Open Journal of Discrete Mathematics, 2016, 6, 25-40
Published Online April 2016 in SciRes. http://www.scirp.org/journal/ojdm
http://dx.doi.org/10.4236/ojdm.2016.62004

Scientific Research Publishing

Algebra and Geometry of Sets in Boolean Space

Vladimir Leontiev[1], Garib Movsisyan[2], Zhirayr Margaryan[3]

[1]Moscow State University, Moscow, Russia
[2]BIT Group, Moscow, Russia
[3]Yerevan State University, Yerevan, Armenia
Email: vkleontiev@yandex.ru, garib@hkzap.ru, jiromr@mail.ru

Received 16 October 2015; accepted 28 March 2016; published 31 March 2016

Abstract

In the present paper, geometry of the Boolean space B^n in terms of Hausdorff distances between subsets and subset sums is investigated. The main results are the algebraic and analytical expressions for representing of classical figures in B^n and the functions of distances between them. In particular, equations in sets are considered and their interpretations in combinatory terms are given.

Keywords

Equations on Sets, Hausdorff Distance, Hamming Distance, Generating Function, Minkowski Sum, Sum of Sets

1. Distance between Subsets B^n

Let $B=\{0,1\}$, $B^n=\{0,1\}^n$ and B^n be the set of all words of finite length in the alphabet B. For $X,Y\in 2^{B^n}$ we take:

$$\rho(X,Y)=\min_{\substack{u\in X\\ v\in Y}}\rho(u,v).$$

It is clear that $\rho(X,Y)$ is the Hausdorff distance between the subsets X,Y and $0\le\rho(u,v)\le n$, and $\rho(u,v)=\|u+v\|$ is the Hamming distance between the points: $u=(u_1u_2\cdots u_n), v=(v_1v_2\cdots v_n)\in B^n$, where $u+v=((u_1\oplus v_1)(u_2\oplus v_2)\cdots(u_n\oplus v_n))$, and $\oplus$ is the addition operation with respect to mod 2.

The Hausdorff distance has essential role in many problems of discrete analysis [1] and thus has certain interest. On the other hand, there only are a few essential results concerning distances between the subsets B^n, and

How to cite this paper: Leontiev, V., Movsisyan, G. and Margaryan, Z. (2016) Algebra and Geometry of Sets in Boolean Space. *Open Journal of Discrete Mathematics*, **6**, 25-40. http://dx.doi.org/10.4236/ojdm.2016.62004

their investigation offers significant difficulties.

First, we present the following simple properties of the Hausdorff distance:

1) $\rho(X,Y)=\rho(Y,X)$;

2) $\rho(X,Y)=0 \rightleftarrows X \cap Y \neq \varnothing$;

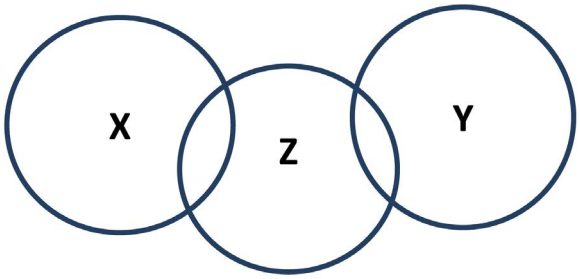
3) Если $X \subseteq X', Y \subseteq Y'$, то $\rho(X,Y)=\rho(X',Y')$;

4) $\rho(X,Y)=\rho(X+a,Y+a)$, for $a \in B^n$.

Let us note that, generally speaking, the Hausdorff distance does not satisfy the triangle inequality:

$$\rho(X,Y) \leq \rho(X,Z)+\rho(Z,Y), \tag{1}$$

which is demonstrated in the following picture:



But inequality (1) holds true if $|Z|=1$.

Distance between Spheres in B^n

Let $S_p^n(x)$ be a sphere of radius p with the center at $x \in B^n$. We take, for an arbitrary subset, $M \subseteq B^n$:

$$S_p^n(M)=\bigcup_{x \in M} S_p^n(x).$$

Thus, we have the following two equvalent interpretations for $S_p^n(M)$:

1) $S_p^n(M)$ is the set of all points in B^n which are at the distance $\leq p$ from the set M;

2) $S_p^n(M)$ is the set of all points in B^n, covered by the spheres of the radius p with the centers at points of the set M.

Examples.

1) $S_1^n\left(S_1^n(a)\right)=S_2^n(a)$, for an arbitrary point: $a \in B^n$;

2) $S_p^n\left(B^n\right)=B^n$, for an arbitrary $p \geq O$;

3) If $S_p^n(M)=B^n$ and $S_{p-1}^n(M) \neq B^n$, then p is the radius of the covering of the set B^n [2].

Theorem 1. $\rho\left(S_p^n(M_1), S_q^n(M_2)\right)=\max\{0, \rho(M_1,M_2)-p-q\}$.

Proof. We consider two cases.

a) $p+q>n$. Then,

$$S_p^n(M_1) \cap S_q^n(M_2) \neq \varnothing$$

and, consequently,

$$\rho\left(S_p^n(M_1), S_q^n(M_2)\right)=0.$$

b) $p+q \leq n$. Let $x \in S_p^n(M_1), y \in S_q^n(M_2)$. We present them in the form:

$$x=x_1+x_2, \text{ where } x_1 \in M_1, \|x_2\| \leq p;$$

$$y=y_1+y_2, \text{ where } y_1 \in M_2, \|y_2\| \leq q.$$

From here we have:

$$\rho(x,y)=\rho(x_1+x_2,y_1+y_2)=\|x_1+x_2+y_1+y_2\|.$$

As $\|x_1 + x_2 + y_1 + y_2\| \geq \|x_1 + y_1\| - \|x_2 + y_2\|$, consequently we have:

$$\min_{x_1 \in M_1, y_1 \in M_2} \|x_1 + x_2 + y_1 + y_2\| \geq \min_{x_1 \in M_1, y_1 \in M_2} \left(\|x_1 + y_1\| - \|x_2 + y_2\|\right)$$
$$= \min_{x_1 \in M_1, y_1 \in M_2} \|x_1 + y_1\| - \max_{x_2 \leq p, y_2 \leq q} \|x_2 + y_2\|.$$

Then, taking into account that:

$$\max_{\|x_2\| \leq p, \|y_2\| \leq q} \|x_2 + y_2\| = p + q,\ p + q \leq n,$$

we have:

$$\rho\left(S_p^n(M_1), S_q^n(M_2)\right) = \rho(M_1, M_2) - p - q.$$

The theorem is proved.

Let:

$$R(r_1, r_2) = \max_{\substack{|X| = r_1 \\ |Y| = r_2}} \rho(X, Y).$$

Taking into account that the sphere of the radius p with the center at $(00\cdots0)$ and the sphere of the radius q with the center at $(11\cdots1)$ contain, respectively, as many points as:

$$\sum_{t=0}^{p} \binom{n}{t} \text{ and } \sum_{t=q}^{n} \binom{n}{t},$$

we get the following corollary.

Corrollary. If $q > p$, then:

$$R\left(\sum_{t=0}^{p} \binom{n}{t}, \sum_{t=q}^{n} \binom{n}{t}\right) \geq q - p.$$

The value of the function $R(r_1, r_2)$ for definite values of r_1, r_2 was calculated in [1].

Theorem 2. *If* $q > p$, *then*:

$$R\left(\sum_{t=0}^{p} \binom{n}{t}, \sum_{t=q}^{n} \binom{n}{t}\right) = q - p.$$

The general form of the standard generating function for the distance between the subsets $X, Y \subseteq B^n$ has the following form:

$$F_{p,q}(z) = \sum_{\substack{|X| = p \\ |Y| = q}} z^{\rho(X,Y)}. \tag{2}$$

The summation in (2) is over all pairs of the subsets (X, Y) with $|X| = p, |Y| = q$.

Let us consider a few examples.

1) $p = q = 1$.

In this case, we have:

$$F_{1,1}(z) = \sum_{x,y \in B^n} z^{\rho(x,y)} = \sum_x \sum_y z^{\rho(x,y)} = \sum_x \sum_{k=0}^{n} \binom{n}{k} z^k = 2^n (1+z)^n.$$

Thus, $F_{1,1}(z) = 2^n (1+z)^n$, which is the well-known function of distribution of distances between the points in the space B^n with the metrics of Hamming.

2) $p = 1$, and q is an arbitrary positive integer which does not exeed 2^n.

In this case:

$$F_{1,q}(z) = \sum_{\substack{x \in B^n \\ |Y| = q}} z^{\rho(x,Y)} = \sum_x \sum_{|Y| = q} z^{\rho(x,Y)}. \tag{3}$$

As:

$$\rho(x,Y)=\rho(x+a,Y+a),$$

for arbitrary points $a,x\in B^n$ and any subset $Y\subseteq B^n$, then we get from (3):

$$F_{1,q}(z)=2^n\sum_{|Y|=q}z^{\rho(0,Y)}.$$

Then:

$$\rho(0,Y)=\min_x\{\rho(0,x)=\|x\|,x\in B^n\}. \tag{4}$$

Consequently, the distance between the zero point and an arbitrary subset *Y* equals the minimal weight of the points which are in *Y*.

Hence, $\rho(0,Y)\geq k$, if there are not points with $\|x\|\leq k-1$ in *Y*. The numbers of subsets *Y* with $|Y|=q$ and the condition $\rho(0,Y)\geq k$ are found by the following formula:

$$\lambda_q(k)=\binom{2^n-S_{k-1}^n}{q}, \tag{5}$$

where $S_r^n=\sum_{i=0}^{r}\binom{n}{i}$

where $S_r^n=\sum_{i=0}^{r}\binom{n}{i}$ is the cardinality of the sphere with the radius *r* in B^n.

From (5), we get the following statement:

Lemma1. *If* $\lambda^o(q,k)$ *is the number of the subsets of cardinality q* (*in* B^n) *having the distance k to the zero point, then*:

$$\lambda^o(q,k)=\lambda_q(k)-\lambda_q(k+1).$$

For $k=0:\lambda^o(q,0)=\binom{2^{n-1}}{q-1}$.

Theorem 3. *The following formula holds true*:

$$F_{1,q}(z)=2^n\binom{2^{n-1}}{q-1}+2^n\sum_{k=1}^{n}z^k\left[\binom{2^n-S_{k-1}^n}{q}-\binom{2^n-S_k^n}{q}\right]. \tag{6}$$

Proof. By definition:

$$F_{1,q}(z)=2^n\sum_{|Y|=q}z^{\rho(0,Y)}.$$

From this and Lemma 1, taking into account (3) and (4), we get:

$$F_{1,q}(z)=2^n\left[\binom{2^{n-1}}{q-1}+\sum_{Y}z^{\rho(0,Y)}\right]=2^n\binom{2^{n-1}}{q-1}+2^n\sum_{k=1}^{n}\lambda^o(q,k)z^k$$
$$=2^n\binom{2^{n-1}}{q-1}+2^n\sum_{k=1}^{n}z^k\left[\binom{2^n-S_{k-1}^n}{q}-\binom{2^n-S_k^n}{q}\right].$$

The theorem is proved.

If $\Phi_{1,p}(z)$ is the generating function of the random value $\xi=\rho(a,Y)$ uniformly distributed on the pairs (a,Y), where $|Y|=q$, then the following holds true.

Corollary 1. *The following formula holds true*:

$$\Phi_{1,p}(z)=q+\frac{1}{\binom{2^n}{q}}\sum_{k=1}^{n}z^k\left[\binom{2^n-S_{k-1}^n}{q}-\binom{2^n-S_k^n}{q}\right].$$

Corollary 2. *The following holds true*:

$$M\xi = \frac{1}{\binom{2^n}{q}} \sum_{k=1}^{q} k \left[\binom{2^n - S_{k-1}^n}{q} - \binom{2^n - S_k^n}{q} \right].$$

Corollary 3. *The formula for* $F_{1,1}(z)$ *follows from* (6).
Proof. From (6) we get for $p = 1$:

$$F_{1,1}(z) = 2^n + 2^n \sum_{k=1}^{n} z^k \left[\left(2^n - S_{k-1}^n\right) - \left(2^n - S_k^n\right) \right] = 2^n + 2^n \sum_{k=1}^{n} z^k \binom{n}{k} = 2^n (1+z)^n.$$

Corollary 4. *For* $q = 2$, *the following formula holds true*:

$$M\xi = \frac{n}{2} - \frac{\sqrt{n}}{\sqrt{\pi}} + 0(1).$$

Proof. By definition and from Corollary 2, we derive:

$$\phi_{2,1}^1(1) = M\xi = \frac{1}{\binom{2^n}{2}} \sum_{k=1}^{n} k \left[\binom{2^n - S_{k-1}^n}{2} - \binom{2^n - S_k^n}{2} \right]. \tag{7}$$

Transforming the terms in (7), we get:

$$M\xi = \frac{1}{2\binom{2^n}{2}} \sum_{k=1}^{n} k \binom{n}{k} \left[2^{n+1} - 2S_{k+1}^n - \binom{n}{k} - 1 \right]. \tag{8}$$

Then, using the following formulas:

$$\sum_{k=1}^{n} k \binom{n}{k} = n2^{n-1}, \sum_{k=1}^{n} k \binom{n}{k} S_{k-1}^n = n \sum_{k=1}^{n} \binom{n-1}{k-1} S_{k-1}^n,$$

$$\sum_{k=1}^{n} k \binom{n}{k}^2 = \frac{n}{2} \binom{2^n}{n}.$$

Let us "compress" the sum:

$$S = \sum_{k=1}^{n} \binom{n-1}{k-1} S_{k-1}^n.$$

By definition, we have:

$$\begin{aligned} S &= \sum_{k=1}^{n} \binom{n-1}{k-1} \sum_{r=0}^{k-1} \binom{n}{r} = \sum_{k=1}^{n} \binom{n-1}{k-1} \left(2^n - \sum_{r=k}^{n} \binom{n}{r} \right) = 2^n \sum_{k=1}^{n} \binom{n-1}{k-1} \sum_{k=1}^{n} \binom{n-1}{k-1} \sum_{r=k}^{n} \binom{n}{r} \\ &= 2^{n-1} \left(2^n - 1\right) - \sum_{k=1}^{n} \binom{n-1}{k-1} \sum_{r=k}^{n} \binom{n}{r} = 2^{n-1} 2^n - \sum_{k=1}^{n} \binom{n-1}{k-1} \sum_{r=k}^{n} \binom{n}{r} \\ &= 2^{2n-1} \sum_{k=1}^{n} \binom{n-1}{k-1} \sum_{r=k}^{n} \binom{n}{r}. \end{aligned}$$

Furthermore, if:

$$R = \sum_{k=1}^{n} \binom{n-1}{k-1} \sum_{r=k}^{n} \binom{n}{r},$$

then:

$$R=\sum_{k=1}^{n}\binom{n-1}{k-1}\sum_{r=k}^{n}\underset{u}{coef}\left\{(1+u)^n u^{-n+r-1}\right\}=\underset{u}{coef}\left\{\frac{(1+u)^n}{u^{n+1}}\sum_{k=1}^{n}\binom{n-1}{k-1}\sum_{r=k}^{n}u^r\right\}$$

$$=\underset{u}{coef}\left\{\frac{(1+u)^n}{u^{n+1}}\sum_{k=1}^{n}\binom{n-1}{k-1}\frac{u^k-u^{n+1}}{1-u}\right\}$$

$$=\underset{u}{coef}\left\{\frac{(1+u)^n}{u^{n+1}(1-u)}\sum_{k=1}^{n}\binom{n-1}{k-1}u^k\right\}-\underset{u}{coef}\left\{\frac{(1+u)^n}{(1-u)}\sum_{k=1}^{n}\binom{n-1}{k-1}\right\}.$$

Further:

$$coef\left\{\frac{(1+u)^n u}{u^{n+1}(1-u)}\sum_{k=1}^{n}\binom{n-1}{k-1}u^{k-1}\right\}=\underset{u}{coef}\left\{\frac{(1+u)^n}{u^n(1-u)}(1+u)^{n-1}\right\}$$

$$=\underset{u}{coef}\left\{\frac{(1+u)^{2n-1}}{u^{n+1}(1-u)}\right\}=\sum_{r=0}^{n}\binom{2n-1}{n-r}=\sum_{r=0}^{n}\binom{2n-1}{r}=2^{2n-2}$$

And:

$$\underset{u}{coef}\left\{\frac{(1+u)^n}{1-u}\sum_{k=1}^{n}\binom{n-1}{k-1}\right\}=0.$$

From here it follows that $R=2^{2n-2}$.
Then:

$$\sum_{k=1}^{n}k\binom{n}{k}\left[2^{n+1}-2S_{k-1}^{n}-\binom{n}{k}-1\right]$$

$$=2^{n+1}2^{n-1}n-2\sum_{k=1}^{n}k\binom{n}{k}S_{k-1}^{n}-\sum_{k=1}^{n}k\binom{n}{k}^2-\sum_{k=1}^{n}k\binom{n}{k}=n2^{2n}-2nS-\frac{n}{2}\binom{2n}{n}-n2^{n-1}$$

$$=n2^{2n}-2n\left\{\left(2^{2n-1}-2^n\right)-R\right\}-\frac{n}{2}\binom{2n}{n}-n2^{n-1}=n2^{n+1}-2nR-\frac{n}{2}\binom{2n}{n}-n2^{n-1}$$

$$=\frac{n}{2}2^{2n}-\frac{n}{2}\binom{2n}{n}+3n2^{n-1}.$$

Taking this and (8) into account, we get:

$$M\xi=\frac{n}{2}-\frac{\sqrt{n}}{\sqrt{\pi}}+0(1).$$

And the generating function:

$$F_{p,q}(z)=\sum_{\substack{|X|=p\\|Y|=q}}z^{\rho(X,Y)}$$

can be expressed by the following parameters:

2) if $M\subseteq B^n$, then the family of all subsets of cardinality p, having distances $\geq r$ from M is expressed as $\binom{B^n\setminus S_{r-1}^{n}(M)}{p}$. Indeed, $S_{r-1}^{n}(M)$ contains all the points of B^n, having distances $\leq r-1$ from the set M. Hence, the set $B^n\setminus S_{r-1}^{n}(M)$ does not contain such points; consequently, for an arbitrary subset $X\in\binom{B^n\setminus S_{r-1}^{n}(M)}{p}$, the expression $\rho(X,M)\geq r$ holds true.

The cardinality of this family is:

$$\left(\begin{matrix}\left|B^n \setminus S_{r-1}^n(M)\right| \\ p\end{matrix}\right)=\left(\begin{matrix}2^n-\left|S_{r-1}^n(M)\right| \\ p\end{matrix}\right).$$

2) The number of all m-element subsets having the distance r from M is:

$$\left(\begin{matrix}2^n-\left|S_{r-1}^n(M)\right| \\ p\end{matrix}\right)-\left(\begin{matrix}2^n-\left|S_r^n(M)\right| \\ p\end{matrix}\right).$$

Summarizing all the previous, we get the following statement.

Theorem 4. *The following expression is true*:

$$F_{p,q}(z)=\sum_{|Y|=q}\sum_{r=1}\left\{\left(\begin{matrix}2^n-\left|S_{r-1}^n(Y)\right| \\ p\end{matrix}\right)-\left(\begin{matrix}2^n-\left|S_r^n(Y)\right| \\ p\end{matrix}\right)\right\}z^r.$$

2. Sum of Sets in B^n

Let $X,Y\in B^n$; we take:

$$X+Y=\{u+v,u\in X,v\in Y\}$$

The operation "+" is defined in the family 2^{B^n} of all subsets of B^n, and (2^{B^n}, "+") is a monoid with the neutral element $0=0^n$ [3] [4].

Besides, the following inequality holds true:

$$\max\{|X|,|Y|\}\le|X+Y|\le|X||Y|.$$

Here both limits are reachable.

The properties of "+" are as follows:

1) $X+0=X$;
2) $X=Y\to X+u=Y+u$ for all $u\in B^n$;
3) $(X+Y)+Z=X+(Y+Z)$-associativity;
4) $X+Y=Y+X$-communacativity;
5) $(X\cup Y)+Z=(X+Z)\cup(Y+Z)$-distributivity;
6) $(X\cap Y)+Z=(X+Z)\cap(Y+Z)$;
7) $(X\setminus Y)+Z=(X+Z)\setminus(Y+Z)$.

Examples.

If X is a subspace in B^n, then:

1) $X+X=X$;
2) $X+Y=X$, if $Y\subseteq X$.

Let the following holds true:

$$\|X+Y\|=\min_{\substack{x\in X\\ y\in Y}}\|x+y\|.$$

Then $\rho(X,Y)=\|X+Y\|$.

Thus, there is certain analogy between the norm of the sum of points and the distance between those points, as well as between the norm of the sum of the sets and the distance between those sets.

In the general form, the following statement connecting the operations "∪" и+, is true:

$$(X\cup Y)+(U\cup V)=(X+U)\cup(X+V)\cup(Y+U)\cup(Y+V).$$

2.1. Sum of Facets in B^n and the Distance between Them

A facet or interval in B^n is the set of points $J=\{a\le x\le b\}$, where the partial order $x\le y$ is defined in the classic way [5] [6]:

$$x \le y \rightleftarrows x_i \le y_i, i = \overline{1,n}, \quad \text{for} \quad x = (x_1\ x_2 \cdots x_n), y = (y_1\ y_2 \ldots y_n).$$

Every interval J can be written in the form of a word of the length n, in the alphabet $A = \{0,1,c\}$, the letters of which are ordered linearly: $0 < 1 < c$.

Examples.

If $n = 4$ and $J = \{(0100) \le x \le (0111)\}$, then every point of J can be presented by the word $(01cc)$, which means the following: all the points which are obtained from the word $(01cc)$ by the substitution either 0 or 1 for a letter of the given word, are contained in the interval J. Consequently, the cardinality of the interval J is $2^2 = 4$, for the given case, *i.e.* $|J| = 4$. Hence, each interval J has its corresponding code word $\lambda(J)$ in the alphabet A. The number of letters c in the code $\lambda(J)$ is the dimension of the interval J, *i.e.* is $\dim J$. And the following formula is obvious:

$$|J| = 2^{\dim J}.$$

If the operation "*" is introduced on the alphabet A:

*	0	1	c
0	0	1	c
1	1	0	c
c	c	c	c

then the sum $J_1 + J_2$ of the intervals J_1 and J_2 is the Minkowski sum:

$$J_1 + J_2 = \{u + v, u \in J_1, v \in J_2\}.$$

Examples.

1) If $J_1 = \lambda(01c), J_2 = \lambda(100)$, then $\lambda(J_1 + J_2) = (11c)$, *i.e.* $J_1 + J_2 = \{(110),(111)\}$, which corresponds to the definition of the sum $J_1 + J_2$.

2) If $J_1 = \lambda(c\ c \cdots c)$, then $J_1 + J_2 = J_1 = B^n$ for every interval J_2.

The distance between the intervals J_1 and J_2, having the codes $\lambda(J_1)$ and $\lambda(J_2)$-taking into account the introduced definitions-are calculated in the following way.

Let $\lambda_1(J)$ be the number of occurrences of letter 1 in the code of the interval J.

Statement 1. $\rho(J_1, J_2) = \lambda_1(J_1 + J_2)$.

Thus, the distance between the intervals J_1 and J_2 is the number of occurrences of letter 1 in the code of their sum.

Examples.

1) Let $\lambda(J_1) = (011c1c), \lambda(J_2) = (11c0c0)$.

Then $\lambda(J_1 + J_2) = (10\ c\ c\ c\ c)$ and $\rho(J_1, J_2) = 1$.

Let $J_n^p = \{J_p\}$ be the family of all p-dimensional intervals of B^n. Then $|J_n^p| = \binom{n}{p} 2^{n-p}$.

Let us consider the direct product $J_n^p \times J_n^q$ and introduce uniform distribution on it with the generating function:

$$F_{p,q}(z) = \frac{1}{|J_n^p||J_n^q|} \sum_{J_n^p, J_n^q} z^{\rho(J_n^p, J_n^q)}.$$

Theorem 5. *The following formula is true*:

$$F_{p,q}(z) = \frac{1}{\binom{n}{p} 2^{n-p}} \frac{1}{2\pi i} \oint_{|u|=r} \frac{(u+2)^q (u+2+1)^{n-q}}{u^{p+1}} du,$$

where $r < 1$.

Let us consider the matrix $\|\alpha_{ij}\|$ the rows of which are the codes $\lambda(J_1), \lambda(J_2), \cdots, \lambda(J_m)$ of the intervals from the family $\{J_1, J_2, \cdots, J_m\}$.

Lemma 2. *The following expression is true*:

$$\sum_{i<j}\rho\left(J_i,J_j\right)=\sum_{i=1}^{n}k_i^0k_i^1,$$

where $k_i^0k_i^1$ *is the number of zeros and, respectively, units in the i-th column of the matrix* $\left\|\alpha_{ij}\right\|$.

Proof. According to the definition:

$$\sum_{i,j}\rho\left(J_i,J_j\right)=\sum_{i,j}\sum_{k=1}^{n}\delta_{i_j}^k, \tag{9}$$

where $\delta_{i_j}^k=\begin{cases}1, & \text{if } \alpha_i^k\neq\alpha_j^k \text{ and } \alpha_i^k\neq c,\alpha_j^k\neq c;\\ 0, & \text{otherwise,}\end{cases}$

and $\lambda\left(J_i\right)=\left(\alpha_i^1\ \alpha_i^2\cdots\alpha_i^n\right)$ is the code of the interval J_i.

It follows from (9):

$$\sum_{i,j}\rho\left(J_i,J_j\right)=\sum_{k=1}^{n}\sum_{i,j}\delta_{i_j}^k. \tag{10}$$

The internal sum in (10) equals the number of such pairs $\left(\alpha_i^k,\alpha_j^k\right)$ in which one of α_i^k-s is unit and the other is zero, *i.e.* is $k_i^1k_i^0$. The Lemma is proved.

Example.

1) Let $S(3)$ be the family of all edges in B^3. We consider the matrix of their codes:

$$\left\|\alpha_{ij}\right\|=\begin{Vmatrix}c&0&0\\c&0&1\\c&1&0\\c&1&1\\\vdots&\vdots&\vdots\\0&c&0\\0&c&1\\1&c&0\\1&c&1\\\vdots&\vdots&\vdots\\0&0&c\\0&1&c\\1&0&c\\1&1&c\end{Vmatrix}$$

The total number of the edges in B^3 is $\binom{n}{1}2^{n-1}/_{n=3}=12$. Each column of the matrix has the length 12, and all letters of the alphabet $\{0,1,c\}$ occur in equal number, 4 times. Therefore, $k_i^0=k_i^1=4$, $i=1,2,3$.

From here, we get:

$$\sum_{J_i,J_j\in S(3)}\rho\left(J_i,J_j\right)=\sum_{i=1}^{3}4\times4=48.$$

2) In the general form, if $S(n)$ is the family of all edges in B^n, each column contains 2^{n-1} letters *c* and $k_i^0=k_i^1=\dfrac{n2^{n-1}-2^{n-1}}{2}=(n-1)2^{n-2}$. From here, we get:

$$\sum_{J_i,J_j\in S(n)}\rho\left(J_i,J_j\right)=(n-1)^2\,2^{2n-4}n=(n-1)^2\,n2^{2n-4}. \tag{11}$$

Thus, the sum of the pairwise distances between the intervals in B^n is calculated by formula (11).

2.2. The Sum of Spheres in B^n

In the general form, the following statement holds true.

Lemma 3. *The following formula is true*:

$$S_p^n(M) = M + S_p^n(0).$$

Proof. By definition:

$$S_p^n(M) = \underset{x\in M}{U} S_p^n(x) = \underset{x\in M}{U}\left\{x + S_p^n(0)\right\} = M + S_p^n(0).$$

Thus, the above introduced parameter $S_p^n(M)$ of the setMis rather easily expressed in the terms of the operation "+".

Lemma4. $S_p^n\left(S_q^n(M)\right) = S_{p+q}^n(M)$ *if* $p+q \le n$.

Proof. If $v \in S_p^n\left(S_q^n(M)\right)$, then either v is at the distance $\le p$ from $S_q^n(M)$ or there is a point $a \in S_q^n(M)$ such that $\rho(v,a) \le p$.

Then, from $a \in S_q^n(M)$, it follows that $\rho(a,z) \le q$, for all $z \in M$.

From here we get:

$$\rho(v,z) \le \rho(v,a) + \rho(a,z) \le p+q$$

or:

$$v \in S_{p+q}^n(M).$$

Hence, $S_p^n\left(S_q^n(M)\right) \subseteq S_{p+q}^n(M)$.

And if $v \in S_{p+q}^n(M)$, then there is a point $z \in M$ such that $\rho(v,z) \le p+q$.

Hence, $\rho\left(v, S_q^n(z)\right) \le p$ and, consequently, $v \in S_p^n\left(S_q^n(M)\right)$, that is, $S_{p+q}^n(M) \subseteq S_p^n\left(S_q^n(M)\right)$, and the proof is completed.

Theorem 6. *The following expression is true*:

$$S_p^n(M_1) + S_q^n(M_2) = S_{p+q}^n(M_1 + M_2) \tag{12}$$

Proof. We have from Lemma 4:

$$S_{p+q}^n(M_1 + M_2) = S_p^n\left(S_q^n(M_1 + M_2)\right).$$

Then, we have from Lemma 3:

$$\begin{aligned} S_{p+q}^n(M_1 + M_2) &= S_p^n(0) + S_q^n(M_1 + M_2) = S_p^n(0) + S_q^n(0) + M_1 + M_2 \\ &= \left(S_p^n(0) + M_1\right) + \left(S_q^n(0) + M_2\right) = S_p^n(M_1) + S_q^n(M_2). \end{aligned}$$

And the proof is over.

Formula (12) defines the rule of "addition" for arbitrary spheres in the space B^n.

2.3. Sum of Layers in B^n

Let $B_p^n = \left\{x \in B^n, \|x\| = p\right\}$ be the *p*-th layer of the *n*-dimensional cube, or be the sphere of the radius *p* with the center at zero [7] [8].

According to definition, $B_p^n + B_q^n$ is the sum of the layers in B^n or it is the sum of the points with the weights *p* and *q*. As $\|x\| - \|y\| \le \|x+y\| \le \|x\| + \|y\|$, then all points from $\left(B_p^n + B_q^n\right)$ have weights from the interval $\{p-q, p+q\}$.

Then, the following statement is true.

Lemma 5. *The following expression holds true*:

$$\left(B_p^n + B_q^n\right) = \bigcup_{|p-q|+2r \le \min\{2n-(p+q),(p+q)\}} B_{a+2r}^n.$$

Proof. First, let us note the following.

If $x \in B_p^n + B_q^n$, and $\|x\| = m$, then $B_m^n \subseteq B_p^n + B_q^n$. Consequently, every layer B_r^n is invariant with respect to the operation of the symmetric group S_n and, for $g \in S_n$, we have:

$$g(x+y) = g(x) + g(y), \text{ where } x, y \in B^n.$$

In standard terms, the symmetric group S_n operates on B^n, and every layer is a transitive set or an orbit of action of the group S_n.

If $x \in B_p^n + B_q^n$, then $x = y + z$, where $y \in B_p^n, z \in B_q^n$. Therefore, for each permutation $g \in S_n$ we have: $g(x) = g(y+z) = g(y) + g(z)$, and we get:

$$\{g(x)\} \subseteq B_m^n \text{ и } B_m^n \subseteq B_p^n + B_q^n.$$

Taking this into account, to describe the set $B_p^n + B_q^n$, it is sufficient to describe only the weights of the points which are included into this sum. The minimal weight of these is $d = |p-q|$.

We discuss the following outline:

$$z = 111100$$

$$z_1 = 110000$$

$$z_2 = 011000$$

$$z_3 = 001100$$

$$z_4 = 000110$$

$$z_5 = 000011$$

$$\|z + z_1\| = 2, \|z + z_2\| = 2, \|z + z_3\| = 2, \|z + z_4\| = 4, \|z + z_5\| = 6.$$

Here $n = 6, p = 4, q = 2$ and the "block" of the first 2 units is shifted by a unit in each consecutive word. Thus, we get all weights: $\|z + z_i\| : 2, 4, 6$.

In the general case, the situation is absolutely analogous, and the weights are arranged as follows:

$$p-q,\ p-q+2,\ p-q+4, \cdots,$$

for $p \geq q$.

Here the condition for z holds true:

$$p - q + 2r \leq \min\{p+q, 2n - (p+q)\}.$$

Examples.

1) $B_1^n + B_1^n = B_0^n \cup B_2^n$;
2) $B_2^n + B_2^n = B_0^n \cup B_2^n \cup B_4^n$;
3) $B_2^n + B_3^n = B_1^n \cup B_3^n \cup B_5^n$.

Theorem 7. *The following expression is true*:

$$B_p^n + S_q^n(M) = S_{l_1}^n(M) \setminus S_{l_2}^n(M),$$

where $l_1 = \min(p+q, n), l_2 = \max(0, p-q) - 1$.

Proof. From Lemmas 3 and 5, we have:

$$B_p^n + S_q^n(M) = B_p^n + \bigcup_{i=0}^{q} B_i^n + M = \bigcup_{i=0}^{q} (B_p^n + B_i^n) + M$$

$$= \bigcup_{i=|p-q|}^{p+q} B_i^n + M = S_{p+q}^n(0) \setminus S_{|p-q|}^n(0) + M = S_{p+q}^n(M) \setminus S_{|p-q|}^n(M).$$

The proof is over.

2.4. Sum of Subspaces in B^n

As usual, let $L(X)$ be the subspace generated by the vectors from the set X, or be the space "worn" on X.

Statement 2. $L(X_1 + X_2) = L(X_1) + L(X_2)$,
and:

$$\dim L(X_1 + X_2) = \dim L(X_1) + \dim L(X_2) - \dim\left(L(X_1) \cap L(X_2)\right)$$

Statement 3. *Let* $X + X \subseteq L(X)$.
And if:

$$|X| > \frac{|L(X)|}{2}, \tag{13}$$

then the following equality is true:

$$X + X = L(X).$$

Proof. We assume the contrary, that is, $y \in L(X) \setminus (X + X)$.
Then, we have:

$$X + y \subseteq L(X) \text{ and } (X + y) \cap X = \varnothing.$$

Hence, $X \cup (X + y) \subseteq L(X)$. Consequently, $|X| + |X + y| \geq |L(X)|$. That is, $2|X| \leq |L(X)|$.
This contradicts the initial condition and the proof is over.
The following example shows that condition (12) is not necessary.
Example.
Let $X = \{(0000),(1000),(0100),(0010),(0001),(1111)\}$. Then $X + X = L(X)$, although
$|X| = 6 < \frac{16}{2} = 8$.

3. Equations in Sets

The "simplest" equation by sets is the following:

$$X + Y = A \tag{14}$$

where $X, Y, A \in 2^{B^n}$.
Equation (14) always has the trivial solution: $X = \{x\}, Y = A + x$, where $x \in B^n$.
The significance of Equation (14) is explained by the following circumstances.
1) The standard problems of covering and partitioning in the Boolean space B^n [6] can be formulated as problems of describing the set of solutions of Equation (14).
2) For certain additional conditions, the solution of Equation (14) forms a perfect pair (perfect code) in the additive channel of communication [9].
3) The set of all solutions of Equation (14) coincides with the class of equivalence of the additive channel of communication [3].
Examples.
1) If $A = B^n$, we can take $\left(S_p^n(0), S_p^n(0)\right), p > \frac{n}{2}$ as the solution (X, Y) for Equation (14).
2) If A is a subspace of B^n, then Equation (14) has the following solution: $X = A, Y \subseteq A$.
The following statements are true:
Statement 4. *If the equations* $X + Y = A, X + Y = C$ *are solvable, then the equation* $X + Y = A + C$ *also is solvable.*
Proof. Let the pairs $(X_0, Y_0), (X_1, Y_1)$ be the solutions of the equations $X + Y = A$ and $X + Y = C$, respectively. Then for the pairs $\left((X_0 + X_1), (Y_0 + Y_1)\right)$ we have
$(X_0 + X_1) + (Y_0 + Y_1) = (X_0 + Y_0) + (X_1 + Y_1) = A + C$, as was required to be proved.
Statement 5. *For* $|p - q| + 2r \leq \min\{p + q, n\}$, *the equation*:

$$X + Y = \bigcup_{r=0} B^n_{|p-q|+2r}$$

has the solution $X = B_p^n, Y = B_q^n$.

Statement 6. *For* $0 \le p \le n$ *and* $M \subseteq B^n$, *the equation* $X + Y = S_p^n(M)$ *has the following solution*:

$$X = S_{p_1}^n(M_1), Y = S_{p_2}^n(M_2),$$

where $p_1 + p_2 = p, M_1 + M_2 = M$.

Statement 7. *For* $0 \le p, q \le n, M \subseteq B^n$, *the equation* $X + Y = S_p^n(M) \setminus S_q^n(M)$ *has the following solution*:

$$X = B_{p_1}^n, Y = S_{p_2}^n(M), \text{ where } p = \min(n, p_1 + p_2), q = \max(0, p_1 - p_2) - 1.$$

Statement 8. *The sets of solutions* (X,Y) *of the equations* $X + Y = A$ *and* $(X + M_1) + (Y + M_2) = A + (M_1 + M_2)$ *coincide for all* $M_1, M_2 \subseteq B^n$.

Below, when discussing Equation (14), without violating generality, we may assume $0 \in X \bigcap Y \bigcap A$, if necessary.

Statement 9. *The equation* $X + X = A$ *has no solution for* $|A| > \frac{n(n+1)}{2}, A \setminus \{0\} \subseteq B_p^n$.

Proof. If $A \subseteq B_p^n$ and $X + X = A$, for $a, b \in X$ we have $a + b \in A$ and $\|a + b\| = p$ or $\rho(a,b) = p$. Thus, X is an equidistant code [2], therefore, $|X| \le n + 1$. Consequently:

$$|A| \le \frac{n(n+1)}{2}.$$

From here it follows that the equation $X + X = A$ has no solution for $|A| > \frac{n(n+1)}{2}$, if $A \setminus \{0\} \subseteq B_p^n$.

Statement 10. *The equation* $X + X = A$ (*in "facets", i.e. X, A are facets in* B^n) *is solvable iff the code of the interval A does not contain the letter* 1.

Let (X_0, Y_0) be a solution of the equation $X + X = A$. As the following equality:

$$(X_0 \cup Y_0) + (X_0 \cup Y_0) = A$$

holds iff:

$$(X_0 + X_0) \subseteq A \text{ и } (Y_0 + Y_0) \subseteq A,$$

then the following statement is true.

Statement 11. *If* (X_0, Y_0) *is a solution of the equation* $X + Y = A$, *then* $(X_0 \cup Y_0)$ *is a solution of the equation* $X + X = A$, *iff* $(X_0 + X_0) \subseteq A$ *and* $(Y_0 + Y_0) \subseteq A$.

Statement 12. *If A is a subspace from* B^n, *then every subset* $X \subseteq A, |X| > \frac{|A|}{2}$, *is a solution of the equation* $X + X = A$.

In an additive channel of communication [3] an equivalence class has a unique representation by transitive sets of certain "generating" channels. The problem is to order these transitive sets by cardinalities of "generating" channels.

Let $N(A) = \{(X,Y), X + Y = A\}$.

We introduce the following parameters:

$$m(A) = \min_{(X,Y) \in N(A)} |X \cup Y|, \quad \bar{m}(A) = \begin{cases} |A \cup \{0\}|, & \text{if } N(A) = \varnothing \\ \min\limits_{(X,X) \in N(A)} |X| \end{cases}.$$

Such definition of $\bar{m}(A)$ is justified, because it is not always that the equation $X + Y = A$ has tions (for instance, if $|A| = 3, |A| = 5$, or for $0 \notin A$), though the equation $X + Y = A$ always has a solution.

One can easily prove that:

$$m(A) \le \bar{m}(A) \le |A \cup \{0\}|. \tag{15}$$

Statement 13. *For the subspace* $A \subseteq B^n$, *the following is true*:

$$m(A) = \bar{m}(A).$$

Proof. It follows from (15) that it is sufficient to prove that the following equality is true:

$$m(A) \geq \bar{m}(A).$$

Let (X_0, Y_0) be a solution of the equation $X + Y = A$, for which:

$$m(A) = |X_0 \cup Y_0|. \tag{16}$$

On the other hand, it follows from Statement 11 that $(X_0 \cup Y_0)$ is a solution of the equation $X + X = A$ and, consequently, $|X_0 \cup Y_0| \geq \bar{m}(A)$. Taking this and (16) into account, we get:

$$m(A) \geq \bar{m}(A).$$

Theorem 8. *The following estimations are true*:

1) $m(A) \geq \left]\frac{1}{2}\left((8|A|-7)^{\frac{1}{2}}+1\right)\right[$, *for* $A \subseteq B^n$;

2) $m(A) \leq 2^{\left[\frac{k}{2}\right]} + 2^{\left]\frac{k}{2}\right[} - 2$, *for the subspace* $A \subseteq B^n$, *for* $\dim A = k \geq 3$.

Proof. We have:

$$A = X + Y \subseteq (X \cup Y) + (X \cup Y).$$

From this and definition of addition of sets we get:

$$|A| \leq \|(X \cup Y) + (X \cup Y)\| \leq \frac{m(A)(m(A)-1)}{2} + 1.$$

Consequently:

$$m(A) \geq \left]\frac{1}{2}\left((8|A|-7)^{\frac{1}{2}}+1\right)\right[.$$

To prove the 2nd estimation, we consider such subspaces $L_1, L_2 \subseteq A$ for which the following is true:

$$L_1 \cap L_2 = \{0\}, \dim L_1 = \left[\frac{k}{2}\right], \dim L_2 = \left]\frac{k}{2}\right[.$$

Let:

$$X = (L_1 \setminus a_1) \cup (L_2 \setminus a_2) \cup (a_1 + a_2),$$

where $a_1 \in L_1$, $a_2 \in L_2, a_1 \neq 0, a_2 \neq 0$.

Let us prove that $(X, X) \in N(A)$.

We have:

$$\begin{aligned} X + X &= ((L_1 \setminus a_1) \cup (L_2 \setminus a_2) \cup (a_1 + a_2)) + ((L_1 \setminus a_1) \cup (L_2 \setminus a_2) \cup (a_1 + a_2)) \\ &= ((L_1 \setminus a_1) + (L_1 \setminus a_1)) \cup ((L_2 \setminus a_2) + (L_1 \setminus a_1)) \cup ((a_1 + a_2) + L_1 \setminus a_1) \\ &\quad \cup (L_1 \setminus a_1 + L_2 \setminus_2) \cup ((L_2 \setminus a_2) + (L_2 \setminus a_2)) \cup ((a_1 + a_2) + (L_2 \setminus a_2)) \\ &\quad \cup ((L_1) a_1 + (a_1 + a_2)) \cup ((L_2) a_2 + (a_1 + a_2)) \cup \{0\} \\ &= ((L_1 \setminus a_1) + (L_1 \setminus a_1)) \cup ((L_2 \setminus a_2) + (L_2 \setminus a_2)) \cup ((L_1 \setminus a_1) + (L_2 \setminus a_2)) \\ &\quad \cup ((a_1 + a_2) + (L_1 \setminus a_1)) \cup ((a_1 + a_2) + (L_2 \setminus a_2)). \end{aligned}$$

As (Statement 12) $(L_1 \setminus a_1) + (L_1 \setminus a_1) = L_1, (L_2 \setminus a_2) + (L_2 \setminus a_2) = L_2$ we get:

$$X + X = L_1 \cup L_2 \cup L \setminus ((L_1 + a_2) \cup (L_2 + a_1)) \cup (a_1 + a_2) + (L_1 \setminus a_1)) \cup ((a_1 + a_2) + (L_2 \setminus a_2)).$$

Then, using:

$$(L_1 \setminus a_1) + (a_1 + a_2) = (L_1 + a_2) \setminus a_1; L_2 \setminus a_2 + (a_1 + a_2) = (L_2 + a_1) \setminus a_2,$$

we get:

$$X + X = L_1 \cup L_2 \cup \left(L \setminus \left(\left(L_1 + a_2\right) \cup \left(L_2 + a_1\right)\right) \cup \left(\left(L_1 + a_2\right) \setminus a_1\right) \cup \left(\left(L_2 + a_1\right) \setminus a_2\right) = A.$$

Hence, taking this and Statement 13 into account we get:

$$m(A) = \bar{m}(A) \le |X \cup X| = \left|\left(L_1 \cup L_2\right) \setminus \left(a_1 \cup a_2\right) \cup \left(a_1 + a_2\right)\right| = |L_1| + |L_2| - 3 + 1 = 2^{\left\lceil \frac{k}{2} \right\rceil} + 2^{\left\lceil \frac{k}{2} \right\rceil} - 2.$$

The statement is proved.

Examples.

1) $A = B^4$. We have:

$$m(A) = \bar{m}(A) = 6.$$

2) $A = B^5$. We have:

$$9 \le m(A) \le \bar{m}(A) \le 10,$$

but actually:

$$m(A) = \bar{m}(A) = 10.$$

3) $A = B^7$. We have:

$$17 \le m(A) \le \bar{m}(A) \le 22.$$

We consider the set:

$$X = \{0\,0\,0\,0\,0\,0\,0,\ 0\,0\,0\,0\,1\,0\,0,\ 0\,0\,0\,0\,1\,1\,0,\ 0\,0\,0\,1\,1\,0\,1,\ 0\,0\,1\,0\,0\,0\,1,\ 0\,0\,1\,0\,1\,1\,1,$$
$$0\,1\,0\,0\,0\,0\,0, 0\,1\,0\,0\,1\,0\,0,\ 0\,1\,1\,0\,1\,0\,0,\ 0\,1\,1\,0\,1\,0\,1,\ 0\,1\,1\,1\,0\,1\,1,\ 0\,1\,1\,1\,1\,0\,0,$$
$$0\,1\,1\,1\,1\,1\,0,\ 1\,0\,0\,0\,0\,1\,0,\ 1\,0\,0\,1\,1\,0\,1,\ 1\,0\,0\,1\,1\,1\,0,\ 1\,0\,1\,0\,0\,0\,0,\ 1\,0\,1\,1\,0\,1\,1,$$
$$1\,1\,0\,0\,1\,0\,1,\ 1\,1\,0\,1\,1\,0\,0\}.$$

We have: $X + X = B^7, u|X| = 20$. Hence, $m(A) \le \bar{m}(A) \le 20$.

4) $A_1 = \{0\,0\,0\,0\,0\,0,\ 1\,0\,0\,0\,0\,0,\ 0\,1\,0\,0\,0\,0,\ 0\,0\,1\,0\,0\,0,\ 0\,0\,0\,1\,0\,0,\ 0\,0\,0\,0\,1\,0,\ 0\,0\,0\,0\,0\,1\}$.

$A_2 = \{1\,0\,0\,0\,0\,0,\ 0\,1\,0\,0\,0\,0,\ 0\,0\,1\,0\,0\,0,\ 0\,0\,0\,1\,0\,0,\ 0\,0\,0\,0\,1\,0,\ 0\,0\,0\,0\,0\,1\}$.

We have:

$$6 \le m(A_1) \le 7 \quad \text{and} \quad 6 \le m(A_2) \le 7.$$

But actually $m(A_1) = m(A_2) = 7$.

Suggestion. *For each* $A \subseteq B^n$ *the following is true*:

$$m(A) \le 2^{\left\lceil \frac{k}{2} \right\rceil} + 2^{\left\lceil \frac{k}{2} \right\rceil} - 2, \quad \textit{where} \quad k = \dim L(A) \ge 3.$$

References

[1] Nigmatulin, R.G. (1991) Complexity of Boolean Functions. Moscow, Nauka, 240 (in Russian).

[2] McWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting Codes, Parts I and II. North-Holland Publishing Company, Amsterdam.

[3] Leontiev, V.K. (2001) Selected Problems of Combinatorial Analysis. Bauman Moscow State Technical University, Moscow, 2001 (in Russian).

[4] Leontiev, V.K. (2015) Combinatorics and Information. Moscow Institute of Physics and Technology (MIPT), Moscow, 2015 (in Russian).

[5] Leontiev, V.K., Movsisyan, G.L. and Osipyan, A.A. (2014) Classification of the Subsets B^n, and the Additive Channels. *Open Journal of Discrete Mathematics* (*OJDM*), **4**, 67-76.

[6] Leontiev, V.K., Movsisyan, G.L., Osipyan, A.A. and Margaryan, Zh.G. (2014) On the Matrix and Additive Communication Channels. *Journal of Information Security* (*JIS*), **5**, 178-191.

[7] Leontiev, V.K., Movsisyan, G.L. and Margaryan, Zh.G. (2012) Constant Weight Perfect and D-Representable Codes. *Proceedings of the Yerevan State University, Physical and Mathematical Sciences*, 16-19.

[8] Movsisyan, G.L. (1982) Perfect Codes in the Schemes Johnson. *Bulletin of MSY, Computing Mathematics and Cybernetics*, **1**, 64-69 (in Russian).

[9] Movsisyan, G.L. (2013) Dirichlet Regions and Perfect Codes in Additive Channel. *Open Journal of Discrete Mathematics* (*OJDM*), **3**, 137-142.