Specification of all Maximal Subsets of the Hamming Space with Respect to Given Diameter *

Sergei L. Bezrukov

Abstract

We present a specification of all maximum subsets of the n-cube B^n with respect to a given diameter and show relations between this problem and the discrete isoperimetric problem. As a corollary, for any number m, $1 \leq m \leq 2^n$, we specify an m-element subset of B^n with minimal possible diameter. We also present a simple proof for a theorem of Katona on intersecting families [4].

1 Introduction

Denote by B^n the n-dimensional unit cube with Hamming metric $\rho(\alpha, \beta)$, $\alpha, \beta \in B^n$. For a fixed integer $d \in [0, n]$ consider the problem of constructing a maximum size subset $A \subseteq B^n$ such that $\rho(\alpha, \beta) \leq d$ for any $\alpha, \beta \in A$. We call such a subset A d-maximal. The number d is called the diameter of A and denoted by $D(A)$. Note that in continuous case the ball of radius $d/2$ has maximum area among all plane figures of diameter d. One of the d-maximal subsets of B^n is found in [1,2]. The main goal of this paper is to specify all d-maximal subsets of B^n. Throughout the paper we assume $d < n$. Denote by $S_r^n(\alpha)$ the ball of radius r centered in $\alpha \in B^n$.

Theorem 1

(i) *If $d = 2t$ then $S_t^n(\alpha)$ is a d-maximal set for any $\alpha \in B^n$;*

(ii) *If $d = 2t + 1$ then $S_t^n(\alpha) \bigcup S_t^n(\beta)$ is a d-maximal set for any $\alpha, \beta \in B^n$ such that $\rho(\alpha, \beta) = 1$.*

For $\alpha = (\alpha_1, \ldots, \alpha_n) \in B^n$ denote $\overline{\alpha} = (\overline{\alpha}_1, \ldots, \overline{\alpha}_n)$, the complementary vector of α. Partition B^n into 2^{n-1} pairs $(\alpha, \overline{\alpha})$ of complementary vectors and denote by $\mathcal{M}^n$ the collection of all 2^{n-1}-element subsets of B^n, obtained by choosing exactly one vector from each pair $(\alpha, \overline{\alpha})$.

*This paper is a translation from Russian of the author's article published in Problems of Information Transmission, v. XXIII (1987), No 1, 106–109.

Theorem 2

(i) If $d < n-1$ then there are no d-maximal subsets other then the ones described in Theorem 1;

(ii) If $d = n-1$ then $\mathcal{M}^n$ is the collection of all d-maximal subsets.

2 Proofs of the Theorems

Let $A \subseteq B^n$. Denote

$$\begin{aligned} G_t(A) &= \{\alpha \in B^n \setminus A \mid \rho(\alpha, A) \le t\}, \\ \overline{A} &= \{\alpha \in B^n \mid \alpha = \overline{\beta},\, \beta \in A\}. \end{aligned}$$

Lemma 1 *$D(A) \le d$ iff $A \bigcap (\overline{A} \cup G_{n-d-1}(\overline{A})) = \emptyset$.*

Proof.
Assume $D(A) \le d$ and $\alpha \in A$. Then $S^n_{n-d-1}(\overline{\alpha}) \cap A = \emptyset$, because for $\beta \in S^n_{n-d-1}(\overline{\alpha}) \cap A$ one has $d+1 \le \rho(\alpha, \beta) \le D(A)$. Note that

$$\overline{A} \cup G_{n-d-1}(\overline{A}) = \bigcup_{\alpha \in \overline{A}} S^n_{n-d-1}(\alpha),$$

which implies the necessity of the above condition.

To prove its sufficiency, assume $A \cap (\overline{A}) \cup G_{n-d-1}(\overline{A})) = \emptyset$. If $D(A) \ge d+1$, then there exist vectors $\alpha, \beta \in A$ such that $\rho(\alpha, \beta) \ge d+1$. Therefore, $\beta \in S^n_{n-d-1}(\alpha)$ and $A \cap (\overline{A} \bigcup G_{n-d-1}(\overline{A})) \ne \emptyset$. This contradiction completes the proof. $\square$

Corollary 1 *If $A \subseteq B^n$ is a d-maximal subset, then $2|A| + |G_{n-d-1}(A)| \le 2^n$.* $\square$

Denote by $I^n_t(m)$ the problem that consists in finding an m-element subset $A_0 \subseteq B^n$ such that $|G_t(A_0)| \le |G_t(A)|$ for any $A \subseteq B^n$, $|A| = m$. Denote $g(m,n,t) = |G_t(A_0)|$. We show that the function $f(m,n,t) = 2m + g(m,n,t)$ in non-decreasing in m for fixed n, t. Indeed, the inequality $f(m,n,t) < f(m+1,n,t)$ is equivalent to $g(m,n,t) \le 1 + g(m+1,n,t)$. On the other hand, if $C \subseteq B^n$ is a solution to $I^n_t(m+1)$ and $\alpha \in C$, then $g(m,n,t) \le |G_t(C \setminus \alpha)| \le g(m+1,n,t) + 1$.

Proof of Theorem 1.

Assume $d = 2t$. It is known from [3] that $S^n_t(\alpha)$ is a solution to $I^n_s(m_0)$ for any $s = 1, \ldots, n$, where

$$m_0 = |S^n_t(\alpha)| = \sum_{i=0}^{t} \binom{n}{i}.$$

One has

$$2m_0 + g(m_0, n, n-d-1) = \sum_{i=0}^{t} \binom{n}{i} + \sum_{i=0}^{n-t-1} \binom{n}{i} = 2^n.$$

Let A be a d-maximal subset and $|A| = m$. By Corollary 1, $2m + |G_{n-d-1}(A)| \le 2^n$, hence $2m + g(m, n, n-d-1) \le 2^n$. Using the monotonicity of g and the equality $D(S_t^n(\alpha)) = d$ one gets $m = m_0$.

Now, assume $d = 2t+1$. It is known from [3] that $S_t^n(\alpha) \cup S_t^n(\beta)$ with $\rho(\alpha, \beta) = 1$ is a solution to $I_s^n(m_0)$ for any $s = 1, \dots, n$, where

$$m_0 = |S_t^n(\alpha) \cup S_t^n(\beta)| = \sum_{i=0}^{t} \binom{n}{i} + \binom{n-1}{t}.$$

Taking into account the equality $2m_0 + g(m_0, n, n-d-1) = 2^n$ and using the arguments above, one gets that if A is a d-maximal subset then $|A| = m_0$, which completes the proof of the Theorem. □

Corollary 2 *If A is a d-maximal subset, then A is a solution to $I_{n-d-1}^n(|A|)$.* □

Lemma 2 *Let $d < n-1$ and A is a d-maximal subset. Then A is a solution to $I_1^n(|A|)$.*

Proof.
It follows from the proof of Theorem 1, that $|A| + |\overline{A} \cup G_{n-d-1}(\overline{A})| = 2^n$. Since $A \cap (\overline{A} \cup G_{n-d-1}(\overline{A})) = \emptyset$ then

$$A = B^n \setminus (\overline{A} \cup G_{n-d-1}(\overline{A})).$$

Therefore, $|G_t(A)| = |G_{n-d-1}(\overline{A})| - |G_{n-d-2}(\overline{A})|$.

Let $d = 2t$. One has

$$\begin{aligned} |A| &= \sum_{i=0}^{t} \binom{n}{i}, \\ G_{n-d-1}(\overline{A})| &= 2^n - 2|A| = \sum_{i=1}^{n-d-1} \binom{n}{t+i}, \\ |G_{n-d-2}(\overline{A})| &\ge \sum_{i=1}^{n-d-2} \binom{n}{t+i}. \end{aligned}$$

This implies $|G_1(A)| \le \binom{n}{t+1}$, i.e. A is a solution to $I_1^n(|A|)$.

The proof of Lemma in the case $d = 2t+1 < n-1$ is similar. □

Proof of Theorem 2.

Let $A \subseteq B^n$ be a d-maximal subset. Denote by $I^n(m)$ the problem that consists in finding an m-element subset $A_0 \subseteq B^n$, such that $|\Gamma(A_0)| \le |\Gamma(A)|$ for any $A \subseteq B^n$, $|A| = m$, where

$$\Gamma(A) = \{\alpha \in A \mid S_1^n(\alpha) \not\subseteq A\}.$$

Since $G_1(A) = \Gamma(B^n \setminus A)$, the set of solutions to $I^n(m)$ can be obtained from the one for $I_1^n(2^n - m)$ and vise versa. In particular, denoting $C = B^n \setminus A$, we get by Lemma 2 that C is a solution to $I^n(2^n - |A|)$.

Assume $d = 2t < n - 1$. Denote

$$m_1 = |A| = \sum_{i=0}^{t} \binom{n}{i}, \quad m_2 = |C| = \sum_{i=0}^{n-t-1} \binom{n}{i}.$$

It is proved in [3] (Theorem 6.1), that $S_{n-t-1}^n(\alpha)$ is the only solution to $I^n(m_2)$ up to the choice of $\alpha \in B^n$. Hence, $S_t^n(\overline{\alpha})$ is the only solution to $I_1^n(m_1)$. Therefore, $A = S_t^n(\overline{\alpha})$.

Assume $d = 2t + 1 < n - 1$. Denote

$$m_3 = |A| = \sum_{i=0}^{t} \binom{n}{i} + \binom{n-1}{i}, \quad m_4 = |C| = \sum_{i=0}^{n-t-2} \binom{n}{i} + \binom{n-1}{t+1}.$$

It is proved in [3] (Lemma 6.1) that there exists a coordinate x_j, $1 \le j \le n$, such that $C^0(j) = S_{n-t-2}^{n-1}(\alpha')$ and $C^1(j) = S_{n-t-2}^{n-1}(\beta')$, where $C^0(j)$ and $C^1(j)$ are the intersections of the set C with the hyperplanes $x_j = 0$ and $x_j = 1$ respectively. Here α' and β' are projections of resp. α and β to the correspondent hyperplanes. By Theorem 6.2 of [3], we have $\rho(\alpha, \beta) \le 2$. It is not difficult to show that if $\rho(\alpha, \beta) = 2$, then $D(A) > d$. This implies, $\rho(\alpha, \beta) = 1$, i.e the vectors α, β differ in the j-th entry only. Furthermore,

$$C = S_{n-t-2}^{n-1}(\alpha) \cup S_{n-t-2}^{n-1}(\beta) = S_{n-t-2}^{n}(\alpha) \cup S_{n-t-2}^{n}(\beta).$$

Therefore $A = S_t^n(\overline{\alpha}) \cup S_t^n(\overline{\beta})$.

The proof in the case $d = n - 1$ follows from Lemma 1. □

3 Applications of the Theorems

1. Consider the problem of constructing an m-element subset of B^n with minimal possible diameter. Represent the integer m in the form

$$m = \sum_{i=0}^{k} \binom{n}{i} + \delta, \quad 0 < \delta \le \binom{n}{k+1}.$$

Obviously, $D(A) = n$ for any $A \subseteq B^n$, $|A| \ge 2^{n-1}$. If $m \le 2^{n-1}$ and $\binom{n-1}{k} < \delta \le \binom{n}{k+1}$, Theorem 1 implies $D(A) \ge 2k + 2$ for any $A \subseteq B^n$, $|A| = m$. However, such a subset A may be obtained by deleting arbitrary $\sum_{i=0}^{k+1} \binom{n}{t} - m$ vectors from a ball of radius $k + 1$. The argument in the case $m \le 2^{n-1}$ and $0 < \delta < \binom{n-1}{k}$ is similar.

2. Consider arbitrary n-element set and let $\mathcal{F}_l$ be a family of it's subsets such that $|F_i \cap F_j| \ge l > 1$ for any $F_i, F_j \in \mathcal{F}_l$, $i \ne j$. We call such a family, consisting of maximal possible number of subsets, the maximal one. A complete specification of the maximal families with $l > 1$ can be found in [4]. A solution to this problem can also be deduced Theorem 2.

For this note, that there is a natural correspondence between the vectors of the n-cube B^n and the subsets of n-element set and the Hamming distance between two vertices of the n-cube is equal to the size of the symmetric difference of the corresponding subsets.

If $F_i, F_j \in \mathcal{F}_l$, then $|F_i \Delta F_j| = |F_i \cup F_j| - |F_i \cap F_j| \leq n - l$. Therefore, if $n - l = 2t$ then $D(\mathcal{F}_l) \leq 2t$ and, by Theorem 1,

$$|\mathcal{F}_l| \leq \sum_{i=0}^{t} \binom{n}{i} = m_0.$$

On the other hand, the ball $S_t^n(\mathbf{1})$, where $\mathbf{1} = (1, \ldots, 1) \in B^n$, corresponds to some family $\mathcal{F}_l$. Hence, the size of any maximal family equals m_0. Similarly, if $n - l = 2t + 1$ is odd, then one can easily show that the diameter of any maximal family $\mathcal{F}_l$ is equal to $n - l$. Therefore, any maximal family corresponds to some $(n - l)$-maximal subset, i.e. for some $\alpha, \beta, \gamma \in B^n$ $\mathcal{F}_l = S_t^n(\alpha)$ for $n - l$ even and $\mathcal{F}_l = S_t^n(\beta) \cup S_t^n(\gamma)$ with $\rho(\beta, \gamma) = 1$ for $n - l$ odd. Furthermore, it is easy to verify that if $\alpha \neq \mathbf{1}$ and $\beta \neq \mathbf{1}$ (or $\gamma \neq \mathbf{1}$), then there always exist some $F_i, F_j \in \mathcal{F}_l$ such that $|F_i \cap F_j| < l$. Therefore if $n - l$ is even, then there exists the only maximal family and there are exactly n maximal families for $n - l$ is odd.

Note that for $l = 1$ the above statements are not valid. It is not difficult to show [5] that in this case for the number M of maximal families one has

$$\log_2 M \geq 0.5 \binom{n}{\lfloor n/2 \rfloor}, \quad \text{as } n \to \infty.$$

Following a conjecture in [5], $\log_2 M \sim 0.5 \binom{n}{\lfloor n/2 \rfloor}$ as $n \to \infty$.

References

[1] Kleitman D.J. *On a Combinatorial Conjecture of Erdős.* J. Combin. Theory, v.**1** (1966), No 2, 209–214.

[2] Ahlswede R., Katona G.O.H. *Contributions to the Geometry of Hamming Spaces.* Discrete Math., v.**17** (1977), No 1, 1–22.

[3] Aslanyan L.A. *The Isoperimetric Problem and Similar Problems for Discrete Spaces.* (in Russian) - Problems of Cybernetics, Moscow 1979, v.**36**, 85–127.

[4] Katona G.O.H. *Intersection Theorems for Systems of Finite Sets.* Acta Math. Acad. Sci. Hungar., v.**15** (1964), 329–337.

[5] Erdős P., Kleitman D.J. *Extremal Problems Among Subsets of a Set.* Discrete Math., v.**8** (1974), No 2, 281–294.