Ternary trades and their codes[1]

G.B. Khosrovshahi*
Department of Mathematics, University of Tehran, and
Institutes for Studies in Theoretical Physics and Mathematics (IPM),
Tehran, Iran

Reza Naserasr
Institutes for Studies in Theoretical Physics and Mathematics (IPM),
Tehran, Iran

B. Tayfeh-Rezaie
Department of Mathematics, University of Tehran, and
Institutes for Studies in Theoretical Physics and Mathematics (IPM),
Tehran, Iran

Dedicated to Professor S. S. Shrikhande
for his profound contributions to combinatorics

Abstract. In this paper, the notion of trades over finite fields is introduced. In particular, trades over $GF(3)$ (ternary trades) are studied. By considering the incidence matrix of t-subsets vs. k-subsets of a v-set as a parity check matrix of a ternary code, we obtain a new family of codes in which every codeword is a ternary trade. The spectrum of weights of these codes is discussed; a simple and fast algorithm for decoding is given; and the automorphism group of the codes is determined. We also provide a table of all non-isomorphic ternary trades of weight at most 12.

AMS classification: 05B05; 94B05; 94B35

Keywords: Trade; Ternary trade; Ternary code; Automorphism group; Decoding

1. Introduction

For given integers v, k and t such that $v > k > t > 0$, let S be a v-set and let $P_k(S)$ denote the set of all k-subsets (called blocks) of S. Let $P^v_{t,k}$ be the $\binom{v}{t}$ by $\binom{v}{k}$ *incidence*

[1]This research was supported in part by IPM.

*Corresponding author; Mailing address: IPM, P.O.Box 19395-5746, Tehran, Iran; Email: reza-gbk@karun.ipm.ac.ir

matrix whose rows are indexed by the t-subsets of S, whose columns are indexed by the blocks of S (in some fixed ordering for t-subsets and some fixed ordering for blocks), and the entry $P^v_{t,k}(A,B)$ of row A and column B is 1 if $A \subset B$ and 0 otherwise.

The integral solutions T of the equation

$$P^v_{t,k}T = 0 \tag{1}$$

which form a $\mathbb{Z}$-module, are well known combinatorial objects called *(v,k,t) trades*. The entries of a trade T are indexed by the blocks with the same ordering as the columns of $P^v_{t,k}$. By considering the vector space formed by the solutions of (1) over a finite field $GF(p)$, p being prime, we will introduce a new notion of trades.

Considering $P^v_{t,k}$ as a parity check matrix of a p-ray code, we obtain a new family of codes (denoted by $C^v_{t,k}(p)$) in which every codeword is a trade over $GF(p)$. The length of the code is $\binom{v}{k}$ and its dimension is $\binom{v}{k} - \mathrm{rank}_p(P^v_{t,k})$ ($\mathrm{rank}_p(P^v_{t,k})$ is obtained from a theorem of R. M. Wilson). The codes $C^v_{1,k}(2)$, namely the binary codes arising from $(v,k,1)$ trades over $GF(2)$, were studied in [5]. In this paper, we study the case $C^v_{2,3}(3)$. For $C^v_{2,3}(3)$, the spectrum of weights is discussed; a simple and fast algorithm for decoding is given; and the automorphism group of the codes is determined. We also provide a table of all non-isomorphism codewords (trades) of weight at most 12.

Finally we note that the graphical codes were recently studied extensively by D. Jungnickel and S. A. Vanstone [2] and by some some other authors and our work in this paper and [5] in some sense is an extention of graphical codes on complete graphs.

2. Preliminaries

Let v, k and t be positive integers satisfying $v - t > k > t \geq 0$ and S be a v-set. A (v,k,t) *trade* $T = \{T^+, T^-\}$ over $\mathbb{Z}$ consists of two disjoint collections T^+ and $T^-$of blocks of S not necessarily distinct, such that for every t-subset A of S, the number of blocks containing A is the same in both T^+ and T^-. The *foundation* of T is the set of all elements covered by T^+ and T^- and is denoted by $found(T)$. The number of blocks is the same in T^+ and T^- and is called the *volume* of T (denoted by $vol(T)$).

We now introduce the notion of trades over $GF(p)$.

Definition. A (v,k,t) *trade* T over $GF(p)$ is a collection of blocks of S such that each block is repeated at most $(p-1)$ times and that for every t-subset A of S, the number of blocks containing A is equal to $0 \pmod{p}$.

For a given trade T over $\mathbb{Z}$, one can naturally associate a $\binom{v}{k}$-integral column vector which is a solution T of (1), and conversely every integral solution of (1) corresponds to a trade over $\mathbb{Z}$. The set of all (v,k,t) trades over $\mathbb{Z}$ forms a $\mathbb{Z}$-module. Similarly, every trade over $GF(p)$ corresponds to a $\binom{v}{k}$-dimnesional column vector which is a solution of (1) over $GF(p)$ and vice versa. In the sequel, by abuse of notations we will denote both the vector and combinatorial representations of a trade by T. Let $C^v_{t,k}(p)$ be a p-ray code with parity check matrix $P^v_{t,k}$. So there is a correspondence between codewords of $C^v_{t,k}(p)$ and (v,k,t) trades over $GF(p)$ and we use the words "trade" and "codeword" interchangeably.

Hereafter, we only focus on $(v,3,2)$ trades over $GF(3)$ which we call them *ternary* trades. Also we write C^v instead of $C^v_{2,3}(3)$. For these trades, we can partition the blocks of a trade T (as in trades in the usual sense) into two disjoint collections T^+ and T^-. In this representation of T we denote the number of appearances of the pair ij $(i,j\in S)$ by λ^+_{ij} and λ^-_{ij} in the blocks of T^+ and T^-, respectively. Then for each pair ij, $\lambda^+_{ij}-\lambda^-_{ij}\equiv 0 \pmod 3$. Every simple trade over $\mathbb{Z}$ (a trade with no repeated blocks) is also a ternary trade but the converse is not true. As an important example, for any 5-subset L of S, we have the trade I_L, where $I^+_L = P_3(L)$ and $I^-_L=\varnothing$.

From hereafter, we use the standard notation of coding theory: by a (n,k,d) code C, we mean a linear code of length n, dimension k, and minimum distance d. The weight of a codeword $c\in C$ is denoted by $\mathrm{wt}(c)$ and the weight enumerator of C by $A_C(x)$.

Interested reader on codes can consult [6, 7], and interested reader on trades is referred to [1].

We close this section by stating the well known p-rank theorem of Wilson. The theorem shows that the dimension of $P^v_{2,3}$ is $\binom{v}{2}-1$.

Theorem A [8]. For $t\le \min\{k, v-k\}$,

$$\mathrm{rank}_p(P^v_{t,k}) = \sum \binom{v}{i} - \binom{v}{i-1}$$

where the sum is extended over those indices i such that p does not divide the binomial coefficient $\binom{k-i}{t-i}$.

3. Spectrum

In this section, we determine the spectrum of weights for $v = 0 \pmod 3$. It is shown that for $v\ge 9$, there exists a codeword of any weight at least 12. We would like to point out that the same result is valid for all sufficiently large v but the proofs for the cases $v\equiv 1,2 \pmod 3$ are more laborious and therefore are not given here. First we provide the characterization of all codewords of weight at most 12. There exist exactly 9 non-isomorphic ternary trades of weight at most 12 which are denoted by T_1 to T_9 and are shown in the Table 1 of the Appendix. The following facts about simple trades over $\mathbb{Z}$ have been known for sometimes. For these trades, the minimum volume is 4 and trades of this volume have a unique structure (see T_1) [1]. The next possible volume is 6 and there exist 4 non-isomorphic trades of this kind (see T_2 to T_5) [3,4]. T_6 to T_9 are ternary trades but not trades over $\mathbb{Z}$ and have been obtained by computer. Therefore, we have the following theorem.

Theorem 1. For every v, C^v is a $\left(\binom{v}{3}, \binom{v}{3} - \binom{v}{2} + 1, 8\right)$ ternary code.

In the proof of Theorem 2 below, we need a special family of trades which are introduced in the following example.

Example. For $\alpha, \beta \geq 1$, let $X = \{1, 2, \ldots, 3\alpha\}$ and $Y = \{3\alpha + 1, \ldots, 3\alpha + 3\beta\}$. Let $T_{\alpha,\beta} = \{T^+, T^-\}$ be defined as follows:

$$T^+ = \{x_1x_2y | x_1, x_2 \in X \text{ and } y \in Y\},$$
$$T^- = \{xy_1y_2 | x \in X \text{ and } y_1, y_2 \in Y\}.$$

It is easy to see that $T_{\alpha,\beta}$ is a ternary trade.

The weight enumerator polynomial of C^6 is given in the Appendix. As one can see, the spectrum of weights of C^6 is $8, 10, 12, 13, \ldots, 16, 18, 20$. For $v \geq 9$, we have the following theorem.

Theorem 2. Let $v \equiv 0 \pmod 3$ and $v \geq 9$. Then C^v has a codeword of weight d if and only if $d = 8, 10, 12, 13, \ldots, \binom{v}{3}$.

Proof. Let $d \leq 12$. By Table 1 of the Appendix there exist a codeword of weight d if and only if $d = 8, 10, 12$. Now let $d = \binom{v}{3}$. By induction we show that a trade T of weight d and foundation size v exists. For $v = 9$, let T^+ be the blocks of a 2-(9,3,2) design and T^- be all of the remaining blocks. To establish the main statement of the induction, let $v \geq 12$ and for every $w \equiv 0 \pmod 3$ and $w < v$, assume that a trade T_w with $|\text{found}(T_w)| = w$ and $\text{wt}(T_w) = \binom{w}{3}$ exists. Now for $v = 3(\alpha + \beta)$ $(\alpha, \beta \geq 2)$, we consider the trades $T_{3\alpha}$ with $\text{found}(T) = \{1, 2, \ldots, 3\alpha\}$ and $\text{wt}(T_{3\alpha}) = \binom{3\alpha}{3}$ and $T_{3\beta}$ with $\text{found}(T_{3\beta}) = \{3\alpha + 1, 3\alpha + 2, \ldots, 3\alpha + 3\beta\}$ and $\text{wt}(T_{3\beta}) = \binom{3\beta}{3}$. Now the trade $T = T_{\alpha,\beta} + T_{3\alpha} + T_{3\beta}$ is the desired trade.

To complete the proof we again use the inductive argument. For small v, namely $v = 9, 12$, and 15, we have constructed codewords of all weights greater than 12 via a computer program. For $v \geq 18$, we assume that a codeword of weight d for $12 \leq d \leq \binom{v-3}{3}$ based on the set $\{1, 2, 3, \ldots, v-3\}$ exists. Therefore it suffices to construct codewords of larger weights. By adding $T_{\frac{v-3}{3},1}$ to each of the trades of smaller weight, one can obtain a codeword of weight d for $\binom{v-3}{3} < d < \binom{v}{3}$.$\square$

4. Decoding

In this section, we present a simple and fast algorithm for decoding the ternary code C^v. C^v is a 3-error correcting code, so we assume that at most three errors are admissible during transmission. We call the indices of transformed entries *bad blocks*.

Consider a received word X. Let $[e_{xy}] = P^v_{23}X$ and define $e : P_2(S) \to \mathbb{Z}_3$ as $e(xy) = e_{xy}$. Let R= $\{xy | x, y \in S, e(xy) \neq 0\}$. R in fact is the set of unbalanced pairs of X. Assume that Q is the set of points covered by the elements of R. A point $x \in$ Q is called *special* if there are exactly two pairs in R containing x and e has the same value for these pairs. For a special point x, there are two possibilities for the bad blocks:

(i) There is a unique bad block containing x say xyz with error $e(xy)$.

(ii) There are three bad blocks of the unique form xyz, xyt, and xzr with errors $-1, 1$, and 1, respectively. In this situation, we have two other special points t and r.

We now consider the case in which Q contains no special point. Clearly, each point of Q appears in at least two bad blocks. Therefore, we have the unique form for the bad blocks: xyz, xyt, and xzt. It is not difficult to see that x is the unique point of Q such that e has the same value for all pairs in R containing x.

Based on the above observations, we state the following algorithm.

Algorithm. Let X be a received word with at most three errors.

(1) Compute $[e(xy)] = P^v_{tk}X$ and then let R= $\{xy | x, y \in S, e(xy) \neq 0\}$.

(2) If there is no special point in Q, then find the unique point x such that e has the same value for the pairs in R containing x. Then the bad blocks are xyz, xyt, and xzt (with errors $e(yz), e(yt)$, and $e(zt)$, respectively), where $y, z, t \in Q$.

(3) While R$\neq \varnothing$ do

(i) Find a special point x in Q with pairs say xy and xz. If not found, change the last bad block to its primary state and choose a special point different from the last one.

(ii) By putting $e(xy) = e(xz) = 0$, omit the pairs xy and xz from R and let $e(yz) := e(yz) - e(xy)$. If $e(yz) \neq 0$, add yz to R. Save xyz as the last bad block with error $e(xy)$ and x as the last point.

The decoding procedure is carried out within time $O(n^{\frac{5}{3}})$, where n is the length of the code.

5. Automorphism

In this section we characterize the full automorphism group of C^v denoted by $\mathrm{Aut}(C^v)$. Let S_v be the symmetric group on v points.

Theorem 3. For $v \geq 6$, $\mathrm{Aut}(C^v) \cong S_v \times \mathbb{Z}_2$.

Proof. Let $\sigma \in S_v$. The action of σ over S induces a permutation π on blocks of S (the coordinate positions). Clearly $\pi(C^v) = C^v$ and hence π is an element of $\mathrm{Aut}(C^v)$ which corresponds to $(\pi, 0)$. By multiplying every coordinate position of C^v by -1 together with the action of π we obtain another element of $\mathrm{Aut}(C^v)$ which corresponds to $(\pi, 1)$. This shows that $S_v \times \mathbb{Z}_2$ is isomorphic to a subgroup of $\mathrm{Aut}(C^v)$. To complete the proof, it is sufficient to prove that they are equal.

Because of the unique structure of the codewords of weight 10, it is clear that if the action of an automorphism of the code is multiplication of at least one column of C^v by -1, then it is necessary to multiply all the columns of C^v by -1. Therefore it is sufficient to show that very element of $\mathrm{Aut}(C^v)$ which only permutes the columns of the code is an induced permutation coming from S_v. To show this, let π be such an element. The completion of the proof again relies on the unique structure of codewords of weight 10. In fact the action of π over codewords of weight 10 induces an action of π over 5-subsets of S. So let $\pi(12345) = abcde$, then for every $x \in S \backslash \{1, 2, \ldots, 5\}$, π transfers $1234x$ to $abcdy$. By this we obtain a permutation σ on S for which $\sigma x = y$ and it is clear that π is the induced permutation of σ over 3-subsets of S. $\square$

Appendix

1. Table 1 contains the ternary trades of weight at most 12.

T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9
135	123	123	123	123	123	123	123	123
146	124	124	167	145	124	124	124	124
236	156	156	247	167	125	125	125	125
245	256	157	257	248	134	367	134	134
	345	267	346	368	135	467	136	135
	346	345	357	578	145	567	234	145
					234		246	
					235		345	
					245			
					345			
136	125	126	127	124		136	145	623
145	126	127	136	136		146	146	624
235	134	135	235	157		156	235	625
246	234	145	246	238		237	236	634
	356	237	347	458		247		635
	456	567	567	678		257		645

Table 1.

2. The weight enumerator polynomials of C^v for $v = 6$ and $v = 7$ are presented below.

$$A_{C^6}(x) = 1 + 30x^8 + 12x^{10} + 240x^{12} + 120x^{13} + 120x^{14} + 144x^{15} + 30x^{16} + 20x^{18} + 12x^{20}.$$

$$\begin{aligned} A_{C^7}(x) = 1 &+ 30x^8 + 42x^{10} + 2940x^{12} + 2100x^{13} + 9900x14 + 46368x^{15} + 52290x^{16} \\ &+ 95760x^{17} + 527460x^{18} + 402990x^{19} + 692496x^{20} + 2328900x^{21} + 1189650x^{22} \\ &+ 129402x^{23} + 3339000x^{24} + 1173564x^{25} + 928620x^{26} + 1512560x^{27} + 346380x^{28} \\ &+ 162540x^{29} + 167469x^{30} + 21630x^{31} + 5040x^{32} + 1890x^{33} + 60x^{35}. \end{aligned}$$

References

1. A. S. Hedayat, *The theory of trade-off for t-designs,* in: Coding Theory and Design Theory, Part II, Design Theory, IMA Math. Appl. Vol. 21 (D. Ray-Chaudhuri, ed.), Springer, New York, 1990, pp. 101-126.

2. D. Jungnickel and S. A. Vanstone, *Graphical codes revisited*, IEEE Trans. Inform. Th. **43**(1) (1997), 136-146.

3. G. B. Khosrovshahi and H. R. Maimani, *On* 2-$(v, 3)$ *Steiner trades of small volumes,* Ars Combin. **52** (1999), 199–220.

4. G. B. Khosrovshahi, H. R. Maimani and R. Torabi, *Classifications of* 2-$(6, 3)$ *and* 2-$(7, 3)$ *trades*, Australas. J. Combin. **19** (1999), 55–72.

5. G. B. Khosrovshahi and R. Naserasr, *Hypergraphical codes arising from binary codes*, Designs and codes—a memorial tribute to Ed Assmus. Des. Codes Cryptogr. **18** (1999), no. 1-3, 183–186.

6. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North Holland, Amsterdam, 1977.

7. J. H. van Lint, *Introduction to Coding Theory*, Second edition. Graduate Texts in Mathematics, 86. Springer-Verlag, Berlin, 1992.

8. R. M. Wilson, *A diagonal form for the incidence matrices of* t*-subsets vs.* k*-subsets*, European J. Combin. **11** (1990), 609-615.