)^{tr} = (a + B_w)(a + B_w^{tr}) = a^2 + a(B_w + B_w^{tr}) + B_wB_w^{tr} = a^2 - B_w^2 = 0 \\
V_2(p)V_2(p)^{tr} = (a + B_w + B_{cw})(a + B_w^{tr} + B_{cw}^{tr}) = a^2 - (B_w + B_{cw})^2 = 0.
\]

To obtain the rank of the matrix \( V_t(p) \) we note that \( \text{End}(\Delta') \cong \left( \frac{\mathbb{F}_q}{2} \right) \cong \mathbb{F}_q^{2 \times 2} \). So the representation \( \Delta' \) is the sum of two equivalent representations over \( \mathbb{F}_q \). These have the same degree, \( p + 1 \), half of the degree of \( \Delta' \) and therefore \( p + 1 \) divides the rank of any matrix in \( \text{End}(\Delta') \). \( \square \)

Remark 12. The matrices of rank \( p + 1 \) in \( \text{End}(\Delta') \) yield \( q + 1 \) different self-dual codes invariant under \( \Delta'(\text{SL}_2(p)) \). In general these fall into different equivalence classes. For instance for \( q = 7 \), where 2 is a square mod 7, the codes spanned by the rows of \( V_1(p) \) and \( V_2(p) \) are inequivalent for \( p = 5 \) and \( p = 13 \) but have the same minimum distance.

The first few codes \( V_3(p) \) have the following parameters (computed with Magma [1]):

<table>
<thead>
<tr>
<th>( p )</th>
<th>5</th>
<th>13</th>
<th>29</th>
<th>37</th>
<th>53</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2(p+1) )</td>
<td>12</td>
<td>28</td>
<td>60</td>
<td>76</td>
<td>108</td>
</tr>
<tr>
<td>( d(V_3(p)) )</td>
<td>6</td>
<td>9</td>
<td>18</td>
<td>18</td>
<td>24</td>
</tr>
<tr>
<td>( \text{Aut}(V_3(p)) )</td>
<td>2.M_{12}</td>
<td>SL_2(13)</td>
<td>SL_2(29)</td>
<td>\geq SL_2(37)</td>
<td>\geq SL_2(53)</td>
</tr>
</tbody>
</table>

For \( q = 5, 7, \) and 11 and small lengths we computed \( d(V_q(p)) \) with Magma:

<table>
<thead>
<tr>
<th>( (p,q) )</th>
<th>( (13, 5) )</th>
<th>( (29, 5) )</th>
<th>( (5, 7) )</th>
<th>( (13, 7) )</th>
<th>( (5, 11) )</th>
<th>( (13, 11) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2(p+1) )</td>
<td>28</td>
<td>60</td>
<td>12</td>
<td>28</td>
<td>12</td>
<td>28</td>
</tr>
<tr>
<td>( d(V_3(p)) )</td>
<td>10</td>
<td>16</td>
<td>6</td>
<td>9</td>
<td>7</td>
<td>11</td>
</tr>
</tbody>
</table>
References


