Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 158-163*

An analogue of the Pless symmetry codes

Gabriele Nebe nebe@math.rwth-aachen.de
Darwin Villar darwin.villar@rwth-aachen.de
Lehrstuhl D für Mathematik, RWTH Aachen University
52056 Aachen, Germany

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. A series of monomial representations of $\mathrm{SL}_2(p)$ 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.

1 Introduction

In 1969 Vera Pless [6] discovered a family of self-dual ternary codes $\mathcal{P}(p)$ of length $2(p+1)$ for primes p with $p \equiv -1 \pmod 6$. Together with the extended quadratic residue codes $\mathrm{XQR}(q)$ 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 [3, Chapter 16, §8]). For $p = 5$, the Pless code $\mathcal{P}(5)$ coincides with the Golay code $\mathfrak{g}_{12}$ which is also the extended quadratic residue code $\mathrm{XQR}(11)$ 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 $3\lfloor \frac{n}{12} \rfloor + 3$. 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 $\mathrm{SL}_2(p)$. This construction allows to read off a large subgroup of the automorphism group of the Pless codes (which was already described in [6]). A different but related series of monomial representations of $\mathrm{SL}_2(p)$ is investigated to construct a new series of self-dual ternary codes $\mathcal{V}(p)$ of length $2(p+1)$ for all primes $p \equiv 5 \pmod 8$. The automorphism group of $\mathcal{V}(p)$ contains the group $\mathrm{SL}_2(p)$. For $p = 5$ we again find $\mathcal{V}(5) \cong \mathfrak{g}_{12}$ the Golay code of length 12, but for larger primes these codes are new. In particular the code $\mathcal{V}(29)$ is an extremal ternary code of length 60, so we now know three extremal ternary codes of length 60: $\mathrm{XQR}(59)$, $\mathcal{P}(29)$ and $\mathcal{V}(29)$.

2 Codes and monomial groups

Let K be a field, $n \in \mathbb{N}$. Then the **monomial group** $\mathrm{Mon}_n(K^*) \leq \mathrm{GL}_n(K)$ 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 $\mathrm{Mon}_n(K^*) \cong K^* \wr S_n \cong (K^*)^n : S_n$ is the semidirect product of the subgroup $(K^*)^n$ of diagonal matrices in $\mathrm{GL}_n(K)$ with the group of permutation matrices. For any subgroup $S \leq K^*$ we define $\mathrm{Mon}_n(S) := S^n \wr S_n$ to be the subgroup of monomial matrices having all non-zero entries in S. There is a natural epimorphism $\pi : \mathrm{Mon}_n(S) \to S_n$ mapping any monomial matrix to the associated permutation.

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 $g \in \mathrm{Mon}_n(K^*)$ such that $Cg = C'$. The* **monomial automorphism group** *of C is $\mathrm{Aut}(C) := \{g \in \mathrm{Mon}_n(K^*) \mid Cg = C\}$.*

Let G be some group. A linear K-representation Δ of degree n is a group homomorphism $\Delta : G \to \mathrm{GL}_n(K)$. The representation is called **monomial**, if its image $\Delta(G)$ is conjugate in $\mathrm{GL}_n(K)$ to some subgroup of $\mathrm{Mon}_n(K^*)$. We call the monomial representation **transitive**, if $\pi(\Delta(G))$ is a transitive subgroup of S_n. In this case the set $\{h \in G \mid 1\pi(\Delta(h)) = 1\} =: H$ is a subgroup of index n in G and Δ 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

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

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

$$G = \dot\bigcup_{\ell=1}^{m} \dot\bigcup_{j=1}^{k_\ell} H g_\ell h_{\ell,j}$$

and the right transversal $\{g_\ell h_{\ell,j} \mid \ell = 1, \ldots, m, k = 1, \ldots, k_\ell\}$ 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 $\Delta := \lambda_H^G : G \to \mathrm{Mon}_n(\lambda(H))$ defined by

$$(\lambda_H^G(g))_{g_\ell h_{\ell j}, g_{\ell'} h_{\ell',j'}} = \begin{cases} 0 & \text{, if } g_\ell h_{\ell j} g (g_{\ell'} h_{\ell',j'})^{-1} \notin H \\ \lambda(g_\ell h_{\ell j} g (g_{\ell'} h_{\ell',j'})^{-1}) & \text{, if } g_\ell h_{\ell j} g (g_{\ell'} h_{\ell',j'})^{-1} \in H \end{cases}.$$

The representation λ restricts in two obvious ways to a representation of H_ℓ:

$$\lambda_\ell : H_\ell \to K^*, h \mapsto \lambda(h) \text{ and } \lambda_\ell^{g_\ell} : H_\ell \to K^*, h \mapsto \lambda(g_\ell h g_\ell^{-1}).$$

Let $\mathcal{I} := \{\ell \in \{1, \ldots, m\} \mid \lambda_\ell = \lambda_\ell^{g_\ell}\}$ and reorder the double coset representatives so that $\mathcal{I} = \{1, \ldots, d\}$.

Remark 2. *([4, Section I (1)]) In the notation above the* **endomorphism ring**

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

has dimension d and the **Schur basis** *of* $\mathrm{End}(\Delta)$ *is* $(B_1 = I_n, B_2, \ldots, B_d)$ *where* $(B_\ell)_{1,g_\ell} = 1$ *and* $(B_\ell)_{1,g_k h_{k,i}} \neq 0$ *if and only if* $\ell = k$. *More generally we get* $(B_\ell)_{g_k h_{k,i}, g_{k'} h_{k',i'}} = 0$ *if* $g_{k'} h_{k',i'} h_{k,i}^{-1} g_k^{-1} \notin H g_\ell H$. *Otherwise write* $g_{k'} h_{k',i'} h_{k,i}^{-1} g_k^{-1} = h g_\ell h_{\ell,j}$ *for some* $h \in H$. *Then* $(B_\ell)_{g_k h_{k,i}, g_{k'} h_{k',i'}} = \lambda(h)^{-1}\lambda(h_{\ell,j}^{-1})$.

3 Generalized Pless codes.

In this section we reinterpret the construction of the famous Pless symmetry codes $\mathcal{P}(p)$ discovered by Vera Pless [6], [5]. Let p be an odd prime and

$$\mathrm{SL}_2(p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_p^{2\times 2} \mid ad - bc = 1 \right\}$$

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

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

Then B is a subgroup of $\mathrm{SL}_2(p)$ or index $p+1$. Let

$$\lambda : B \to K^*, \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mapsto \left(\frac{a}{p}\right) = \begin{cases} 1 & , a \in (\mathbb{F}_p^*)^2 \\ -1 & , a \notin (\mathbb{F}_p^*)^2 \end{cases}$$

and $\Delta := \lambda_B^{\mathrm{SL}_2(p)} : \mathrm{SL}_2(p) \to \mathrm{Mon}_{p+1}(K^*)$ be the monomial representation induced by λ. The following facts about this representation are well known, and easily computed from the general description in the previous section.

Remark 3. *(1)* $\mathrm{SL}_2(p) = B \mathbin{\dot\cup} BwB$ *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 $\mathrm{SL}_2(p)$ *is* $[1, wh_x : x \in \mathbb{F}_p]$ *where* $h_x := h_1^x$.

(4) The Schur basis of $\mathrm{End}(\Delta)$ *is* (I_{p+1}, P), *where* $P_{1,1} = 0$, $P_{1,wh_x} = 1$ *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* $PP^{tr} = p$.

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

$$\mathcal{G}(p) := \left\langle \begin{pmatrix} \Delta(g) & 0 \\ 0 & \Delta(g) \end{pmatrix}, Z := \begin{pmatrix} 0 & I_{p+1} \\ jI_{p+1} & 0 \end{pmatrix} \middle| g \in \mathrm{SL}_2(p) \right\rangle \leq \mathrm{Mon}_{2(p+1)}(K^*)$$

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

(2) $\mathrm{End}(\mathcal{G}(p)) = \left\{ \begin{pmatrix} A & B \\ jB & A \end{pmatrix} \middle| A, B \in \mathrm{End}(\Delta) \right\}$ *is generated by*

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

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* $P_q(p) := aI_{2(p+1)} + XY \in \mathrm{End}(\mathcal{G}(p))$ *and define the* **generalized Pless code** $\mathcal{P}_q(p) \leq K^{2(p+1)}$ *to be the code spanned by the rows of* $P_q(p)$.

As $PP^{tr} = pI_{p+1} = -a^2 I_{p+1}$ the code $\mathcal{P}_q(p)$ is self-dual with respect to the standard inner product. So we have the following theorem.

Theorem 6. *Let* $a \in \mathbb{F}_q^*$ *such that* $a^2 = -p$. *The code* $\mathcal{P}_q(p)$ *has generator matrix* $(aI_{p+1}|P)$ *and is a self-dual code in* $\mathbb{F}_q^{2(p+1)}$. *The sum of the first two rows of this matrix has weight* $(p+7)/2$ *if* q *is odd and* 4 *if* q *is even. The group* $\mathcal{G}(p)$ *is a subgroup of* $\mathrm{Aut}(\mathcal{P}_q(p))$. $\mathcal{P}_3(p)$ *is the Pless symmetry code* $\mathcal{P}(p)$ *as given in [6].*

Minimum distance of the Pless codes computed with Magma [1].

p	5	11	17	23	29	41	47
$2(p+1)$	12	24	36	48	60	84	96
$d(\mathcal{P}_3(p))$	6	9	12	15	18	21	24
$\mathrm{Aut}(\mathcal{P}_3(p))$	$2.M_{12}$	$\mathcal{G}(11).2$	$\mathcal{G}(17).2$	$\mathcal{G}(23).2$	$\mathcal{G}(29).2$	$\geq \mathcal{G}(41)$	$\geq \mathcal{G}(47)$

4 A new series of self-dual codes invariant under $\mathrm{SL}_2(p)$.

Applying the same strategy as in the previous section we now construct a monomial representation of $\mathrm{SL}_2(p)$ of degree $2(p+1)$ where p is a prime so that $p-1 \equiv 4 \pmod 8$. We assume that $\mathrm{char}(K) \neq 2$. Then the subgroup $B^{(2)} := \left\{ \left(\begin{array}{cc} a^2 & 0 \\ b & a^{-2} \end{array} \right) \middle| a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\} \leq \mathrm{SL}_2(p)$ of index $2(p+1)$ in $\mathrm{SL}_2(p)$ has a unique linear representation $\gamma : B^{(2)} \to K^*$ with $\gamma(B^{(2)}) = \{\pm 1\}$, so $\gamma\left(\left(\begin{array}{cc} a^2 & 0 \\ b & a^{-2} \end{array} \right)\right) = \left(\frac{a}{p}\right)$. Then $\Delta' := \gamma_{B^{(2)}}^{\mathrm{SL}_2(p)}$ is a faithful monomial representation of degree $2(p+1)$. To obtain explicit matrices we choose $w := \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right)$ as above. By assumption $2 \in \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$. Put $\epsilon := \mathrm{diag}(2, 2^{-1})$. Then $B = B^{(2)} \dot\cup B^{(2)}\epsilon$ and

$$\mathrm{SL}_2(p) = B \dot\cup BwB = B^{(2)} \dot\cup B^{(2)}wB^{(2)} \dot\cup B^{(2)}\epsilon \dot\cup B^{(2)}\epsilon w B^{(2)}$$

and a right transversal is given by $[1, wh_x, \epsilon, \epsilon w h_x : x \in \mathbb{F}_p]$. From Remark 2 we find.

Lemma 7. *$\mathrm{End}(\Delta')$ has a Schur basis $(B_1, B_w, B_\epsilon, B_{\epsilon w} = B_\epsilon B_w)$ where $B_\epsilon = \left(\begin{array}{cc} 0 & I \\ -I & 0 \end{array} \right)$ and $B_w = \left(\begin{array}{cc} X & Y \\ -Y^{tr} & X^{tr} \end{array} \right)$ with*

$$X = \left(\begin{array}{cccc} 0 & 1 & \dots & 1 \\ -1 & & & \\ \vdots & & R_X & \\ -1 & & & \end{array} \right), Y = \left(\begin{array}{cccc} 0 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & R_Y & \\ 0 & & & \end{array} \right)$$

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

$$(R_X)_{a,b} = \begin{cases} 0 & , b-a \notin (\mathbb{F}_p^*)^2 \\ \left(\frac{c}{p}\right) & , b-a = c^2 \in (\mathbb{F}_p^*)^2 \end{cases}, (R_Y)_{a,b} = \begin{cases} 0 & , 2(b-a) \notin (\mathbb{F}_p^*)^2 \\ \left(\frac{c}{p}\right) & , 2(b-a) = c^2 \in (\mathbb{F}_p^*)^2 \end{cases}$$

Remark 8. *Note that $(-1) = c^2$ is a square but not a 4th power, so $\left(\frac{c}{p}\right) = -1$ and hence X is skew symmetric and $B_w^{tr} = -B_w$, $B_{\epsilon w}^{tr} = -B_{\epsilon w}$. We compute that $B_w^2 = B_{\epsilon w}^2 = -p$ and $B_\epsilon^2 = -1$ so $\mathrm{End}(\Delta') \cong \left(\frac{-p,-1}{K}\right)$ is isomorphic to a quaternion algebra over K. We also compute that $(B_w + B_{\epsilon w})^2 = -2p$.*

Definition 9. *Let p be a prime $p \equiv_8 4$, $K = \mathbb{F}_q$ so that there is some $a \in K^*$ such that $a^2 = -tp$ for $t = 1$ or $t = 2$. We then put*

$$V_t(p) := \begin{cases} aI_{2(p+1)} + B_w & , t = 1 \\ aI_{2(p+1)} + B_w + B_{\epsilon w} & , t = 2 \end{cases}$$

and let $\mathcal{V}_q(p)$ be the linear code spanned by the rows of $V_t(p)$.

We compute $V_1(p)V_1(p)^{tr} = V_2(p)V_2(p)^{tr} = 0$ and get the following theorem.

Theorem 10. *$\mathcal{V}_q(p)$ is a self-dual code in $\mathbb{F}_q^{2(p+1)}$. Its monomial automorphism group contains the group $\mathrm{SL}_2(p)$.*

Remark 11. *The matrices of rank $p+1$ in $\mathrm{End}(\Delta')$ yield $q+1$ different self-dual codes invariant under $\Delta'(\mathrm{SL}_2(p))$. 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.*

Minimum distance of $\mathcal{V}_3(p)$ computed with MAGMA [1]:

p	5	13	29	37	53
$2(p+1)$	12	28	60	76	108
$d(\mathcal{V}_3(p))$	6	9	18	18	24
$\mathrm{Aut}(\mathcal{V}_3(p))$	$2.M_{12}$	$\mathrm{SL}_2(13)$	$\mathrm{SL}_2(29)$	$\geq \mathrm{SL}_2(37)$	$\geq \mathrm{SL}_2(53)$

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* 24, 1997, 235-265.

[2] Andrew M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, *Actes du Congrès International des Mathématiciens* (Nice, 1970), Tome 3, Gauthier-Villars, Paris, 1971, 211-215.

[3] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[4] Jürgen Müller, On endomorphism rings and character tables, Habilitationsschrift, RWTH Aachen, 2003.

[5] V. Pless, Symmetry codes over GF(3) and new five-designs, *J. Combinatorial Theory* Ser. A 12, 1972, 119-142.

[6] V. Pless, On a new family of symmetry codes and related new five-designs, *Bull. Amer. Math. Soc.* 75, 1969, 1339-1342.