Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 312-317*

Partitions and constant-value codes

A. J. Van Zanten A.J.vanZanten@twi.tudelft.nl
Delft University of Technology, Faculty of Information Technology and Systems
Dept. of Mathematics, P.O. Box 5031, 2600 GA Delft, THE NETHERLANDS
Veselin Vavrek veselin@chonbuk.ac.kr
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
P.O. Box 323, 5000 V. Tarnovo, BULGARIA

Abstract. We study the relationship between partitions of some integer a in $GF(p)$ in unequal parts of size at most $(p-1)/2$, and binary vectors with so-called value a. In particular we investigate a group of transformations acting on the family $A = \{A, A, ..., A\}$, where A stands for the set of all vectors of value i.

1 Preliminaries

Let p be some odd prime. We shall study the partitions of positive integers consisting of unequal parts the size of which is at most $(p-1)/2$. It will be obvious that we can represent such partitions by binary vectors $c = (c_1, c_2, \cdots, c_{(p-1)/2})$ of length $(p-1)/2$. Here, $c_i = 1$ if and only if the partition contains a part of size i . We interpret all vectors as row vectors. The number of ones in such a vector c is called the weight of the partition and is denoted by $|c|$. It stands for the number of parts in the partition. Let c be some partition. We define

$$a = \sum_{j=1}^{(p-1)/2} jc_j \mod p \tag{1}$$

and call a the value of c or $val(c)$, with $a \in \{0, 1, \cdots, p-1\}$. For a fixed value a, we collect all vectors having this value in a set A_a consisting of $|A_a|$ binary vectors of length $(p-1)/2$. So, this set contains all "conventional" partitions of the integers $a, a+p, a_2p, \cdots$ into unequal parts. We shall call such a set a *constant-value code*. We also introduce integers n_e and n_o, being the number of vectors in A_a with an even number of ones and an odd number, respectively. (We suppress the a-dependency of these integers in our notation). The complement of a partition c is defined as the partition corresponding to the vector $c = c + 1$, where 1 is the all-one vector of length $(p-2)/2$. Since the value of 1 is equal to

$$L := (p^2 - 1)/8 \mod p \tag{2}$$

all vectors of a set A_a have a complement of the same value $L-a$. Hence, we can write $A_a^c = A_{L-a}$ and we call A_a^c the complement of A_a. We also need the "value of the first halve of 1", defined by

$$K = 1+2+\cdots+[(p-1)/4] = (p^2 \mp 2p - 3)/32 \mod p, \tag{3}$$

for $p = \mp 1 \mod 4$. Consequently we have

$$L - 4K = (1 \pm p)/4 \mod p \tag{4}$$

Finally, we introduce the number $k \in GF(p)$, defined by

$$2k = L = (p^2-1)/8 \tag{5}$$

as equality in $GF(p)$. In order to deal with the sets $A_a,\ a \in \{0,1,\cdots,p-1\}$, we also introduce

$$N(p) = \begin{cases} \dfrac{2^{(p-1)/2}+1}{p}, & p = \pm 3 \mod p; \\ \dfrac{2^{(p-1)/2}-1}{p}, & p = \pm 1 \mod p. \end{cases} \tag{6}$$

2 A group of transformations

Let $I = \{1,2,\cdots,(p-1)/2\}$ and let m be some integer with $1 \le m \le p-1$. We introduce index sets

$$I_1 = \{i : i \in I,\ mi \mod p \in I\}, \quad I_2 := I \backslash I_1 \tag{7}$$

and a permutation matrix P with elements

$$p_{ij} = 1,\ j = mi \mod p,\ i \in I_1, or\ j = -mi \mod p,\ i \in I_2 \tag{8}$$

while $p_{i,j} = 0$ otherwise.

Theorem 1. *Let l be the order of $m \mod p$. Then the matrix P defined by (8) represents a permutation on I consisting of $(p-1)/l$ cycles of length $l/2$, for l is even, and of $(p-1)/2l$ cycles of length l, for l is odd.*

Proof. Consider the mapping $\mathcal{P} : GF(p) \to GF(p), \mathcal{P} = ma$. This mapping gives rise to a permutation of the elements of I in the following way. First, $\mathcal{P}$ permutes the nonzero elements of $GF(p)$ according to $(p-1)/l$ cycles of length l. Next, we change all elements a in these cycles which are not in I into $a' := a - p$, and then omit the minus sign of a'. If -1 is in the same cycle as 1, which is the case for l is even, this cycle of length l is transformed into a cycle of length $l/2$ followed by the same cycle of length $l/2$, while all elements now are in I. The same holds for all other cycles. If -1 and 1 are in different cycles of length l, which is the case for l is odd, then both cycles become identical after changing the minus signs. So, when omitting repeated cycles, we end up with a permutation of the elements of I as described in the theorem. For the matrix P the same holds. More precisely, this matrix represents the mapping $\mathcal{P}^{-1}$, modified by the above procedure. □

Next, we define a translation vector $t = (t_1, t_2, \cdots, t_{(p-1)/2})$, with $t_j = 1$ for $j = mi \mod p$, for $i \in I_1$, and $t_j = 0$ otherwise. Furthermore, we consider the transformation $T_m := GF(p)^{(p-1)/2} \to GF(p)^{(p-1)/2}$ defined by

$$T_m(c) = cP + t \tag{9}$$

Theorem 2. *For each m, $1 \leq m \leq p-1$, T_m induces a permutation τ_m on the set $A = A_0, A_1, \cdots, A_{p-1}$ such that $\tau_m(A_a) = A_b$, with $b = m(S_m - a)$ and $S_m = \sum_{i \in I_1} i$.*

Proof. We shall determine the value w' of the vector $b = T_m(a)$, with $val(a) = w$. The components $i \in I$ contribute $\sum_{i \in I_1} mi(1 - a_i)$ to w' and those in I_2 yield $\sum_{i \in I_2}(p - mia_i)$. Hence, both contributions together and taken mod p, give $w' = \sum_{i \in I_1} mi - \sum_{i \in I} mia_i = mS - mw$. □

Special cases

$m = 2$	$I_1 = 1, 2, \cdots, [(p-1)/4],\ I_2 = I \backslash I_1,$ $t = (0, 1, 0, 1 \cdots),\ w' = 2(S_2 - w) = 2(K - w);$
$m = (p-1)/2$	$I_1 = 1, 3, 5, \ldots,\ I_2 = 2, 4, 6, \ldots, t = (1, 0, 1, 0 \ldots),$ $w' = (p-1)/2 \cdot (S_{(p-1)/2} - w) = (p-1)/2 \cdot (L - K - w);$
$m = p-1$	$I_1 = \emptyset,\ I_2 = I,\ t = 0, P = E.$

Let $w_{i,n}$ be the value of the set $\tau_m^n(A_i)$. The integers $w_{i,n}$ satisfy in $GF(p)$ the recurrence relation

$$w_{i,n} = m(S_m - w_{i,n-1}),\ w_{i,0} = i, \tag{10}$$

which has as solution

$$w_{i,n} = \frac{m}{m+1} S_m(1 - (-m)^n) + i(-m)^n. \tag{11}$$

The permutations $\tau_m, 1 \leq m \leq p-1$, generate a permutation group G_A on A.

Theorem 3.

(i) G_A can be generated by a permutation $\tau_{-\alpha}$, where α is a generator of $GF(p)^*$.

(ii) G_A has one orbit A_k of size 1, whereas all other A_i, $i \neq k$, are in one orbit of size $p-1$.

Proof. Since α generates the multiplicative group of $GF(p)$, we can write $m = \alpha^e$ for any $m \in 1, 2, \ldots, p-1$. The permutation τ_m generates a subgroup of G_A. Equality (10) implies that $\frac{m}{m+1} S_m$ has the same value for all m. Since $S_1 = L$, it follows that $\frac{m}{m+1} S_m = \frac{L}{2}$. Next, from (10) and (11) we have that $w_{i,n} = i$ is equivalent to

$$(L/2 - i)(1 - (-m)^n) = 0 \tag{12}$$

The only i-value which satisfies this equation is $i = L/2 = k$. So, A_k is invariant with respect to all transformations of G_A. Furthermore, it will be clear from (11), that the length of the orbit to which $A_i, i \neq k$, belongs under the action of τ_m, is equal to the order of $-m \mod p$. So, if we take $m = -\alpha$, the orbit has length $p-1$. □

Example. For $p = 11$ we have the following data: $L = 4, k = 3, K = 3$. The family A of constant-value codes consists of the sets:

$A_0 = (0,0,0,0,0), (0,1,0,1,1), (1,1,1,0,1)$ $A_1 = (1,0,0,0,0), (0,0,1,1,1), (1,1,0,1,1)$
$A_2 = (0,1,0,0,0), (1,0,1,1,1)$
$A_3 = (0,0,1,0,0), (1,1,0,0,0), (0,1,1,1,1)$ $A_4 = (0,0,0,1,0), (1,0,1,0,0), (1,1,1,1,1)$
$A_5 = (0,0,0,0,1), (1,0,0,1,0), (0,1,1,0,0)$ $A_6 = (1,0,0,0,1), (0,1,0,1,0), (1,1,1,0,0)$
$A_7 = (0,1,0,0,1), (0,0,1,1,0), (1,1,0,1,0)$ $A_8 = (0,0,1,0,1), (1,0,1,1,0), (1,1,0,0,1)$
$A_9 = (0,0,0,1,1), (0,1,1,1,0), (1,0,1,0,1)$ $A_{10} = (1,0,0,1,1), (0,1,1,0,1), (1,1,1,1,0)$

In this case, 2 generates the multiplicative group of the relevant field, i.e. $GF(11)^*$. So, according to Theorem 3 the transformation $\tau_{-2} = \tau_9$ is a generator of G_A, and it acts transitively on the family $A_i | i \neq k$. In order to apply Theorem 2, we obtain $I_1 = 3, 4, 5$, and hence $S_9 = 3+4+5 = 1 \mod 11$. Indeed, the relations $\tau_9(A_a) = A_b$ and $b = 9(1-a)$ provide us with the transformations:

$$A_2 \to A_2,\ A_0 \to A_9 \to A_5 \to A_8 \to A_3 \to A_4 \to A_6 \to A_{10} \to A_7 \to A_1 \to A_0$$

3 Constructing A_{i+1} from A_i

Next, we shall discuss a method to transform a vector $a \in A_i$ into a vector $b \in A_{i+1}$. For the sake of convenience we assume that 2 is a generator of $GF(p)^*$. So, the matrix P in (8) corresponds to a $(p-1)/2$-cycle which we denote by

$$d := (d_1(=1), d_2, \ldots, d_{(p-1)/2}), \quad d_i \in I \tag{13}$$

Corresponding to (13) we define a binary vector p of length $(p-1)/2$, such that its i-th component is equal to the parity of the number of $d_j, j < i$, which are in I_2.

Now, let a be a binary vector representing some partition, and let $val(a) = i$. We define a translation vector t as follows. If $a_{d_j} \neq p_j,\ 1 \leq j < k$, and $a_{d_k} = p_k$

for some k, $1 \leq k \leq (p-1)/2$, we put $t_{d_j} = 1$, whereas all other components are zero. Formally, we can obtain t by

$$t = (1, \ldots, 1, 0, \ldots, 0)Q \tag{14}$$

where the vector at the rhs contains k ones followed by $(p-1)/2 - k$ zeros, while the transformation matrix Q has elements $q_{i,j} = 1$ if $j = d_i$ and $q_{i,j} = 0$ otherwise.

Theorem 4.

(i) *If* $a \in A_i$*, then* $b = a + t \in A_{i+1}$*, unless* $a = a_0 := p^c Q$*;*

(ii) *For* $p = \pm 3 \mod 8$*, the translation in (i) gives one-to-one mappings* $A_i \to A_{i+1}, \forall i \in GF(p) \backslash \{k-1, k\}$, $A_{k-1} \backslash \{a_0\} \to A_k$ *and* $A_k \to A_{k+1} \backslash \{a_0^c\}$*;*

(iii) *For* $p = \pm 1 \mod 8$*, the translation in (i) gives one-to-one mappings* $A_i \to A_{i+1}, \forall i \in GF(p) \backslash \{k-1, k\}$, $A_{k-1} \to A_k \backslash \{a_0^c\}$ *and* $A_k \backslash \{a_0\} \to A_{k+1}$.

Proof. We only have to take into account the change in the contribution to $val(a)$ due to the components $a_{d_1}, \ldots, a_{d_k}$. These contribute an amount of

$$\sum_{i=1}^{k} (-1)^{p_i} a_{d_i} 2^{i-1} \mod p,$$

where the signs are determined by the components of p. Because of the definition of k, we only have $(-1)^{p_i} = -1$ for those positions where $a_{d_i} = 0$, for $1 \leq i < k$. But these are precisely the positions where b has ones. Hence, we find

$$val(b) - val(a) = -\sum_{i=1}^{k} 2^{i-1} + (-1)^{p_k}(b_k - a_k)2^{k-1}. \tag{15}$$

If $a_k = p_k = 1$, then $b_k = 0$, and if $a_k = p_k = 0$, then $b_k = 1$, so the second term in the rhs always equals 2^{k-1}. We conclude that $val(b) - val(a) = -(2^{k-1} - 1) + 2^{k-1} = 1$. The only exception occurs when $a_{d_j} = p_j$ for all $j, ` \leq j \leq (p-1)/2$. In that case k is not defined. So,we proved parts (i) and (ii) under the assumption that 2 generates $GF(p)$, which is true if and only if $p = \pm 3 \mod 8$, or equivalently, when $\chi(2) = -1$. Similar results can be obtained in the case $p = \pm 1 \mod 8$. □

We may conclude from Theorems 3 and 4, applying eq. (6), that for all p the following result holds.

Corollary *For all* $i \neq k$ *one has* $|A_i| = N(p)$*, whereas* $|A_i| = N(p) + 1$ *for* $p = \pm 1 \mod 8$*, and* $|A_i| = N(p) - 1$ *for* $p = \pm 3 \mod 8$.

Example In our example $p = 11$, we now take $m = 2$. For this m-value, $I_1 = \{1, 2\}$ and $I_2 = \{3, 4, 5\}$. The 5-cycle (13) equals $d = (1\ 2\ 4\ 3\ 5)$, and hence $p = (0, 0, 0, 1, 0)$.

For $a = (1, 1, 1, 0, 1) \in A_0$, we find $k = 3$ and $t = (1, 1, 1, 0, 0)Q = (1, 1, 0, 1, 1)$. So, $b = a + t = (0, 0, 1, 1, 1)$, which indeed is a vector in A_1. If we take $a = (1, 1, 0, 1, 1) \in A_2$, then k is not defined, illustrating Theorem 4(i), since $a_p = (1, 1, 1, 0, 1)Q = (1, 1, 0, 1, 1)$. Taking for a the vectors ((0, 1, 0, 0, 0) and (1, 0, 1, 1, 1), both from A_2, yields (1, 1, 0, 0, 0) and (0, 1, 1, 1, 1), respectively. The third vector $(0, 0, 1, 0, 0) \in A_3$ is the complement a_p, thus confirming Theorem 4(ii).

As an illustration of Theorem 4(iii), we consider the simple case of $p = 7$, where $k = 3$. A generator of $GF(7)^*$ is -2. The corresponding matrix P, as defined by (8), stands for the cycle $(1\ 2\ 3)$. Now, if we continue our construction with 2 (though 2 is not a generator), we have $I_1 = \{1\}$ and $I_2 = \{2, 3\}$, and therefore $p = (0, 0, 1)$. Applying this vector, yields the following translations:

$$a = (0, 1, 0) \in A_2 \to (1, 1, 0) \in A_3, \quad a = (0, 0, 1) \in A_3 \to (1, 0, 1) \in A_4$$

In both translations k is equal to 1, while k is not defined for the vector $p^c = (1, 1, 0)$.

4 Remarks

Research on this topic is still in progress. Our primary motive was to develop a new approach, i.e in the context of algebraic coding theory, to the old and famous problem of determining the sign of the Gauss sum $G(2)$ (cf. [1] for a probably exhausting list of papers on this issue). It turns out that this problem is equivalent to determining the sign of $n_e - n_0$ (see Section 1) in the codes A_i. It was this background of which forced us to require the size of the parts in a partition not to exceed $(p-1)/2$. Actually, this condition is not too restrictive, since partitions of a containing one part of size $(p-1)/2$, can be dealt with by considering the partitions of $a - (p-1)/2$ as defined in this paper. Theorems 1 and 2 have their origin in [2, Lemma 4.2.4.4].

References

[1] B. Bruce, C. Berndt, R. J. Evans, The determination of Gauss sums, *Bull. Amer. Math. Soc.* 5, 1981, 107-129.

[2] V. V. Vavrek, Linear Codes and Conference Matrices (diss.), Delft University Press, Delft, 2005.