A diametric theorem in $\mathbb{Z}_m^n$ for Lee and related distances

Rudolf Ahlswede[1], and Faina I. Solov'eva[2]

[1] Universität Bielefeld, Fakultät für Mathematik, Postfach 100131, 33501 Bielefeld, Germany; hollmann@math.uni-bielefeld.de
[2] Sobolev Institute of Mathematics and Novosibirsk State University, pr. ac. Koptyuga 4, Novosibirsk 630090, Russia; sol@math.nsc.ru

Abstract. We present the diametric theorem for additive anticodes with respect to the Lee distance in $\mathbb{Z}_{2^k}^n$, where $\mathbb{Z}_{2^k}$ is an additive cyclic group of order 2^k. We also investigate optimal anticodes in $\mathbb{Z}_{p^k}^n$ for the homogeneous distance and in $\mathbb{Z}_m^n$ for the Krotov-type distance.

1 Introduction

In this paper we establish the diametric theorem for optimal additive anticodes in $\mathbb{Z}_{2^k}^n$ with respect to the Lee distance, where $\mathbb{Z}_{2^k}$ is any additive cyclic group of order 2^k. We also study additive anticodes for related distances such as the homogeneous distance, see [7], and the Krotov-type distance, see [13].

Farrell [8], see also [15], has introduced the notion of an anticode (n, k, d) as a subspace of $GF(2)^n$ with diameter constraint d (the maximum Hamming distance between codewords) and dimension k. In fact earlier anticodes were used by Solomon and Stiffler [16] to construct good linear codes meeting the Griesmer bound, see also [6]. Such anticodes may contain repeated codewords.

Like in [1] we study anticodes without multiple codewords. The notion of an optimal anticode investigated in the paper is different from the notion in [15], Chapter 17. Let G^n be the direct product of n copies of a finite group G defined on the set $\mathcal{X} = \{0, 1, \ldots, q-1\}$. We investigate

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

where $D(\mathcal{U}) = \max\limits_{u,u' \in \mathcal{U}} d(u, u')$ is the diameter of $\mathcal{U}$, $d(\cdot, \cdot)$ is the Hamming distance for any finite group G, the Lee distance or the homogeneous distance for any cyclic group $\mathbb{Z}_{p^k}$, where p is prime, or a Krotov-type distance for $\mathbb{Z}_m^n$. In [4] the complete solution of the long standing problem of determining

$$\max\{|\mathcal{U}| : \mathcal{U} \subset \mathcal{X}^n \text{ with } D_H(U) \leq d\},$$

for the Hamming distance d, is presented and all extremal anticodes are given. Another diametric theorem in Hamming spaces for group anticodes is established in [1]: for any finite group G, every permitted Hamming distance d, and all $n \geq d$ subgroups of G^n with diameter d have maximal cardinality q^d.

In Section 2 we give necessary definitions and auxiliary results from [1], in Sections 3 and 4 we prove the diametric theorem for $\mathbb{Z}_{2^k}^n$ with respect to the Lee distance, in Section 5 we investigate optimal anticodes in $\mathbb{Z}_{p^k}^n$ endowed with the homogeneous distance, and Section 6 is devoted to optimal anticodes in $\mathbb{Z}_m^n$ for Krotov type distances.

2 Preliminary definitions and auxiliary results

Throughout in what follows we consider groups additive and write the concatenation of words multiplicative, i.e. for $u^n \in \mathbb{Z}_m^n$ we use $u^n = u_1 u_2 \dots u_n$. The all-zero word of length n is denoted by 0^n.

Definition 1. *For any $\mathcal{U} \subset \mathcal{X}^n$ and $\mathcal{S} \subset \mathcal{X}$, where $\mathcal{S} \neq \emptyset$, we define*

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

¿From this definition we have the property

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

Definition 2. *For any $\mathcal{U} \subset \mathcal{X}^n$ we define*

$$\mathcal{U}_{(n)} = \{u_n \in \mathcal{X} : \text{ there exists a word } u_1 \dots u_{n-1} \text{ such that } u_1 \dots u_{n-1} u_n \in \mathcal{U}\}.$$

For two sets $\mathcal{U}, \mathcal{V} \subset \mathcal{X}^n$ their cross-diameter is defined as

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

Let G be any finite Abelian group. Denote by $\mathcal{S}_0$ a subset of G containing 0. Further we will use the following three lemmas, which can be found in [1].

Lemma 1. *For any subgroup $\mathcal{U}$ of G^n (briefly $\mathcal{U} < G^n$) a non-empty subset $\mathcal{U}_{\{0\}}0$ of $\mathcal{U}$ is its subgroup.*

Lemma 2. (Generalization of Lemma 1) *If $\mathcal{U} < G^n$ then for a non-empty subset $\mathcal{U}_{\mathcal{S}_0}0$ from $\mathcal{U}$ it is true that $\mathcal{U}_{\mathcal{S}_0}0 \leq \mathcal{U}$.*

Lemma 3. *If $\mathcal{U}$ is a subgroup of G^n, then*

(i) there is exactly one subset $\mathcal{S}_0$ in G with $\mathcal{U}_{\mathcal{S}_0} \neq \emptyset$;
(ii) the set $\mathcal{S}_0$ is a group;
(iii) the set $\mathcal{U}_{\mathcal{S}_0}\mathcal{S}_0$ is a subgroup of $\mathcal{U}$.

By Lemma 3 we have $\mathcal{U}_{\mathcal{S}_0}\mathcal{S}_0 \leq \mathcal{U}$, so we can decompose a group $\mathcal{U}$ into cosets of the subgroup $\mathcal{U}_{\mathcal{S}_0}\mathcal{S}_0$:

$$\mathcal{U} = \bigcup_{\alpha} (\mathcal{U}_{\mathcal{S}_0} + \alpha)(\mathcal{S}_0 + \psi(\alpha)) \tag{2.2}$$

for suitable ψ.

3 A diametric theorem in $\mathbb{Z}_{2^k}^n$ for Lee distance

Let $\mathbb{Z}_m$ be an additive cyclic group of order m. The Lee weight of $i \in \mathbb{Z}_m$ is defined as

$$w_L(i) = \min\{i, m - i\}.$$

For $u = (u_1, \dots, u_n) \in \mathbb{Z}_m^n$, $w_L(u) = \sum_{i=1}^{n} w_L(u_i)$ and for $u, v \in \mathbb{Z}_m^n$ the Lee distance between u and v is

$$d_L(u, v) = w_L(u - v).$$

Let $\mathcal{U}$ be any subgroup of $\mathbb{Z}_m^n$. The Lee diameter of $\mathcal{U}$ we define as

$$D_L(\mathcal{U}) = \max_{u,v \in \mathcal{U}} d_L(u, v).$$

For any two sets $\mathcal{U}, \mathcal{V} \subset \mathbb{Z}_m^n$ their Lee cross-diameter is

$$D_L(\mathcal{U}, \mathcal{V}) = \max_{u \in \mathcal{U}, v \in \mathcal{V}} d_L(u, v).$$

It is well-known that the order of any group is divisible by the order of any of its subgroups.

Let $\mathbb{Z}_m$ be an additive cyclic group, then for any $r|m$ denote by $\left(\frac{m}{r}\right)$ the subgroup of $\mathbb{Z}_m$ generated by the element $\frac{m}{r}$. It can be written in the form

$$\left(\frac{m}{r}\right) = \left\{0, \frac{m}{r}, 2\frac{m}{r}, \dots, (r-1)\frac{m}{r}\right\}$$

and has an order r.

Lemma 4. (Diameter of a subgroup $\left(\frac{m}{r}\right)$ of $\mathbb{Z}_m$) *For any $r|m$ we have*

$$D\left(\left(\frac{m}{r}\right)\right) = \begin{cases} D(\mathbb{Z}_{2^k}) = 2^{k-1} & \text{if } m = 2^k \text{ for some } k \geq 1, \\ \lceil \frac{r-1}{2} \rceil \cdot \frac{m}{r} & \text{otherwise.} \end{cases}$$

Proof. First consider the case $m = 2^k$, $k \geq 1$. Any subgroup of the group $\mathbb{Z}_{2^k}$ is a cyclic group (2^{r-s}) for some $s \in \{0, 1, \dots, k\}$ with the generator 2^{r-s}. It is easy to see that any subgroup (2^{r-s}) contains the element $2^{k-1} \in \mathbb{Z}_{2^k}$. The Lee weight of this element is

$$w_L(2^{k-1}) = \min\{2^{k-1}, 2^k - 2^{k-1}\} = 2^{k-1}.$$

By the definition of the Lee weight we have

$$w_L(2^t) < w_L(2^{k-1})$$

for any $t \neq k - 1$. Then

$$D((2^{r-s})) = 2^{k-1} \text{ for any } s \text{ from } \{0, 1, \dots, k\}.$$

Let now m be any integer not equal to a power of 2 and let r be any integer such that $r|m$. By the definition of the subgroup $\left(\frac{m}{r}\right)$ we have

$$\left(\frac{m}{r}\right) = \left\{0, \frac{m}{r}, 2\frac{m}{r}, \ldots, (r-1)\frac{m}{r}\right\}$$

and the order of $\left(\frac{m}{r}\right)$ is $|\left(\frac{m}{r}\right)| = r$. Then we have $r-1$ non-zero elements in $\left(\frac{m}{r}\right)$ distinguished by pairs $i \cdot \frac{m}{r}$ and $(r-1-i)\frac{m}{r}$, such that $w_L(i \cdot \frac{m}{r}) = w_L((r-1-i)\frac{m}{r}) = i \cdot \frac{m}{r}$ for $i = 1, \ldots, \lfloor\frac{r-1}{2}\rfloor$. If r is even we have one maximal element $\lceil\frac{r-1}{2}\rceil \cdot \frac{m}{r}$ with $w_L(\lceil\frac{r-1}{2}\rceil \cdot \frac{m}{r}) = \lceil\frac{r-1}{2}\rceil \cdot \frac{m}{r}$. It is easy to see that $w_L(i \cdot \frac{m}{r}) < w_L(\lceil\frac{r-1}{2}\rceil \cdot \frac{m}{r})$ for any $i < \lceil\frac{r-1}{2}\rceil$ regardless of the parity of r. Therefore $D((\frac{m}{r})) = \lceil\frac{r-1}{2}\rceil \cdot \frac{m}{r}$.

Lemma 4 has the following useful consequences.

Corollary 1. *Let $r = 2l$ be even and $r|m$, then $D\left(\left(\frac{m}{r}\right)\right) = D(\mathbb{Z}_m) = \frac{m}{2}$.*

Corollary 2. *Let $r = 2l+1$ be odd and $r|m$, then $D\left(\left(\frac{m}{r}\right)\right) = \frac{l}{2l+1}m < \frac{m}{2}$.*

Corollary 3. *For any odd r or s such that $r|m$, $s|m$, and $s > r$ we have $D\left(\left(\frac{m}{s}\right)\right) > D\left(\left(\frac{m}{r}\right)\right)$.*

Remark 1. Like for the Hamming distance (see [1]) in the Lee case for $m = 2^k$ all subgroups of $\mathbb{Z}_m$ have the same diameter. This makes the approach via the transformation L introduced in [1] possible.

Lemma 5. *For any odd r and s such that $r|m$, $s|m$ and $s > r$ we have*

$$\frac{\log_2 s}{D\left(\left(\frac{m}{s}\right)\right)} > \frac{\log_2 r}{D\left(\left(\frac{m}{r}\right)\right)}. \tag{3.1}$$

Further, if r is even and the other relations hold again, the inequality also holds. In particular for $s = p^j$, $r = p^i$, $j > i$ it is true

$$\frac{j}{D((p^{k-j}))} > \frac{i}{D((p^{k-i}))}.$$

Proof. By Corollary 2 it suffices to show for any natural number l that

$$\frac{2l+1}{l}\log_2(2l+1) < \frac{2l+3}{l+1}\log_2(2l+3),$$

or that

$$(2l+1)^{\frac{2l+1}{l}} < (2l+3)^{\frac{2l+3}{l+1}},$$

or

$$(2l+1)^{2l^2+3l+1} < (2l+3)^{2l^2+3l},$$

which is equivalent to

$$(2l+1) < \left(\frac{2l+3}{2l+1}\right)^{2l^2+3l} = \left(1 + \frac{2}{2l+1}\right)^{2l^2+3l}.$$

Since $(1+a)^n > 1 + na$ sufficient is

$$1 + \frac{2(2l^2+3l)}{2l+1} > 1 + 2l,$$

or, equivalently, $4l^2 + 6l > 4l^2 + 2l$, which is true.

The final statement holds by Corollaries 1 and 2.

Remark 2. In summary, having again the relations $r|m$, $s|m$, and $s > r$, the inequality (3.1) can fail only for r odd and s even. Since in this case $D((\frac{m}{s})) = \frac{m}{2}$, the weakest counterexample could be for $r = 2l+1$ and $s = 2l+2$. Here we have to find l such that

$$\frac{\log_2(2l+2)}{\lceil \frac{2l+1}{2} \rceil \frac{m}{2l+2}} < \frac{\log_2(2l+1)}{\lceil \frac{2l}{2} \rceil \frac{m}{2l+1}}$$

or, equivalently, with

$$2l \log_2(2l+2) < (2l+1)\log_2(2l+1)$$

or with

$$\left(1 + \frac{1}{2l+1}\right)^{2l} < 1 + 2l.$$

Since the term to the left is smaller than e this holds for all $l = 1, 2, \ldots$.

On the other hand for $s = 2l' + 2$, $l' > l$ we have to check whether

$$2l \log_2(2l'+2) < (2l+1)\log_2(2l+1).$$

This fails for $l' \geq l'_0(l)$, suitable.

Remind that by $\mathcal{S}_0$ we denote a subset of $\mathbb{Z}_{2^k}$ containing 0.

Lemma 6. *If for any subgroup $\mathcal{U} < \mathbb{Z}_{2^k}^n$, $k \geq 1$, of diameter d it is true that $|\mathcal{S}_0| \geq 2$, then the transformation*

$$L : \bigcup_{\mathcal{S}} \mathcal{U}_{\mathcal{S}} \mathcal{S} \to \left(\bigcup_{\mathcal{S}} \mathcal{U}_{\mathcal{S}} \right) \mathbb{Z}_{2^k}$$

results in a group of diameter not more than d and not decreased cardinality.

Proof. First we show that the transformation L does not decrease the cardinality. Consider the decomposition (2.2). Every u^{n-1} occuring in some $\mathcal{U}_{\mathcal{S}_0} + \alpha$ has multiplicity

$$|\mathcal{S}_0 + \psi(\alpha)| = |\mathcal{S}_0|$$

and gets by the transformation L the multiplicity $|\mathbb{Z}_{2^k}| \geq |\mathcal{S}_0|$. So the cardinality does not decrease.

Furthermore by (2.2) and Lemma 4 we have

$$D(\mathcal{U}_{\mathcal{S}_0}) = D(\mathcal{U}_{\mathcal{S}_0} + \alpha) \leq d - 2^{k-1}$$

and also

$$D(\mathcal{U}_{\mathcal{S}_0}+\alpha,\mathcal{U}_{\mathcal{S}_0}+\alpha')\leq d'-2^{k-1},$$

where $d'\leq d$.

Using the transformation L and Lemma 4 we get

$$D\left(\left(\bigcup_{\mathcal{S}}\mathcal{U}_{\mathcal{S}}\right)\cdot\mathbb{Z}_{2^k}\right)\leq d-2^{k-1}+2^{k-1}=d.$$

Hence the transformation L is appropriate, i.e. does not decrease the cardinality and does increase the diameter d.

Lemma 7. *If for any subgroup $\mathcal{U}<\mathbb{Z}_{2^k}^n$, $k\geq 1$ of diameter d it is true that $\mathcal{S}_0=\{0\}$, then there exist appropriate transformations of the group $\mathcal{U}$ into another subgroup of $\mathbb{Z}_{2^k}^n$ that do not decrease the cardinality and do not increase the diameter d.*

Proof. For $\mathcal{S}_0=\{0\}$ the decomposition (2.2) transforms into the decomposition

$$\mathcal{U}=\bigcup_{i\in\mathcal{U}_{(n)}}(\mathcal{U}_{\{0\}}+\varphi(i))i, \tag{3.2}$$

where $\mathcal{U}_{(n)}$ is from Definition 2. All cosets $\mathcal{U}_{\{0\}}+\varphi(i)$, $i\in\mathcal{U}_{(n)}$, are disjoint or equal.

We distinguish two cases.

Case 1: Since the set $\mathcal{U}_{\{0\}}$ by Lemma 2 is a subgroup for the case if there exist i,j, $i\neq j$, such that

$$\mathcal{U}_{\{0\}}+\varphi(i)=\mathcal{U}_{\{0\}}+\varphi(j),$$

then $\varphi(i)-\varphi(j)\in\mathcal{U}_{\mathcal{S}_0}$.

Case 1a: If $d_L(i,j)=2^{k-1}$ then

$$D(\mathcal{U}_{\{0\}}+\varphi(i))=D(\mathcal{U}_{\{0\}})=d-2^{k-1}.$$

In this case we use the transformation L, i.e. replace all i by $\mathbb{Z}_{2^k}$.

Case 1b: Let $d(i,j)=2^s<2^{k-1}$. W.l.o.g. we consider the case $\mathcal{U}_{\{0\}}=\mathcal{U}_{\{0\}}+\varphi(i)$, where $d(0,i)=2^s$. Since $\mathcal{U}_{(n)}$ is a subgroup in $\mathbb{Z}_{2^k}$ by Lemma 4 we have $D(\mathcal{U}_{(n)})=2^{k-1}$. Therefore we can find in $\mathcal{U}_{(n)}$ an element 2^{k-1}. Either $\mathcal{U}_{\{0\}}=\mathcal{U}_{\{0\}}+\varphi(2^{k-1})$ or $\mathcal{U}_{\{0\}}\neq\mathcal{U}_{\{0\}}+\varphi(2^{k-1})$ we have $D(\mathcal{U}_{\{0\}})=D(\mathcal{U}_{\{0\}}+\varphi(2^{k-1}))=d-2^{k-1}$.

In both cases we use the transformation L, i.e. replace $\mathcal{U}_{(n)}$ by $\mathbb{Z}_{2^k}$ (the smaller one we replace by $\mathbb{Z}_{2^k}$ not changing the diameter).

Case 2: If $\mathcal{U}_{\{0\}} + \varphi(i) \neq \mathcal{U}_{\{0\}} + \varphi(j)$ for any distinct i, j from $\{0, 1, \ldots, 2^k - 1\}$, then we replace all i by 0 and get the subgroup in $\mathbb{Z}_{2^k}^n$ with the same cardinality as the group $\mathcal{U}$ and the diameter does not increase.

¿From Lemmas 1-4, 6, and 7 we get

Theorem 1. *For any cyclic group $\mathbb{Z}_{2^k}$, $k \geq 1$, with respect to the Lee distance it holds*

$$A\mathbb{Z}_{2^k}^n(d) = |\mathbb{Z}_{2^k}|^{\min\left(n, \lfloor \frac{d}{2^{k-1}} \rfloor\right)} = 2^{k \min\left(n, \lfloor \frac{d}{2^{k-1}} \rfloor\right)}.$$

4 Optimal direct products of cyclic groups with specified Lee diameter

Let us consider maximal direct products of subgroups in $\mathbb{Z}_{p^k}$ with n factors and Lee diameter not exceeding d, $p > 2$. Recall that by Lemma 4

$$D\left(\left(\frac{p^k}{p^s}\right)\right) = D((p^{k-s})) = \lceil \frac{p^s - 1}{2} \rceil \cdot p^{k-s}$$

and write $F_{p^s} = (p^{k-s})$.

Clearly, for $k > s \geq t \geq 1$ it is true that $|F_{p^s}| \cdot |F_{p^t}| = |F_{p^{s+1}}| \cdot |F_{p^{t-1}}|$ and

$$D(F_{p^s}) + D(F_{p^t}) \geq D(F_{p^{s+1}}) + D(F_{p^{t-1}}), \tag{4.1}$$

because this is equivalent with

$$\lceil \frac{p^s - 1}{2} \rceil \frac{p^k}{p^s} + \lceil \frac{p^t - 1}{2} \rceil \frac{p^k}{p^t} \geq \lceil \frac{p^{s+1} - 1}{2} \rceil \frac{p^k}{p^{s+1}} + \lceil \frac{p^{t-1} - 1}{2} \rceil \frac{p^k}{p^{t-1}},$$

which is equivalent to

$$\frac{1}{2} - \frac{1}{2p^s} + \frac{1}{2} - \frac{1}{2p^t} \geq \frac{1}{2} - \frac{1}{2p^{s+1}} + \frac{1}{2} - \frac{1}{2p^{t-1}}$$

or to

$$\frac{1}{p^{s+1}} + \frac{1}{p^{t-1}} \geq \frac{1}{p^s} + \frac{1}{p^t}$$

or

$$p^{t-1} + p^{s+1} \geq p^t + p^s.$$

This is true, because $p^{s+1} > 2p^s > p^s + p^t$.

¿From (4.1) readily follows

Lemma 8. *For cardinality p^T, $T = ak + t$, $0 \leq t < k$, the group $\prod_1^a F_{p^k} \cdot F_{p^t}$ has the smallest diameter, namely*

$$D\left(\prod_1^a F_{p^k} \cdot F_{p^t}\right) = a\frac{p^k - 1}{2} + \frac{p^t - 1}{2}p^{k-t}.$$

This optimization problem can also be written as the following linear programming problem

$$\text{(a) } d \leq \sum_{t=1}^{k} a_t \cdot diam(\mathbb{Z}_{p^t})$$
$$\text{(b) } \max \left\{ \prod_{t=1}^{k} p^{a_t \cdot t} : \text{integers } a_1, a_2, \ldots, a_k \text{ satisfy (a)} \right\}$$
$$\text{or (c) } \max \left\{ \sum_{t=1}^{k} a_t \cdot t : \text{integers } a_1, a_2, \ldots, a_k \text{ satisfy (a)} \right\}.$$

The value of t is $f(t) = \frac{t}{diam(\mathbb{Z}_{p^t})}$, which can be seen with Lemma 5 to be monotonically increasing in t.

Therefore it is best to use $\mathbb{Z}_{p^k}$ as often as possible as factor in the subgroup, then $\mathbb{Z}_{p^{k-1}}$ as often as possible (under the constraint (a)) etc.

The result easily generalizes from $m = p^k, \quad F_{p^s}, \quad F_{p^t}, \quad s > t,$ to $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\mu^{\alpha_\mu}$, $F_S = F_{p_1^{\beta_1} p_2^{\beta_2} \cdots p_\mu^{\beta_\mu}}$, $F_T = F_{p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_\mu^{\gamma_\mu}}$, $S > T$. In the case there exists i such that $\beta_i < \alpha_i, \gamma_i \geq 1$ by taking p_i from T and adding it to S. Obviously for $S' = Sp_i$, and $T' = \frac{T}{p_i}$ we have $|F_S| \cdot |F_T| = |F_{S'}| \cdot |F_{T'}|$ and $D(F_S) + D(F_T) \geq D(F_{S'}) + D(F_{T'})$ because

$$\frac{\lceil \frac{S-1}{2} \rceil}{S} + \frac{\lceil \frac{T-1}{2} \rceil}{T} \geq \frac{\lceil \frac{S'-1}{2} \rceil}{S'} + \frac{\lceil \frac{T'-1}{2} \rceil}{T'}$$

holds, since it is true the inequality

$$\frac{1}{2} - \frac{1}{2S} + \frac{1}{2} - \frac{1}{2T} \geq \frac{1}{2} - \frac{1}{2S'} + \frac{1}{2} - \frac{1}{2T'}$$

as a consequence of $S' + T' \geq S + T$.

5 A diametric theorem in $\mathbb{Z}_{p^k}^n$ for homogeneous distance

According to [7] the homogeneous weight of $i \in \mathbb{Z}_{p^k}$ is given by

$$w_{hom}(i) = \begin{cases} 0 & \text{if } i = 0, \\ p-1 & \text{if } i \in \mathbb{Z}_{p^k} \setminus (p^{k-1}), \\ p & \text{if } i \in (p^{k-1}) \setminus \{0\}. \end{cases} \tag{5.1}$$

For $u = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}_{p^k}^n$, $w_{hom}(u) = \sum_{i=1}^{n} w_{hom}(u_i)$ and for $u, v \in \mathbb{Z}_{p^k}^n$ the homogeneous distance between u and v is $d_{hom}(u,v) = w_{hom}(u - v)$. The homogeneous diameter we define as

$$D_{hom}(\mathcal{U}) = \max_{u,v \in \mathcal{U}} d_{hom}(u,v)$$

and for any two sets $\mathcal{U}, \mathcal{V} \subset \mathbb{Z}_{p^k}^n$ the homogeneous cross-diameter is

$$D_{hom}(\mathcal{U}, \mathcal{V}) = \max_{u \in \mathcal{U}, v \in \mathcal{V}} d_{hom}(u, v).$$

Lemma 4′. (Homogeneous diameter of a subgroup of $\mathbb{Z}_{p^k}$) *For any integer $i \in \{1, 2, \ldots, k-1\}$ we have $D_{hom}((p^i)) = D_{hom}(\mathbb{Z}_{p^k}) = p$, where $(p^i) = \{0, p^i, 2p^i, \ldots, (p^{k-i}-1)p^i\}$ has p^{k-i} elements.*

Proof. Since $p^{k-i-1} \leq p^{k-i} - 1$ and $p^{k-i-1}p^i = p^{k-1}$ we have $p^{k-1} \in (p^i)$ for any $i \in \{1, 2, \ldots, k-1\}$. Therefore by (5.1)

$$p = D_{hom}((p^i)) \leq D_{hom}(\mathbb{Z}_{p^k}) = p.$$

It is easy to see that both Lemmas 6 and 7 have corresponding Lemmas 6′ and 7′, we just have to replace in the proofs 2^{k-1} by p and note that a subgroup $\mathcal{U} < \mathbb{Z}_{p^k}$ is of the form (p^i) for some i.

Using this and Lemma 4′ we get for

$$A'\mathbb{Z}_{p^k}^n(d) = \max\{|\mathcal{U}| : \mathcal{U} < \mathbb{Z}_{p^k}^n \text{ with } D_{hom}(\mathcal{U}) \leq d\} \text{ the following}$$

Theorem 2. *For any cyclic group $\mathbb{Z}_{p^k}$, $k \geq 1$, it is true $A'\mathbb{Z}_{p^k}^n(d) = p^{k \min\left(n, \lfloor \frac{d}{p} \rfloor\right)}$.*

6 A diametric theorem in $\mathbb{Z}_m^n$, $m = 4l$, for Krotov-type distance

For the cyclic group $\mathbb{Z}_m$ the Krotov-type weight $w_K : \mathbb{Z}_m \to \mathbb{R}^+$ is defined by

$$w_K(i) = \begin{cases} 0 & \text{if } i = 0, \\ 1 & \text{if } i \text{ is odd}, \\ 2 & \text{otherwise} \end{cases} \tag{6.1}$$

(see also [13]). For any word $u = (u_1, u_2, \ldots, u_n)$ from $\mathbb{Z}_m^n$ we define the Krotov-type weight $w_K(u) = \sum_{i=1}^{k} w_K(u_i)$, distance $d_K(u, v) = w_K(u - v)$, diameter $D_K(\mathcal{U})$, and cross-diameter $D_K(\mathcal{U}, \mathcal{V})$.

As analog to Lemma 4 we get

Lemma 4″. (Diameter of a subgroup of $\mathbb{Z}_m$ for Krotov-type distance) *For any non-trivial $\mathcal{U} < \mathbb{Z}_m$, $m \geq 2$, we have*

$$D_K\left(\left(\frac{m}{s}\right)\right) = \begin{cases} 1 & \text{if } s = 2 \text{ and } \frac{m}{2} \text{ is odd}, \\ 2 & \text{otherwise}. \end{cases}$$

The proof easily follows from (6.1) and the fact that any subgroup $(\frac{m}{s})$ has an even element with the one exception if $s = 2$ and $\frac{m}{2}$ is odd. Lemmas 6″, 7″, the analogs to Lemmas 6, 7, are valid for the case $4|m$. Using these facts and Lemma 4″ we get

Theorem 3. *For any cyclic group $\mathbb{Z}_m$ with $4|m$ with respect to the Krotov-type distance it is true* $A''\mathbb{Z}_m^n(d) = m^{\min\left(n, \frac{d}{2}\right)}$.

References

1. Ahlswede, R.: Another diametric theorem in Hamming spaces: optimal group anticodes. Proc. IEEE Information Theory Workshop, Punta del Este, Uruguay, March 13-17, 212-216 (2006)
2. Ahlswede, R., Katona, G.: Contributions to the geometry of Hamming spaces. Discrete Mathematics 17, 1-22 (1977)
3. Ahlswede, R., Khachatrian, L.: The complete intersection theorem for systems of finite sets. European J. Combinatorics 18, 125-136 (1997)
4. Ahlswede, R., Khachatrian, L.: The diametric theorem in Hamming spaces - optimal anticodes. Adv. Appl. Math. 20, 429-449 (1998).
5. Ahlswede, R., Khachatrian, L.: A pushing-pulling method: New proofs of intersection theorems. Combinatorica 19, 1-15 (1999)
6. Belov, B.I., Logachev, V.N., Sandimorov, V.P.: Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound. Problemy Peredachi Informatsii 10 (3), 36-44 (1974)
7. Constantinescu, I., Heise, W.: A metric for codes over residue class rings of integers. Probl. Inform. Transm. 33 (3), 208-213 (1997)
8. Farrell, P.G.: Linear binary anticodes. Electronics Letters 6, 419-421 (1970)
9. Katona, G.: Intersection theorems for systems of finite sets. Acta Math. Acad. Sci. Hung. 15, 329-337 (1964)
10. Kleitman, D.: On a combinatorial conjecture of Erdös. J. Combin. Theory 1, 209-214 (1966)
11. Krotov, D.S.: $\mathbb{Z}_4$-linear perfect codes. Diskr. Analiz Issled. Oper., Ser. 1, 7 (4), 78-90 (2000) (in Russian).
12. Krotov, D.S.: $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. Electronic Notes in Discrete Mathematics 6, 107-112 (2001)
13. Krotov, D.S.: On $\mathbb{Z}_{2^k}$-dual binary codes. IEEE Trans. Inform. Theory 53 (4), 1532-1537 (2007)
14. MacDonald, J.E.: Design for maximmum minimum-distance error-correcting codes. IBM J. Res. Develop. 4 (1), 43-57 (1960)
15. MacWilliams, F.J. Sloane, N.J.: The Theory of Error-Correcting Codes. Amsterdam-New York-Oxford: North-Holland (1977)
16. Solomon, G., Stiffler, I.I.: Algebraically punctured cyclic codes. Information and Control 8 (2), 170-179 (1965)
17. Venturini, D.: Construction of maximum linear binary codes in the case of large distances. Problems of Cybernetics, 16, 231-238 (1966) (in Russian).