Another diametric theorem in Hamming spaces: optimal group anticodes

Rudolf Ahlswede*
Department of Mathematics
University of Bielefeld
POB 100131, D-33501 Bielefeld, Germany
Email: ahlswede@math.uni-bielefeld.de

***Abstract*— In the last century together with Levon Khachatrian we established a diametric theorem in Hamming space $\mathcal{H}^n = (\mathcal{X}^n, d_H)$.**

Now we contribute a diametric theorem for such spaces, if they are endowed with the group structure $\mathcal{G}^n = \sum_1^n \mathcal{G}$, the direct sum of a group $\mathcal{G}$ on $\mathcal{X} = \{0, 1, \dots, q-1\}$, and as candidates are considered subgroups of $\mathcal{G}^n$.

For all finite groups $\mathcal{G}$, every permitted distance d, and all $n \geq d$ subgroups of $\mathcal{G}^n$ with diameter d have maximal cardinality q^d.

Other extremal problems can also be studied in this setting.

I. Introduction

As in [2] we study optimal anticodes in Hamming spaces $\mathcal{H}^n = (\mathcal{X}^n, d_H)$ but now with the additional constraint that they form a **subgroup** of $\mathcal{G}^n = \sum_1^n \mathcal{G}$, the direct sum of a group $\mathcal{G}$ on $\mathcal{X} = \{0, 1, \dots, q-1\}$. Thus we consider

$$A\mathcal{G}(n,d) = \max\{|\mathcal{U}| : \mathcal{U} \text{ is a subgroup of } \mathcal{G}^n \text{ with } D(\mathcal{U}) \leq d\}, \tag{1.1}$$

where

$$D(\mathcal{U}) = \max_{u,u' \in \mathcal{U}} d_H(u, u') \tag{1.2}$$

is the diameter of $\mathcal{U}$.

Farrell [5], see also [8], has introduced anticodes (n, r, d) as subspaces of $GF(2)^n$ with diameter constraint d and dimension r. But even this special case of our problem (consisting in maximizing r for given n, d) has not even been considered. They were actually used for an analysis of codes (see [8]) and in that connection words in $\mathcal{U}$ were even considered with **multiplicities**.

In [2] we solved the long standing problem of determining

$$A(n,d) = \max\{|\mathcal{A}| : \mathcal{A} \subset \mathcal{X}^n \text{ with } D(\mathcal{A}) \leq d\}$$

and we gave – up to isomorphy – all extremal anticodes:

For $0 \leq i \leq \frac{d}{2}$ define $K_i \subset \mathcal{X}^n$ as cartesian product of the ball $B_i^{n-d+2i}(\bar{0})$ with center $\bar{0}^{n-d+2i}$ and radius i in $\mathcal{X}^{n-d+2i}$ and $\mathcal{X}^{d-2i}$.

Clearly K_i has diameter d.

Diametric Theorem of [2]. Let r be the largest integer s.t.

$$n - d + 2r < \min\left\{n+1, n-d+2\frac{n-d-1}{q-2}\right\},$$

then

$$A(n,d) = |K_r|.$$

Moreover, up to permutations of $\{1, 2, \dots, n\}$ and permutations of the alphabet $\mathcal{X} = \{0, \dots, q-1\}$ in the components the optimal configuration is unique, unless

$$n - d > 1, n - d + 2\frac{n-d-1}{q-2} \leq n$$

and $\frac{n-d-1}{q-2}$ is integral, in which case we have two optimal configurations:

$$K_{\frac{n-d-1}{q-2}} \quad \text{and} \quad K_{\frac{n-d-1}{q-2}-1}.$$

Finally we mention that we write groups additive, because we write concatenation of words multiplicative, for $u^n \in \mathcal{G}^n : u^n = u_1 u_2 \dots u_n$. For $A \subset \mathcal{G}^{n-1}$ and $a \in \mathcal{G}$ we write Aa for the set $\{a^n = a_1 a_2 \dots a_{n-1} a : a_1 a_2 \dots a_{n-1} \in A\}$ and more generally for $B \subset \mathcal{G}^m$ and $a^\ell \in \mathcal{G}^\ell$ we write Ba^ℓ for the set $\{b^m a^\ell : b^m \in B\}$. Furthermore for $A \subset \mathcal{G}^m$, $B \subset \mathcal{G}^\ell$

$$AB = \{ab : a \in A, b \in B\}.$$

*The author was supported by the 'Finite Structures' Marie Curie Host Fellowship for the Transfer of knowledge project carried out by Alfred Renyi Institute of Mathematics, in the framework of the European Community's Structuring the European Research Area programme.

II. More notions

Def. 1: The zero word of length ℓ and the one word of length ℓ is denoted by $\underline{0}^\ell$ and $\underline{1}^\ell$, respectively.

Def. 2: For $\mathcal{U} \subset \mathcal{X}^n$ (or $\mathcal{G}^n$) we define for $S \subset \mathcal{X}$, $S \neq \emptyset$,

$$\mathcal{U}_S = \{u_1 \dots u_{n-1} : u_1 \dots u_{n-1}s \in \mathcal{U} \text{ for all } s \in S \text{ and } u_1 \dots u_{n-1}s \notin \mathcal{U} \text{ for all } s \in \mathcal{X} \smallsetminus S\}.$$

Clearly

$$\mathcal{U}_S \cap \mathcal{U}_{S'} = \emptyset \text{ if } S \neq S'. \tag{2.1}$$

Def. 3: For $\mathcal{U} \subset \mathcal{X}^n$ we define $\mathcal{U}^{(n-1)} = \{u_1 \dots u_{n-1} : u_1 \dots u_n \in \mathcal{U} \text{ for some } u_n \in \mathcal{X}\}$, which equals $\bigcup\limits_{S\neq\emptyset} \mathcal{U}_S$.

Def. 4: For $\mathcal{U} \subset \mathcal{X}^n$ we define $\mathcal{U}_{(n)} = \{u_n \in \mathcal{X} :$ there exists a $u_1 \dots u_{n-1}$ with $u_1 \dots u_n \in \mathcal{U}\}$.

Def. 5: For $\mathcal{U} \subset \mathcal{X}^n$ we define for $\varepsilon \in \mathcal{X}$

$$\mathcal{U}[\varepsilon] = \{u^n = u_1 \dots u_n \in \mathcal{U} : u_n = \varepsilon\}.$$

Def. 6: For $\mathcal{G} = \mathcal{C}_2$, the cyclic group of order 2, we define the down-pushing operation T_0^1 by setting for any $\mathcal{U} = \mathcal{U}_{\{0\}}0 \cup \mathcal{U}_{\{1\}}1 \cup \mathcal{U}_{\{0,1\}}\{0,1\}$

$$T_0^1(\mathcal{U}) = \mathcal{U}_{\{0\}}0 \,\dot\cup\, \mathcal{U}_{\{1\}}0 \cup \mathcal{U}_{\{0,1\}}\{0,1\}.$$

For convenience we also write

$$A = \mathcal{U}_{\{0\}}, B = \mathcal{U}_{\{1\}}, \text{ and } C = \mathcal{U}_{\{0,1\}}. \tag{2.2}$$

Obviously,

$$|\mathcal{U}| = |T_0^1(\mathcal{U})|. \tag{2.3}$$

Def. 7: For two sets $\mathcal{V}, \mathcal{W} \subset \mathcal{X}^n$ their maximal distance is

$$D(\mathcal{V}, \mathcal{W}) = \max_{u\in\mathcal{V}, v\in\mathcal{W}} d_H(u, v).$$

III. The binary case

We first considered and settled the case $\mathcal{X} = \{0, 1\}$ and $\mathcal{G} = \mathcal{C}_2$.

Theorem 1. For $n \geq d$

(i) $A\mathcal{C}_2(n, d) = 2^d$
(ii) $\mathcal{X}^d\underline{0}^{n-d}$ is optimal and up to isomorphy (permutations of components) unique for $d \geq 3$.
(iii) For $d = 2$ there is also the additional solution $\{110, 101, 011, 000\}\underline{0}^{n-3}$.

The proof is based on the following five lemmas.

Lemma 1. For $\mathcal{U} \subset \{0, 1\}^n$

$$D(\mathcal{U}) \geq D\big(T_0^1(\mathcal{U})\big).$$

Proof: Since $D(B1) = D(B0)$, it remains to notice that

$$D\big(B1, A0 \cup C\{0, 1\}\big) \geq D\big(B0, A0 \cup C\{0, 1\}\big). \tag{3.1}$$

Lemma 2. For a subgroup $\mathcal{U} \subset \mathcal{C}_2^n$ $T_0^1(\mathcal{U})$ is again a subgroup.

Proof: Since $u + u = \underline{0}^n \in \mathcal{C}_2^n$, it suffices to show that $u\varepsilon, v\delta \in T_0^1(\mathcal{U})$ implies $(u + v)(\varepsilon + \delta) \in T_0^1(\mathcal{U})$. Since $T_0^1(\mathcal{U})[0] \supset \mathcal{U}[0]$, the implication is obvious for $\varepsilon = \delta = 0$ and $\varepsilon = \delta = 1$. So $u1 + v0$ remains to be checked. That is, $u1 \in C\{0, 1\}$, and therefore also $u0 \in C\{0, 1\}$. Since $\mathcal{U}$ is a subgroup, $(u + v)1$ and $(u + v)0 \in \mathcal{U}$ and in particular $u + v \in C$ and $u1 + v0 \in C\{0, 1\}$.

Lemma 3. For a subgroup $\mathcal{U} \subset \mathcal{C}_2^n$

(i) $C\{0, 1\}$ is a subgroup
(ii) $A0$ is a subgroup
(iii) C and A are subgroups in $\mathcal{C}_2^{n-1}$
(iv) Either $C = \emptyset$ or $A = \emptyset$.

Proof: Ad (i) If $u, v \in C$, then $u\varepsilon, v\delta \in \mathcal{U}$ for all $\varepsilon, \delta \in \{0, 1\}$ and therefore $(u + v)0, (u + v)1 \in \mathcal{U}$ and $(u + v)0, (u + v)1 \in C\{0, 1\}, u + v \in C$.

Ad (ii) $u0 + v0 = (u + v)0 \in A0 \cup C\{0, 1\}$. If now $(u+v)0 \notin A0$, then $(u+v) \in C$ and both, $(u+v)0$ and $(u+v)1 \in C\{0, 1\}$. But then $(u+v)1 + u0 = v1 \in \mathcal{U}$ and since also $v0 \in \mathcal{U}$ we get $v \in C$ in contradiction to $v \in A$.

Ad (iii) This way it is also shown that A is a subgroup in $\mathcal{C}_2^{n-1}$. For C this is shown already in (i).

Ad (iv) By definition $C \cap A = \emptyset$ and as subgroups, if not empty, they contain both $\underline{0}^{n-1}$, a contradiction.

Lemma 4. For a subgroup $\mathcal{U} \subset \mathcal{C}_2^n$ $C \neq \emptyset$ implies $B = \emptyset$ and $\mathcal{U} = C\{0, 1\}$.

Proof: We know from Lemma 3 that $C \neq \emptyset$ implies $A = \emptyset$. Now suppose that $b \in B$. Then $b1 + b1 = \underline{0}^{n-1}0 \in C\{0, 1\}$ and therefore $\underline{0}^{n-1}1 \in C\{0, 1\}$, $b1 + \underline{0}^{n-1}1 = b0 \in \mathcal{U}$, which contradicts $b \in B$ and thus $B = \emptyset$.

Lemma 5. For a subgroup $\mathcal{U} \subset \mathcal{C}_2^n$ with $C = \emptyset$, clearly

(i) $\mathcal{U} = A0 \cup B1 = A0 \,\dot\cup\, A0 + \alpha$, $|\mathcal{U}| = 2|A|$
(ii) $T_0^1(\mathcal{U}) = A0 \,\dot\cup\, (A + g)0$.

Proof: (i) By Lemma 3 $\mathcal{U} = A0 \cup B1$. Since $A0$ is a subgroup of $\mathcal{U}$, $\mathcal{U} = A0 \cup \bigcup\limits_{i=1}^{I} g_i1 + A0$. Necessarily,

$$b1 + b'1 = (b + b')0 \in A0$$
$$b1 = b'1 + (b + b')0$$

and consequently, $I = 1$ and $\mathcal{U} = A0 \cup g1 + A0$.
(ii) This is obvious.

Key Example: For the subgroup
$\mathcal{U} = \{011, 101, 110, 000\} = A0 \cup B1$, we have

$T_0^1(\mathcal{U}) = \{010, 100, 110, 000\} = A0 \cup B0 = \mathcal{C}_2^2 0$.
Notice that $D(\mathcal{U}) = 2 = D\big(T_0^1(\mathcal{U})\big)$.

Finally, these lemmas make it possible, to iteratively apply transformations T_0^1 to a subgroup, keeping the cardinality constant and not increasing the diameter. We keep extracting factors $\{0,1\}$ until in all components $C = \emptyset$ and Lemma 5 applies, and we can extract a factor 0. **The procedure ends with a subgroup of the form $\mathcal{C}_2^d \underline{0}^{n-d}$.**

We leave it as an exercise to show that the Key Example provides the only other extremal configuration.

IV. A related intersection result in the binary case

The case $q = 2$ of the Diametric Theorem stated in the Introduction was first proved much earlier by D. Kleitman [7].

In [1] it was shown that this theorem and Katona's Intersection Theorem in equivalent formulation for unions can be easily transformed into each other by using operations T_0^1. Since these operations transform subgroups into subgroups and for

$$E(\mathcal{U}) = \max_{u,u' \in \mathcal{U}} W(u \ \vee \ u')$$

with W counting the number of 1's, we have as analogue to Lemma 1

Lemma 1'. For $\mathcal{U} \subset \{0,1\}^n$

$$E(\mathcal{U}) \geq E\big(T_0^1(\mathcal{U})\big).$$

so we also get as analogue to Theorem 1 for $K\mathcal{C}_2(n,d) = \max\{|\mathcal{U}| : \mathcal{U}$ is subgroup of $\mathcal{C}_2^n$ with $E(\mathcal{U}) \leq d\}$

Theorem 1'. For $n \geq d$ and all d

(i) $K\mathcal{C}_2(n,d) = 2^d$
(ii) $\mathcal{X}^d \underline{0}^{n-d}$ is optimal and up to isomorphy unique.

The case (iii) in Theorem 1 does not occur because the equivalence holds for downsets.

Remark: The "dual problem" of intersection becomes meaningless, because $\underline{0}^n$ has empty intersections with other $x^n \in \mathcal{U}$. However, we can do it with a coset of a subgroup $\underline{1}^n + \mathcal{U}$. This readily follows, because addition of $\underline{1}^n$ amounts to complementation.

V. The case $\mathcal{G} = \mathcal{C}_3$ and beyond

We show now how the previous approach generalizes. We assume $q = 3$ and the cyclic group $\mathcal{C}_3$ of order 3.

For any subgroup $\mathcal{U} \subset \mathcal{C}_3^n$ we consider sets $\mathcal{U}_S$, that is,

$$\mathcal{U}_{\{0\}}, \mathcal{U}_{\{1\}}, \mathcal{U}_{\{2\}}, \mathcal{U}_{\{0,1\}}, \mathcal{U}_{\{0,2\}}, \mathcal{U}_{\{1,2\}}, \mathcal{U}_{\{0,1,2\}}.$$

A **simple basic observation** is, that for $u \in \mathcal{U}_{\{0,1\}}$

$$u0 + u0 + u1 + u1 = u2 \in \mathcal{U} \tag{5.1}$$

and therefore $\mathcal{U}_{\{0,1\}} = \emptyset$.

Similarly, for $v \in \mathcal{U}_{\{0,2\}}$

$$v0 + v0 + v2 + v2 = v1 \in \mathcal{U} \tag{5.2}$$

and therefore $\mathcal{U}_{\{0,2\}} = \emptyset$.

Finally, for $w \in \mathcal{U}_{\{1,2\}}$

$$w1 + w1 + w2 + w2 = w0 \tag{5.3}$$

and therefore $\mathcal{U}_{\{1,2\}} = \emptyset$.

This leaves us with

$$\mathcal{U}_{\{0\}}, \mathcal{U}_{\{1\}}, \mathcal{U}_{\{2\}}, \mathcal{U}_{\{0,1,2\}}.$$

We summarize this.

Lemma 6. For a subgroup $\mathcal{U} \subset \mathcal{C}_3^n$

(i) $\mathcal{U} = \mathcal{U}_{\{0\}}0 \cup \mathcal{U}_{\{1\}}1 \cup \mathcal{U}_{\{2\}}2 \cup \mathcal{U}_{\{0,1,2\}}\{0,1,2\}$
(ii) $D(\mathcal{U}) \geq D\big(T_0^\alpha(\mathcal{U})\big)$ for $\alpha = 1, 2$, where T_0^α is defined analogously to T_0^1 in Definition 6.

Proof: W.l.o.g. consider $\varepsilon = 1$ and add to the proof of Lemma 1 that $D(\mathcal{U}_{\{1\}}1, \mathcal{U}_{\{2\}}2) = D(\mathcal{U}_{\{1\}}0, \mathcal{U}_{\{2\}}2)$, completing the present proof.

Lemma 7. For a subgroup $\mathcal{U} \subset \mathcal{C}_3^n$ $\quad T_0^\alpha(\mathcal{U})$ is again a subgroup.

We leave the proof and the establishment of the analogues of the other lemmas in Section 3.

Also it is a nice exercise to find out how our approach with operations T_0^α goes.

VI. A general approach not using down pushing

We have learnt that **subsets S containing 0 play a basic role** in proving Theorem 1. We denote them by S_0. They are the starting point of our second approach. We begin with

Lemma 8. For a subgroup $\mathcal{U} \subset \mathcal{G}^n$ a non-empty $\mathcal{U}_{\{0\}}0$ is a subgroup of $\mathcal{U}$.

Proof: For $u, v \in \mathcal{U}_{\{0\}}$, if $u0 + v0 \in \mathcal{U}_S S$, $S \neq \{0\}$, then an $x \in S, x \neq 0$ exists with

$$(u+v)x \in \mathcal{U}_S S \text{ and } (u+v)x - u0 = vx \in \mathcal{U},$$

but this contradicts $v \in \mathcal{U}_{\{0\}}$ (because v occurs with extension 0 only).

Therefore $u0 + v0 \in \mathcal{U}_{\{0\}}$. It remains to be seen that $u0$ has an inverse in $\mathcal{U}_{\{0\}}0$.

Clearly, it has an inverse $v0$ in $\mathcal{U}$

$$u0 + v0 = \underline{0}^n. \tag{6.1}$$

If now $v0 \in \mathcal{U}_S S$, $S \neq \{0\}$, then for some $x \in S, x \neq 0 \quad vx \in \mathcal{U}_S S$ and

$$u0 + vx = u0 + v0 + \underline{0}^{n-1}x = \underline{0}^{n-1}x \in \mathcal{U}.$$

Consequently $u0 + \underline{0}^{n-1}x = ux \in \mathcal{U}$ in contradiction with $u0 \in \mathcal{U}_{\{0\}}0$. Therefore $v0 \in \mathcal{U}_{\{0\}}0$ and $\mathcal{U}_{\{0\}}0$ is subgroup of $\mathcal{U}$.

Lemma 9 (Generalization of Lemma 8). For a subgroup $\mathcal{U} \subset \mathcal{G}^n$ a non-empty $\mathcal{U}_{S_0}0$ is subgroup of $\mathcal{U}$.

Proof: If for $u, v \in \mathcal{U}_{S_0} \quad u0 + v0 \notin \mathcal{U}_{S_0}0$, then $u0 + v0 \in \mathcal{U}_S 0$ and $u + v \in \mathcal{U}_S$, where $S \neq S_0$ and $S \supset S_0$, because $u0 \in \mathcal{U}$ and for all $s \in S_0 \quad vs \in \mathcal{U}$ and hence $u0 + vs \in \mathcal{U}$, $(u+v)s = u0 + vs \in \mathcal{U}$. Now for $x \in S \setminus S_0 \quad (u+v)x - u0 = vx \in \mathcal{U}$, but this contradicts $v \in \mathcal{U}_{S_0}$ and hence $u0 + v0 \in \mathcal{U}_{S_0}0$.

It remains to be seen that $u0$ has an inverse in $\mathcal{U}_{S_0}0$.

There is a $v0$ in $\mathcal{U}$ with

$$u0 + v0 = \underline{0}^n. \tag{6.2}$$

If $v0 \notin \mathcal{U}_{S_0}0$, then $v0 \in \mathcal{U}_S 0$, where $S \neq S_0$ and $S \supset S_0$, because for all $s \in S_0 \quad us \in \mathcal{U}$ and since $u0 + vs = us + v0 \in \mathcal{U}$ also $vs \in \mathcal{U}$.

Now for $x \in S \setminus S_0 \quad u0 + vx \in \mathcal{U}$ and therefore $ux + v0 \in \mathcal{U}$ and $ux \in \mathcal{U}$ in contradiction to $u \in \mathcal{U}_{S_0}$. Thus $\mathcal{U}_{S_0}0$ is a subgroup.

Lemma 10. For a subgroup $\mathcal{U} \subset \mathcal{G}^n$

(i) There is exactly one S_0 with $\mathcal{U}_{S_0} \neq \emptyset$
(ii) S_0 is a group
(iii) $\mathcal{U}_{S_0}S_0$ is a subgroup of $\mathcal{U}$

Proof: Ad (i) Since $\underline{0}^n \in \mathcal{U}_{S_0}S_0$ for all sets of type S_0 (by Lemma 9), disjointness of these sets gives the result.

Ad (ii) Since $\underline{0}^n \in \mathcal{U}_{S_0}S_0$, also $\underline{0}^{n-1}s \in \mathcal{U}_{S_0}S_0$ for all $s \in S_0$, and for all $s, s' \in S_0$

$$\underline{0}^{n-1}s + \underline{0}^{n-1}s' = \underline{0}^{n-1}s'' \in \mathcal{U}.$$

If $s'' \notin S_0$, then this contradicts that $\underline{0}^{n-1} \in \mathcal{U}_{S_0}$. Therefore $s + s' = s'' \in S_0$. Concerning the inverse of s in S_0 use that $\underline{0}^{n-1}s$ has an inverse $\underline{0}^{n-1}(-s) \in \mathcal{U}$. Again by definition of $\mathcal{U}_{S_0} \quad -s \in S_0$.

Ad (iii) $\mathcal{U}_{S_0}S_0$ is subgroup because it is a direct sum of groups and contained in $\mathcal{U}$.

VII. More on the structure of subgroups $\mathcal{U}$

We have learnt that S_0 is a subgroup in $\mathcal{G}$, that so is $\mathcal{U}_{S_0}$ in $\mathcal{G}^{n-1}$, and finally $\mathcal{U}_{S_0}S_0$ in $\mathcal{U}$.

We can decompose $\mathcal{U}$ into cosets of $\mathcal{U}_{S_0}S_0$ and begin with coset leaders of the form $\underline{0}^{n-1}\alpha_i$ $(i = 1, 2, \ldots, I)$, elements of $\mathcal{U}$, such that

$$S_0 + \alpha_i \text{ are disjoint for } i = 1, 2, \ldots, I. \tag{7.1}$$

This gives cosets in $\mathcal{U}$:

$$\mathcal{U}_{S_0}(S_0 + \alpha_i) \quad \text{for } i = 1, 2, \ldots, I.$$

However, necessarily $I = 1$, because otherwise we have a contradiction with the definition of $\mathcal{U}_S$. So we may choose also $\alpha_1 = 0$.

Next we consider $\mathcal{U}_{S_0 + \varphi(\alpha_i)}(S_0 + \alpha_i)$, $\alpha_i \notin S_0$.

For example for $\mathcal{U} = \left\{ \begin{matrix} 00 & 0 \\ 11 & 0 \\ 10 & 1 \\ 01 & 1 \end{matrix} \right\}$, $S_0 = \{0\}$, $\mathcal{U}_{S_0} = \{00, 11\}$ we have

$$\mathcal{U}_{S_0}S_0 \,\dot{\cup}\, \mathcal{U}_{S_0}S_0 + 101 = \mathcal{U}$$

with $\alpha_2 = 1$ and $\varphi(\alpha_2) = 10$.

Generally using $\mathcal{U}_{S_0}S_0$ we can make a decomposition

$$\mathcal{U} = \dot{\bigcup_{\gamma}} (\mathcal{U}_{S_0} + \gamma)(S_0 + \psi(\gamma)) \tag{7.2}$$

for suitable ψ.

Now comes a new idea.

Remember that

$$\mathcal{U} = \dot{\cup}\, \mathcal{U}_S \cdot S. \tag{7.3}$$

By Lemma 10 there exists exactly one S_0 with $\mathcal{U}_{S_0} \neq \emptyset$.

Lemma 11. If for a subgroup $\mathcal{U} \subset \mathcal{G}^n \quad |S_0| \geq 2$, then **the transformation**

$$L : \bigcup_S \mathcal{U}_S S \longrightarrow \left(\bigcup_S \mathcal{U}_S \right) \cdot \mathcal{G}$$

results in a group of diameter $\leq d$ and a not decreased cardinality.

Proof: Use the decomposition in (7.2).

Consequently every u^{n-1} occuring in some $\mathcal{U}_{S_0}+\gamma$ has **multiplicity** $=|S_0+\psi(\gamma)|=|S_0|$ and gets by the transformation multiplicity $|\mathcal{G}|\geq|S_0|$. So the cardinality does not decrease. Furthermore by (7.2)

$$D\big(\mathcal{U}_{S_0}+\gamma\big)\leq d-1$$

and also

$$D\big(\mathcal{U}_{S_0}+\gamma,\mathcal{U}_{S_0}+\gamma'\big)\leq d-1$$

and the transformation L is appropriate.

It remains to analyse the case $S_0=\{0\}$.

Here, due to the definition of $\mathcal{U}_{S_0}$, the decomposition $\mathcal{U}=\bigcup\limits_{\alpha\in\mathcal{U}(n)}\big(\mathcal{U}_{S_0}+\varphi(\alpha)\big)\alpha$ holds with $\mathcal{U}(n)$ from Definition 4. The terms $\big(\mathcal{U}_{S_0}+\varphi(\alpha)\big)\alpha$ are disjoint or equal.

If $\mathcal{U}_{S_0}+\varphi(\alpha)=\mathcal{U}_{S_0}+\varphi(\beta)$, $\varphi(\alpha)-\varphi(\beta)\in\mathcal{U}_{S_0}$, since $d(\alpha,\beta)=1$

$$D\big(\mathcal{U}_{S_0}+\varphi(\alpha)\big)=D(\mathcal{U}_{S_0})\leq d-1,$$

when $D\big(\mathcal{U}_{S_0}+\varphi(\alpha)\big)\leq d-1$ for all α we can replace α by $\mathcal{G}$.

So it remains

$$\mathcal{U}_{S_0}+\varphi(\alpha)\neq\mathcal{U}_{S_0}+\varphi(\beta) \text{ for all } \alpha\neq\beta.$$

Here replace all α by 0. As an illustration look at the

Example: $\mathcal{U}=\left\{\begin{matrix} 11 & 0 \\ 00 & 0 \\ 10 & 1 \\ 01 & 1 \end{matrix}\right\}$

Theorem 3. For any finite abelian group $\mathcal{G}$ and $n\geq d$

$$A\mathcal{G}(n,d)=|\mathcal{G}|^d.$$

As a further problem one can try to extend Theorem 1' to the non-binary case with the constraint $|a^n\vee b^n|\leq d$.

REFERENCES

[1] R. Ahlswede and G. Katona, Contributions to the geometry of Hamming spaces, Discrete Mathematics 17, 1-22, 1977.
[2] R. Ahlswede and L.H. Khachatrian, The diametric theorem in Hamming spaces - optimal anticodes, Advances in Applied Mathematics 20, 429-449, 1998.
[3] R. Ahlswede and L.H. Khachatrian, The complete intersection theorem for systems of finite sets, European J. Combinatorics, 18, 125-136, 1997.
[4] R. Ahlswede and L.H. Khachatrian, A pushing-pulling method: new proofs of intersection theorems, Combinatorica 19(1), 1-15, 1999.
[5] P.G. Farrell, Linear binary anticodes, Electronics Letters 6, 419-421, 1970.
[6] G. Katona, Intersection theorems for systems of finite sets, Acta Math. Acad. Sci. Hung. 15, 329-337, 1964.
[7] D. Kleitman, On a combinatorial conjecture of Erdos, J. Combin. Theory 1, 209-214, 1966.
[8] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland.