ELSEVIER
Discrete Mathematics 241 (2001) 129–138
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Tricolore 3-designs in Type III codes

A. Bonnecaze[a,*,1], P. Solé[b], P. Udaya[c]

[a] *SIS, Université de Toulon et du Var, 83 957 La Garde, France*
[b] *CNRS, I3S ESSI, BP 145 Route des Colles 06 903 Sophia Antipolis, France*
[c] *Department of Computer Science and Software Engineering, University of Melbourne Parkville, Vic., 3052 221 Bouverie Street, Australia*

Abstract

A split complete weight enumerator in six variables is used to study the 3-colored designs held by codewords of fixed composition in Type III codes containing the all-one codeword. In particular, the ternary Golay code contains 3-colored 3-designs. We conjecture that every weight class in a Type III code with the all-one codeword holds 3-colored 3-designs. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Self-dual codes; Colored designs; Invariant theory

1. Introduction

Colored designs were introduced in [1] to study the Harada designs [6] held by the lifted Golay over $\mathbf{Z}_4$. They produce ordinary designs by bleaching and are easily understood in terms of split (complete) weight enumerators. Colored t-designs are known to exist when the permutation part of the automorphism group is t-transitive [1]. This is the case, for instance, of the doubled Golay code in [2], which is invariant under the action of M_{24}.

In the present work, we investigate the tricolore 3-designs held by codewords of extremal Type III codes. It is well known that the ternary Golay is invariant under the monomial action of the 5-transitive group M_{12}. The permutation part of that group, however, is not even 1-transitive [8, Section 5.1]. We show that the codewords of given composition in the ternary Golay, the symmetry code of length 24, the extended quadratic residue code of length 24, hold tricolore 3-designs. Similarly, as observed

* Corresponding author.
E-mail addresses: alexis.bonnecaze@sophia.inria.fr (A. Bonnecaze), ps@essi.fr (P. Solé), udaya@cs.mu.oz.au (P. Udaya).
1 Visiting INRIA, projet SAGA, Sophia-Antipolis, France.

PII: S0012-365X(01)00114-5

in [8, Section 5.2], the permutation part of the automorphism group of the symmetry code is not transitive.

We conjecture, based on these results and computations in lengths $36, 48, 60$, that the codewords of given composition in an extremal Type III code containing the all-one codeword hold tricolore 3-designs.

2. Definitions and notations

The composition of a vector $c \in \mathbf{F}_3^n$ is the triple $(n_0(c), n_1(c), n_2(c))$ where $n_i(c)$ counts the number of $j \in [n]$ with $c_j = i$. A ternary linear code C is a $\mathbf{F}_3$-subspace of $\mathbf{F}_3^n$. A Type III code is a ternary linear code self-dual w.r.t. the usual inner product. It is said to be *extremal* if its minimum distance $d = 3(\lfloor n/12 \rfloor + 1)$. The complete weight enumerator of C denoted by cwe_C is then

$$\mathrm{cwe}_C(x, y, z) := \sum_{c \in C} x^{n_0(c)} y^{n_1(c)} z^{n_2(c)}.$$

The weight enumerator (W_C) is obtained by specialization:

$$W_C(x, y) := \mathrm{cwe}(x, y, y).$$

The split cwe ($\mathrm{scwe}_{C,T}$) in six variables a, b, c, x, y, z is defined for any set of coordinate places $T \subseteq [n]$ as

$$\mathrm{scwe}_{C,T} := \sum_{c \in C} a^{r_0(c)} x^{s_0(c)} b^{r_1(c)} y^{s_1(c)} c^{r_2(c)} z^{s_2(c)},$$

where r_i (resp. s_i) is the composition on T (resp. $[n] \backslash T$). Observe that $J_{C,T}$ is an homogeneous polynomial of degree $n \backslash |T|$ in x, y, z and degree $|T|$ in a, b, c. Specialization gives the 4-variables Jacobi polynomial introduced in Ozeki [9].

$$\mathrm{scwe}_{C,T}(a, b, b, x, y, y) =: J_{C,T}(a, b, x, y).$$

3. Colored designs

A *colored incidence structure* Σ is a set P of “points”, a set B of “blocks”, a set $\mathscr{C}$ of “colors”, together with a function

$$\rho : P \times B \to \mathscr{C};$$

we will say that B has color $\rho(P, B)$ at P.

The application we have in mind is the situation where the characteristic vectors of B are supports of words x say of some code over a not q-ary alphabet with coordinate places P and $\rho(P, B)$ is a function of x_P.

An incidence structure is clearly just a colored incidence structure with two colors, “incident”, and “not incident”. We will say that a colored incidence structure is *uniform* if there is a function $n : \mathscr{C} \to Z$, the *palette*, such that for each color c, every block uses color c $n(c)$ times. For instance, when the alphabet is $\mathbf{Z}_4$ then we can take [1] $\mathscr{C}=0,1,2$ and $n(i)=n_i$ for $i=0,1,2$. See [11] for the case $\mathscr{C}=0,1,2,3$.

A colored incidence structure is *simple* if no two blocks assign the same coloring to Σ.

There are two natural ways to colorize the notion of a t-design. A simple, uniform colored incidence structure Σ is a *colored t-design* if for each t-multiset of colors (repeated choices allowed), there is a number λ such that for any choice of t points, exactly λ blocks use that set of colors for those points. A *strong* colored t-design is one in which the colors and points are ordered. It is easy to see that a t-design is a strong colored t-design with two colors. In general, however, a colored t-design is not strong.

Lemma 1. *A (strong) colored t-design $\mathscr{D}$ is also a (strong) colored t'-design for all $t' \leqslant t$.*

Clearly, the parameters of a (strong) colored t-design depend only on the number of blocks and the palette. For this reason, we will often refer to a t-design as a t-$(|P|,(n(1),n(2),\ldots),|B|)$ design. Thus, for example, the 5-$(24,8,1)$ design would be a 5-$(24,(8,16),759)$. The following is trivial:

Lemma 2. *If $\mathscr{D}$ is a t-$(v,(n_1,n_2,n_3,\ldots n_k),b)$, then*

$$\lambda_{j_1 j_2 j_3 \ldots j_k} = \frac{\prod_i \binom{n_i}{j_i} |B|}{\binom{n}{t}}.$$

It is left to the reader to determine which standard transformations of uncolored designs can be extended to (strong) colored designs. One new transformation is to identify colors (we will call this operation “bleaching”) to obtain a structure with fewer colors. It is easy to see that this preserves the t-design property (except for possibly introducing repeated blocks).

The relation with split weight enumerators goes as follows. The codewords of given composition in a ternary code C hold 3-colored t-designs iff $\mathrm{scwe}_{C,T}$ does not depend on T for $|T|=t$. The structure constants $\lambda_{j_1 j_2 j_3 \ldots j_k}$ can then be easily computed from the datum of $\mathrm{scwe}_{C,T}$.

4. Invariant theory

It should be noted that when T is void the Jacobi polynomial coincide with the cwe of C. In the case of C a type III code containing the all-one vector it was shown in [7, Chapter 19] that the cwe was left invariant by a group G_3 of order 2592 generated by four matrices M_1,M_2,M_3,M_4 corresponding respectively to MacWilliams transform, and some congruence conditions:

$$M_1 := \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & j & j^2 \\ 1 & j^2 & j \end{pmatrix}$$

with $j := \exp(2\pi\sqrt{-1}/3)$, and $M_2 = \zeta I_3$ with $\zeta := \exp(\pi\sqrt{-1}/6)$, and $M_3 = \mathrm{diag}(1, j, 1)$ and $M_4 := \mathrm{diag}(1, 1, j)$. It is a simple exercise to show that, for any T, the split cwe is invariant under the same group acting in the same way on each set of three variables. This a *simultaneous invariant* in the sense of Issai Schur [10] for the diagonal action of G_3. In other words, it is an invariant for the direct sum $G_3 \oplus G_3$ obtained by replacing each element $g \in G_3$ by the 6×6 matrix

$$\begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix}.$$

Let $M_{l,k}$ denote the dimension of the space $\mathscr{M}_{l,k}$ of invariant polynomials in a, b, c, x, y, z of degree k in a, b, c and l in x, y, z. Consider the bivariate Molien series

$$f(u, v) := \sum_{k,l} M_{l,k} u^k v^l.$$

Formula (13) in [11] specializes into the following bivariate analogue of Molien's theorem:

$$f(u, v) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(1 - ug)\det(1 - vg)}.$$

In the case of G_3 a Magma computation gives an explicit if unwieldy rational function. A Taylor expansion yields

$$f(u, v) := 1 + 2a^{12} + 2ba^{11} + 3b^2a^{10} + 4b^3a^9 + \cdots .$$

An important practical tool to compute bases of the spaces $\mathscr{M}_{l,k}$ is the Reynolds operator, which we now define. The Reynolds operator attached to a matrix group G acting on polynomials f by linear substitutions is

$$R(f, G) := \sum_{g\in G} g.f,$$

where the image of f by action of $g \in G$ is denoted by $g.f$. It is well known that $R(f, G)$ is an invariant of G. It is an easy observation that Reynolds operators respect the bigrading. If f has bidegree l, k then $R(f, G_3 \oplus G_3) \in \mathscr{M}_{l,k}$.

5. Polarizations

5.1. Two variables

If P is a polynomial in 4 variables a, b, x, y of total degree n define a differential operator called the normalized polarization operator A_4 by the formula

$$A_4(P) := (aP'_x + bP'_y)/n.$$

We shall require the following lemma. Define a ternary code to be t-homogeneous if the codewords of given Hamming weight hold a t-design.

Lemma 3. *If C is t-homogeneous and of minimum Hamming distance $> t$ then for all T of size t we get*

$$J_{C,T} = A_4^t W_C.$$

5.2. Three variables

If P is a polynomial in 6 variables a, b, c, x, y, z of total degree n define a differential operator called the normalized polarization operator A_6 by the formula

$$A_6(P) := (aP'_x + bP'_y + cP'_z)/n.$$

Define the specialization operator S by

$$S(P)(a, b, c, x, y, z) := P(a, b, b, x, y, y).$$

Define a ternary code to be colorwise t-homogeneous if the codewords of given composition hold a tricolore t-design. The analogue of Lemma 3 is then

Lemma 4. *If the ternary code C is colorwise t-homogeneous and if C has minimum Hamming distance $> t$ then for all T of size t we get*

$$\mathrm{scwe}_{C,T} = A_6^t \mathrm{cwe}_{C,T}.$$

6. Length 12

We now give a basis of the space of interest.

Lemma 5. *A basis of $\mathscr{M}_{3,9}$ is obtained by applying $R(f, G_3 \oplus G_3)$ with f running over the monomials*

$$a^3x^9,\ a^3x^3y^6,\ a^3x^3y^3z^3,\ a^2bx^4y^5.$$

It is important to observe that specialization is one-to-one on those spaces.

Lemma 6. *For $l = 1, 2, 3$ we have*

$$\dim S(\mathscr{M}_{l,12-l}) = \dim(\mathscr{M}_{l,12-l}).$$

Proof. This is checked by taking the image by S of the preceding bases. □

Such good fortune cannot happen in length 24, since the bimolien series for the group G_3'' of order 144 generated by M_1, M_2, M_3 corresponding, respectively, to MacWilliams transform, and some congruence conditions.

$$M_1 := \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$$

and $M_2 = \zeta I_2$ with $\zeta := \exp(\pi\sqrt{-1}/6)$, and $M_3 = \mathrm{diag}(1, j)$ with $j := \exp(2\pi\sqrt{-1}/3)$, is

$$1 + \cdots + 3u^{24} + 4vu^{23} + 6v^2u^{21} + 8v^3u^{21} + \cdots$$

while the bimolien series for G_3 reads

$$1 + \cdots + 4u^{24} + 6vu^{23} + 10v^2u^{21} + 15v^3u^{21} + \cdots.$$

Note that the homogeneous part of degree 12 of both series begins with

$$1 + \cdots + 2u^{12} + 2vu^{11} + 3v^2u^{10} + 4v^3u^9 + \cdots.$$

Observe that the preceding lemma together with the bivariate Molien series entails Lemma 5.

We are now in a position to prove the main result of this section.

Theorem 7. *The codewords of fixed composition in the ternary Golay hold tricolore 3-designs.*

Proof. We need to show that $\mathrm{scwe}_{C,T}$ does not depend on T for $|T| = 3$. Since it lives in $\mathscr{M}_{3,9}$ we can expand it with indeterminate coefficients on the basis given in Lemma 5. Recall that the ternary Golay is 5-homogeneous [7], hence 3-homogeneous. By specialization and Lemmas 3 and 6 we determine these completely by solving a 4×4 linear system. □

Note that this result is best possible since the ternary Golay cannot be colorwise 4-homogeneous as applying 4 times the operator A_6 to its cwe results in fractionnary coefficients, thus contradicting Lemma 4.

Corollary 8. *The cwe of the* (*i times shortened*) *Golay code G is the coefficient of* $a^ib^0c^0$ *in* $A_6^i \mathrm{cwe}_G$ *for* $i = 1, 2, 3$.

When $i = 1$ this is $\mathscr{W}_{\mathscr{G}_{11}}$ in [8, p. 661].

7. Length 24

The approach is the same as in the preceding section. The matter is complicated, however, by the larger size of the coefficients of the bimolien series as previously mentioned.

Lemma 9. *A basis of $\mathscr{M}_{3,21}$ is obtained by taking $R(f, G_3 \oplus G_3)$ with f running over the monomials*:

$$a^3x^9y^3z^9,\ a^3x^{21},\ a^3x^{12}y^6z^3,\ a^3x^9y^{12},$$

$$a^3x^9y^6z^6,\ a^3x^6y^{12}z^3,\ a^3x^3y^{15}z^3,\ a^3y^{15}z^6,$$

$$a^2bx^{13}y^5z^3,\ a^2bx^{13}y^2z^6,\ a^2bx^{10}y^{11},$$

$$a^2bx^{10}y^2z^9,\ a^2bx^7y^{11}z^3,\ a^2bx^7y^8z^6,\ a^2cxy^{15}z^5.$$

We now consider an extremal code of length 24 containing the all-one codeword. Let J_6 denote an arbitrary Jacobi polynomial attached to that code and to some set of coordinate places T of size 3. We expand it on a basis say e_i of $\mathscr{M}_{3,21}$.

$$J_6 := \sum_{i=1}^{15} m_i e_i.$$

Define the *restitution* operator R_6 as the operator acting on $\mathbf{C}[a,b,c,x,y,z]$ by the substitution $a=x, b=y, c=z$. We know that A_6 and R_6 are inverse of each other.

Since $\dim(\mathscr{M}_{0,12})=4$, restitution gives us four independent relations between the m_i's.

Let $J_4 := A_4^2 W_C$. We know that such a code is 3-homogeneous. Therefore by specialization

$$SJ_6 = J_4.$$

This gives 5 relations amongst the m_i's. We obtain 4 further relations by writing that the sum of the exponents of b,c,x,y is at least 9, and one more relation by writing that, as inspection of the cwe shows, there is no codeword of shape $0^{15}1^9$. We are now in a position to prove the main result of this section.

Theorem 10. *The codewords of fixed composition in an extremal ternary self-dual code of length* 24 *containing the all-one vector hold tricolore* 3-*designs.*

Proof. We solve for the m_i, $i=1,\dots,15$, a linear system in $4+5+5+1=15$ equations. □

Again, this is the best possible result, as applying A_6 four times yields non-integral coefficients.

Corollary 11. *The* cwe *of the* (*i times shortened*) *symmetry code S of length* 24 *is the coefficient of $a^ib^0c^0$ in A_6^i*cwe$_S$ *for* $i=1,2,3$.

Case $i=1$ of that corollary appears in [8, p. 662].

8. Conjecture

Conjecture 12. The codewords of given composition in an extremal Type III code containing the all-one codeword hold tricolore 3-designs.

9. Design parameters

9.1. Length 12

Corollary 13. *There exist simple* 3*-colored* 3*-designs with the following parameters*:

Three designs with parameters $3\text{-}(12,(n_0,n_1,n_2),220)$ *where* (n_0,n_1,n_2) *is equal to* $(6,3,3)$ *or any one of its three permutations.*

Three designs with parameters $3\text{-}(12,(n_0,n_1,n_2),22)$ *where* (n_0,n_1,n_2) *is equal to* $(6,6,0)$ *or any one of its three permutations.*

By bleaching colors in various ways we obtain the designs (in the ordinary sense) with the following parameters $3\text{-}(12,6,20)$, $3\text{-}(12,6,2)$, $3\text{-}(12,9,84)$.

9.2. Length 24

Corollary 14. *There exist simple* 3*-colored* 3*-designs with the following parameters*:

Six designs with parameters $3\text{-}(24,(n_0,n_1,n_2),2024)$ *where* (n_0,n_1,n_2) *is equal to* $(15,6,3)$ *or any one of its six permutations.*

Three designs with parameters $3\text{-}(24,(n_0,n_1,n_2),46)$ *where* (n_0,n_1,n_2) *is equal to* $(12,12,0)$ *or any one of its three permutations.*

Six designs with parameters $3\text{-}(24,(n_0,n_1,n_2),10120)$ *where* (n_0,n_1,n_2) *is equal to* $(12,9,3)$ *or any one of its six permutations.*

Three designs with parameters $3\text{-}(24,(n_0,n_1,n_2),41492)$ *where* (n_0,n_1,n_2) *is equal to* $(12,6,6)$ *or any one of its three permutations.*

Three designs with parameters $3\text{-}(24,(n_0,n_1,n_2),111320)$ *where* (n_0,n_1,n_2) *is equal to* $(9,9,6)$ *or any one of its three permutations.*

Proof. The block sizes are computed from the cwe. □

Here again by bleaching colors in various ways, we obtain the following designs in the ordinary sense.

Corollary 15. *There exist* 3*-designs with possibly repeated blocks and the parameters which are given in Table 1.*

Table 1

Blocks in the cwe (n_0, n_1, n_2) up to permutation	Number of blocks	Size of blocks after Bleaching	λ
(15, 3, 6)	2024	3	1
		6	20
		15	455
		9	84
		18	816
		21	1330
(12,12,0)	46	12	5
(12,9,3)	10 120	9	420
		12	1100
		15	2275
		21	6650
(12,6,6)	41 492	6	410
		12	4510
		18	16 728
(9,9,6)	111 320	6	1100
		9	4620
		15	25 025
		18	44 880

Appendix Weight enumerators

The cwe of the ternary Golay is given in [8] by

$$\begin{aligned}\mathrm{cwe}_G := {}& x^{12} + y^{12} + z^{12} + 220x^3y^3z^3(x^3 + y^3 + z^3) \\ & + 22x^6y^6 + 22\,x^6z^6 + 22\,y^6z^6.\end{aligned}$$

The cwe of the symmetry code of length 24 is computed in Magma [8,9] to be:

$$\begin{aligned}\mathrm{cwe}_S := {}& x^{24} + 2024x^{15}y^6z^3 + 2024x^{15}y^3z^6 + 46x^{12}y^{12} \\ & + 10120x^{12}y^9z^3 + 41492x^{12}y^6z^6 + 10120x^{12}y^3z^9 \\ & + 46x^{12}z^{12} + 10120x^9y^{12}z^3 + 111320x^9y^9z^6 \\ & + 111320x^9y^6z^9 + 10120x^9y^3z^{12} + 2024x^6y^{15}z^3 \\ & + 41492x^6y^{12}z^6 + 111320x^6y^9z^9 + 41492x^6y^6z^{12} \\ & + 2024x^6y^3z^{15} + 2024x^3y^{15}z^6 + 10120x^3y^{12}z^9 \\ & + 10120x^3y^9z^{12} + 2024x^3y^6z^{15} + y^{24} + 46y^{12}z^{12} \\ & + z^{24}.\end{aligned}$$

References

[1] A. Bonnecaze, E. Rains, P. Solé, 3-colored 5-designs and $\mathbf{Z}_4$-codes, J. Statist. Plann. Inference 86 (2000) 349–368.

[2] A. Bonnecaze, P.Solé, P. Udaya, Strong 4-colored 5-designs, preprint.

[3] W. Bosma, J. Cannon, C. Playoust, The magma algebra system I: the user language, J. Symbolic Comput. 1997, submitted for publication.

[4] J. Cannon, C. Playoust, Magma: a new computer algebra system, Euromath Bull. 2(1) 113–144.

[5] I. Duursma, et al., 3-Designs from Preparata and Kerdock codes, preprint.

[6] M. Harada, New 5-designs constructed from the lifted Golay code over $\mathbf{Z}_4$, J. Combin. Des. (1998) 225–229.

[7] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[8] C. Mallows, V. Pless, N.J.A. Sloane, Self-dual codes over GF(3), SIAM J. Appl. Math. 31 (4) (1976) 649–666.

[9] M. Ozeki, On the notion of Jacobi polynomials for codes, Math. Proc. Cambridge Philos. Soc. (1997) 15–30.

[10] I. Schur, Vorlesungen Ueber Invariantheorie, Springer, Berlin, 1968.

[11] R. Stanley, Invariants of finite groups and their applications to combinatorics, Bull. AMS (New Series) 1 (1979) 457–511.