Journal of Information Security, 2016, 7, 232-244
Published Online July 2016 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2016.74019

Scientific Research Publishing

On Addition 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 11 May 2016; accepted 16 July 2016; published 19 July 2016

Abstract

In many problems of combinatory analysis, operations of addition of sets are used (sum, direct sum, direct product etc.). In the present paper, as well as in the preceding one [1], some properties of addition operation of sets (namely, Minkowski addition) in Boolean space B^n are presented. Also, sums and multisums of various "classical figures" as: sphere, layer, interval etc. are considered. The obtained results make possible to describe multisums by such characteristics of summands as: the sphere radius, weight of layer, dimension of interval etc. using the methods presented in [2], as well as possible solutions of the equation $X+Y=A$, where $X,Y,A\subseteq B^n$, are considered. In spite of simplicity of the statement of the problem, complexity of its solutions is obvious at once, when the connection of solutions with constructions of equidistant codes or existence the Hadamard matrices is apparent. The present paper submits certain results (statements) which are to be the ground for next investigations dealing with Minkowski summation operations of sets in Boolean space.

Keywords

Hadamard Matrices, Minkowski Addition, Multiset, Cardinality, Multisum, Interval, Quadrate, Boolean Space, Stabilizer, Additive Channel

1. Sum of Sets According to Minkowski

If $x=(x_1x_2\cdots x_n)$, $y=(y_1y_2\cdots y_n)$ are points in B^n, where B^n, is a Boolean space, then:

$$x+y=\big((x_1\oplus y_1)(x_2\oplus y_2)\cdots(x_n\oplus y_n)\big),$$

where $\oplus$ is the mod 2 addition operation.

This addition operation for members of B^n can be extended in subsets of B^n.

How to cite this paper: Leontiev, V., Movsisyan, G. and Margaryan, Z. (2016) On Addition of Sets in Boolean Space. *Journal of Information Security*, **7**, 232-244. http://dx.doi.org/10.4236/jis.2016.74019

In other words, if $X, Y \in 2^{B^n}$, then:

$$X + Y = \{x + y; x \in X, y \in Y\}. \quad (1)$$

Thus, the sum of subsets $X + Y$ is consisted of sums of points belonging to X and Y, respectively.

Examples.

1. if $X \in 2^{B^n}$, $y \in B^n$, then $\{X + y\}$ is the "shift" of the set X to the point y, and $|X + Y| = |X|$.
2. if X is a subset in B^n, then $X + X = X$.
3. $X + B^n = B^n$ for any $X \in 2^{B^n}$.

Also, $\{X + Y\}$ can be interprated as union of "shifts" of the sets X onto points of the sets Y.

The family $\left(2^{B^n}, +\right)$, with an introduced Minkowski addition operation "+" forms a monoid with the neutral element $\{0^n\}$, which is one member set having the zero element of B^n.

The following inequality is valid:

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

Both limits are achievable here. The following statements describe the sets in which these limits are achieved.

Definition [2]. *The pair* (X, Y) *is called additive if for any* $x_i, x_j \in X$ *and* $y_s, y_r \in Y$ *the following is valid*:

$$x_i + x_j \ne y_s + y_r.$$

Statement 1. *The upper limit is achieved if* $f(X, Y)$ *is an additive pair.*

Corollary. *If* $|X + Y| = |X| \cdot |Y|$, *then* $|X_0 + Y_0| = |X_0| \cdot |Y_0|$, *for all* $X_0 \subseteq X, Y_0 \subseteq Y$.

We consider an arbitrary subgroup $G \subseteq B^n$ and the action of this subgroup on the family 2^{B^n}:

$$gX = \{x + g, x \in X\},$$

where $g \in G$. Thus, G acts on 2^{B^n} with shifts transferring the subset into its "shift".

Definition [3]. *A stabilizer of the set X with respect to the group G is the union of "shifts"* G_X *from G, conserving X, i.e.* $gX = X$ *for all* $g \in G_X$.

Statement 2. *The lower limit is achieved if there exists* $z \in B^n$, *for which* $X + z \subseteq G_y$ *or* $Y + z \subseteq G_x$.

Corollary. *If* $|X + Y| = |X|$, *then* $|X + Z| = X$ *for all* $Z \subseteq Y$.

Now let $X \subseteq B^n$ and $X = \{v_1, v_2, \cdots, v_m\}$.

Example.

1. If $G = \{v, 0\}$ is a group of shifts, then for $X = \{v_1, v_2, \cdots, v_m\}$ the following is valid:

$$g_1 X = \{v_1 + v, v_2 + v, \cdots, v_m + v\}.$$

In this case X has a non-obvious stabilizer if all constituents of X can be partitioned into the pairs $(x, x + v)$, $x \in X$, *i.e.* $X = \{(v_i, v_i + v)\}$ with respect to $i = 1, 2, \cdots, m/2$. For $m = 4$ we get $X = \{(v_1, v_1 + v), (v_2, v_2 + v)\}$. It is clear that in this case $X + v = X$ and $v \in G_X$. Thus, all subsets of X, having a non-obvious stabilizers, are described above.

In the general form the stabilizer G_X for an arbitrary group G and an arbitrary set $X \subseteq B^n$ can be described in the following terms [3].

Statement 3. *The constituent* $g \in G_X$ *if the set X can be partitioned into the pairs* (v_i, v_j) *in such a way that* $v_i + v_j = g$ *for all pairs which are included in the partition.*

This statement can be obtained by analogical consideration for $G = B^n$ as in [4].

From the above statement one can construct the following algorithm for building the stabilizer G_X of an arbitrary set X for the subgroup $G \subseteq B^n$, acting on 2^{B^n}. And at same time $|X| = 2m$.

1. First we build the multiset $C = X + X$.
2. Then we choose all the pairs in C having the multiplicity m.
3. Then we build all partitions in A out of these pairs.
4. If $\{P_X\}$ is the set of all partitions of X having the same weights in pairs $x \in C$, then

$$G_X = \{x\} \cup \{0\}.$$

Example.

1. Let $G = B^4$. $X = \{v_1 = (0\,0\,1\,1), v_2 = (1\,0\,1\,0), v_3 = (1\,1\,1\,0), v_4 = (0\,1\,1\,1)\}$.

Then:

$$v_1 + v_2 = (1\,0\,0\,1), v_1 + v_3 = (1\,1\,0\,1), v_1 + v_4 = (0\,1\,0\,0),$$

$$v_3 + v_4 = (1\,0\,0\,1), v_2 + v_4 = (1\,1\,0\,1), v_2 + v_3 = (0\,1\,0\,0).$$

This means that all pairs $(v_1, v_2), (v_3, v_4), (v_1, v_3), (v_2, v_4), (v_1, v_4), (v_2, v_3)$ have the multiplicity 2 in the sum $X + X$. Then we have:

$$X = \{v_1, v_2\} \cup \{v_3, v_4\} = \{v_1, v_3\} \cup \{v_2, v_4\} = \{v_1, v_4\} \cup \{v_2, v_3\}.$$

The sum of the pairs in each of the solutions is the same. Hence, the following set:

$$G_X = \{(v_1 + v_2), (v_1 + v_3), (v_1 + v_4), 0\} = \{(1\,0\,0\,1), (1\,1\,0\,1), (0\,1\,0\,0), (0\,0\,0\,0)\}$$

is a stabilizer for *X*.

Below we present the simple properties of the operation "+"—it is addition in the sense of Minkowski, as was mentioned above—which can be taken as properties of an algebraic system with basic set 2^{B^n} and those for operations of addition, union of sets, set intersection etc.

1. Assosiativity:

$$X + (Y + Z) = (X + Y) + Z$$

2. Commutativity:

$$X + Y = Y + X$$

3. Distributivity with respect to union:

$$(X \cup Y) + Z = (X + Z) \cup (Y + Z)$$

4. $\bigcup_{i=1}^{m} (X + Y_i) = X + \bigcup_{i=1}^{m} Y_i$.

There are finitely many other relations connecting constituents of the algebraic system described above.

1.1. Sum of Spheres in B^n

Let $\rho(x, y) = \|x + y\|$ be the Hamming distance between the points $x, y \in B^n$ and $S_t(v)$ be the set of the points of the sphere of the radius *t* with the centre at the point $v \in B^n$. In other words, $S_t(v)$ is the sphere of the radius *t* having the point *v* as its centre. And at that, $S_n(v) = B^n$ for all $a \in B^n$.

Statement 4 [1]**.**

$$S_t(v) = S_t(0) + v. \tag{2}$$

Statement 5.

$$\overline{S}_t(v) = S_{n-(t+1)}(\overline{v}) \text{ for } t \le n-1$$

Here $\overline{S}_t(v)$ is the set complement of the sphere $S_t(v)$ in B^n and $\overline{v}$ is the logic "negation" of the binary set *v*. We assume that $S_t(v) = \varnothing$, for $t < 0$.

Proof. Let us note that if $x \in \overline{S}_t(v)$, then $\rho(x, v) \ge t + 1$. As:

$$\rho(x, v) \ge \rho(x, \overline{v}) = n,$$

then for $x \in \overline{S}_t(v)$ we have:

$$\rho(x, \overline{v}) = n - \rho(x, v) \le n - (t + 1),$$

or:

$$x \in S_{n-(t+1)}(\overline{v}) \text{ for } t \le n-1.$$

and if $t = n$, then $\overline{S}_t(a) = \varnothing$.

Example.

1. We consider the sphere $S_1(0)$. Then $\overline{S}_1(0) = S_{n-2}(11\cdots1)$.

Formula (2) in the preceding statement allows the following generalization connected with addition.

Let $M \in 2^{B^n}$ and $S_p(M)$ be the set of points belonging to the union of spheres of the radii p with the centres at the points M, that is:

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

$S_p(M)$ is the "generalized" sphere of the radius p having its centre at the point M.

Statement 6 [1]. *The following presentation is valid*:

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

Corollary. *For* $M_1, M_2 \subseteq B^n$ *the following take place*:

1. $S_p(M_1 + M_2) = S_p(M_1) + M_2 = S_p(M_2) + M_1 = S_p(0) + M_1 + M_2$.
2. $S_p(S_g(M_1)) = S_{p+g}(M_1)$.

Statement7 [1]. *The following relation is valid*:

$$S_p(M_1) + S_g(M_2) = S_{p+g}(M_1 + M_2)$$

for $p + g \le n$;
and the next one is valid:

$$S_p(M_1) + S_g(M_2) = B^n$$

for $p + g \ge n$.

Corollary. *For* $M_1, M_2 \subseteq B^n$ *the following is valid*:

$$S_p(M_1) + S_g(M_2) = M_1 + M_2 + S_{p+g}(0)$$

1.2. The Sum of Facets in B^n

A facet, or sub-cube, or interval in B^n is the set of points satisfying the following condition [5] [6]:

$$J = \{u \le x \le v\},$$

where ($\le$) is a coordinate-wise partial order relation in B^n:

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

In other words, an interval can be given by a word of the length n in the alphabet $\{0,1,c\}$, the letters of which are ordered linearly: $0 < 1 < c$.

Indeed, if:

$$J = \{\alpha_1\alpha_2\cdots\alpha_n \le x \le \beta_1\beta_2\cdots\beta_n\},$$

then the code $\lambda(J)$ of the interval J is built in the following way.

Let $\lambda(J) = (\lambda_1\lambda_2\cdots\lambda_n)$. Then:

$$\lambda_i = \begin{cases} \alpha_i = \beta_i, & \text{if } \alpha_i = \beta_i \\ c, & \text{if } \alpha_i < \beta_i \end{cases}$$

Examples.

1. If $J = \{0\,1\,0\,0 \le x \le 0\,1\,1\,1\}$, then $\lambda(J) = (0\,1\,c\,c)$.

2. If $J = B^n = \{0\,0\cdots0 \le x \le 1\,1\cdots1\}$, then $\lambda(B^n) = (c\,c\cdots c)$.

If $\lambda(J) = (\lambda_1\lambda_2\cdots\lambda_n)$ is the code of the interval J, then all points of the interval J are obtained from the code $\lambda(J)$ by replacing the letters in an arbitrary way by zeros or units.

Let $\lambda_1(J)$ and $\lambda_2(J)$ be the numbers of letters 1 and c, respectively included in $\lambda(J)$ which is the code of the interval J. it is clear that $\lambda_2(J)$ is the dimension of J, *i.e.* $\lambda_2(\lambda) = \dim J$ and $|J| = 2^{\dim J}$.

If the operation "$\star$" is introduced in the alphabet A by the following Caley table [7]:

$\star$	0	1	c
0	0	1	c
1	1	0	c
c	c	c	c

then the sum of the intervals J of the system defined above as a sum of subsets is the interval the code of which is calculated by the codes of items (addends) using the above Caley table.

Statement 7 [1]. *The sum* $J_1 + J_2$ *is an interval with the code* $\lambda(J_1 + J_2) = \lambda(J_1) + \lambda(J_2)$ *and dimension* $\lambda_2(J_1 + J_2) = \lambda_2(J_1) + \lambda_2(J_2) - \lambda_2(J_1 \cap J_2)$.

Examples.

1. If $J_1 = \{(0\,1\,0),(0\,1\,1)\}, J_2 = (1\,0\,0)$, then $\lambda(J_1 + J_2) = (1\,1\,c)$.

On the other hand, we get by definition:

$$J_1 + J_2 = \{(0\,1\,0) + (1\,0\,0),(0\,1\,1) + (1\,0\,0)\} = \{(1\,1\,0),(1\,1\,1)\},$$

i.e. $J_1 + J_2 = \{(1\,1\,c), c \in \{0,1\}\}$.

2. If $J_1 = B^n$, then $J_1 + J_2 = B^n$ for any interval J_2.

Statement 8 [1]. $\rho(J_1, J_2) = \lambda_1(J_1 + J_2)$, *where* ρ *is the Hausdorff distance between the sets* [8].

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

1.3. Sum of Layers in B^n

Let $B_p^n = \{x \in B^n, \|x\| = p\}$ be the p-th layer of an$n$-dimensional cube or sphere of the radius p and the centre at zero [9] [10].

By definition $B_p^n + B_q^n$ is the sum of layers in B^n, consisting of the union of sums of the points one of which has the weight $p$and the second has the weight q. It is clear that the symmetrical group S_n operates on each layer in the following manner:

if $g \in S_n$, then $g(x_1 x_2 \cdots x_n) = x_{g(1)} x_{g(2)} \cdots x_{g(n)}$.

Hence, g permutes the coordinates of the point$x$, leaving its Hamming weight unchanged.

At the same time the relation $g(x + y) = g(x) + g(y)$ is valid for $g \in S_n, x, y \in B^n$.

Thus, each layer B_p^n is a transitive set or an orbit of operation of the group S_n on the cube B^n.

Let $|p - g| = a$, $p + g = b$.

Statement 9 [1]. *The following formula is valid*:

$$B_p^n + B_q^n = \bigcup_{2r \le \min\{2n-b,b\}-a} B_{a+2r}^n \tag{3}$$

For not large values of the layer the following table of addition is valid:

$+$	B_0^n	B_1^n	B_2^n
B_0^n	B_0^n	B_1^n	B_2^n
B_1^n	B_1^n	$B_0^n \cup B_2^n$	$B_1^n \cup B_3^n$
B_2^n	B_2^n	$B_1^n \cup B_3^n$	$B_0^n \cup B_2^n \cup B_4^n$

Note that Formula (3) can be rewritten for any number of terms, using the above-mentioned property of distributivity.

Indeed, using (3), we get:

$$B_p^n + B_q^n + B_s^n = \bigcup_{2r \le \min\{2n-b,b\}-a} B_{a+2r}^n + B_s^n = \bigcup_{2r \le \min\{2n-b,b\}-a} \left(B_{a+2r}^n + B_s^n\right),$$

which makes possible to use (3) again.

Example.

1. Let us find the sum $B_1^n + B_2^n + B_4^n$. We have:

$$B_1^n + B_2^n + B_4^n = \left(B_1^n \cup B_3^n\right) + B_4^n = \left(B_1^n + B_4^n\right) \cup \left(B_3^n + B_4^n\right)$$
$$= \left(B_3^n + B_5^n\right) \cup \left(B_1^n \cup B_3^n \cup B_5^n \cup B_7^n\right) = B_1^n \cup B_3^n \cup B_5^n \cup B_7^n.$$

NB. As each layer B_p^n is a sphere of the radius p and the centre at zero point, then all the preceding formulae are rules of 'sphere' addition.

1.4. Sum of Subsets in B^n

If we take subspaces in B^n as terms of the sum $X+Y$, we will get a well-known object. Indeed, if X, Y is a subspace in B^n, then $(X+Y)$ is a subspace, too, and we have:

$$\dim(X+Y) = \dim X + \dim Y - \dim(X \cap Y),$$

in terms of cardinality:

$$|X+Y| = \frac{|X| \cdot |Y|}{|X \cap Y|}.$$

Thus, "theory of addition of subspaces" being a well-developed part of linear algebra, makes possible to answer many questions concerning the subject problem.

1.5. Sum of Spheres in B^n

The k-dimensional interval we denote by J^k.

According to statement 6, we have:

$$J^k + S_t^n(0) = \bigcup_{x \in J_k} S_t^n(x),$$

i.e. $J^k + S_t^n(0)$ is the union of all spheres of the radii t with centres at the points in the interval J_k, or:

$$J^k + S_t^n(0) = \bigcup_{x \in S_t^n(0)} \left(J^k + x\right).$$

Let $t_1 = \min(t, n-k)$.

Statement 10. $J^k + S_t^n(0) = S_{t_1}^{n-k}\left(J^k\right)$.

For the cardinality of the set $J^k + S_t^n(0)$ the following is true:

Corollary. $J^k + S_t^n(0) = 2^k S_{t_1}^{n-k}$, *where* $S_{t_1}^{n-k}$ *is the cardinality of the sphere of the radius* t_1 *in* B^{n-k}.

Proof. If $\lambda\left(J^k\right) = \left\{(cc\cdots c0\cdots 0)\right\}$, for any point the following is valid:

$$z = (\alpha_1\alpha_2\cdots\alpha_k, \beta_1\beta_2\cdots\beta_{n-k}) \in \bigcup_{x \in J^k} S_t^n(x),$$

if $\|\beta_1\cdots\beta_{n-k}\| \le t$. Indeed, in this case z belongs to the sphere of the radius t with the centre at $(\alpha_1\alpha_2\cdots\alpha_k, 0\cdots 0)$. Inversely, if $z = (\alpha_1\alpha_2\cdots\alpha_k, \beta_1\cdots\beta_{n-k})$ and $\|\beta_1\cdots\beta_{n-k}\| \ge t+1$, then $\rho(z,y) \ge t+1$ for any point y in the interval J^k, that is:

$$z \notin \bigcup_{x \in J^k} S_t^n(x).$$

Therefore, $\left|S_t^n(y) + J^k\right| = 2^k\left(1 + \binom{n-k}{1} + \cdots + \binom{n-k}{t_1}\right) = 2^k S_{t_1}^{n-k}$.

1.6. Sum of a Layer and an Interval in B^n

Analogous to the preceding statement and corollary we get the sum of the sets $B_t^n + J^k$.

Statement 11. *The following relation is valid*:

$$B_t^n + J^k = S_{t_1}^{n-k}\left(J^k\right) \setminus S_{p-k-1}^{n-k}\left(J^k\right).$$

Corollary. *The cardinality of the set* $B_t^n + J^k$ *is calculated as follows*:

$$\left|B_t^n + J^k\right| = 2^k\left(S_{t_1}^{n-k} - S_{p-k-1}^{n-k}\right).$$

1.7. Sum of a Sphere and a Layer in B^n

Statement 12. *The following is valid*:

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

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

Proof. We have from statements 9 and 6:

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

$$= \bigcup_{i=\max(0,p-q)}^{\min(p+q,n)} B_i^n + M = S_{l_1}^n(0) \setminus S_{l_2}^n(0) + M = S_{l_1}^n(M) \setminus S_{l_2}^n(M).$$

Q.E.D.

2. Equation in Sets

Let $\left(2^{B^n} +\right)$ be the monoid of all subsets with operation of addition (1) in B^n as was defined above. This monoid is of certain interest both in classical discrete analysis [8] and for a number of problems connected with theory of information [4].

The 'simplest' equation in sets is as follows:

$$X + Y = A \tag{4}$$

where $X, Y, A \in 2^{B^n}$.

It is clear that Equation (4) always has the trivial solution $X = \{0\}, Y = A$.

Examples.

1. If $A = B^n$, then one can choose B^n for X, and any subset of B^n for Y.
2. If A is a subspace of B^n, then $A + A = A$ and, therefore, Equation (4) has the solution $X = Y = A$.
3. $\{(11)\} + \{(01),(10)\} = \{(10),(01)\}; \{(10)\} + \{(00),(01)\} = \{(10),(11)\}$.

Now, let:

$$\|X + Y\| = \min\{\|x\|, x \in X + Y\}.$$

Then $\rho(X,Y) = \|X + Y\|$; consequently, the Hausdorff distance between the sets X and Y:

$$\rho(X,Y) = \min_{\substack{x \in X \\ y \in Y}} \rho(x,y)$$

is expressed by the norm of the sum of these solutions.

On the other hand, if:

$$R(X,Y) = \{\rho(x,y); x \in X, y \in Y\},$$

then $R(X,Y)$ is the reciprocal spectrum of the distance between the points of the sets X and Y and:

$$R(X,X) = \{\|x + y\|, x \in X, y \in X\},$$

that is, $R(X,X) = R(X)$ is the spectrum of the distance between the points of the set X, or rather, the spectrum of X.

Thus, the set $X + X$ describes, to a considerable extent, the set of distances between the points of X or the spectrum of X.

In an additive channel of communication [4] the class of equivalence has one to one presentation by transitive sets of certain 'generating' channels. The problem is to order these transitive sets through cardinalities of 'generating' channels. We need the following numerical parameters, which depend on solutions of Equation (4) and

on the right hand side of A.

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

We introduce the following parameters:

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

$$M(A)=\max_{(X,Y)\in N(A)}|X\cup Y|,\quad \bar{M}(A)=\begin{cases}|A\cup\{0\}|, & \text{if } N(A)=\varnothing\\ \max\limits_{(X,X)\in N(A)}|X| & \end{cases}$$

Introduction of such definitions as $\bar{m}(A)$ and $\bar{M}(A)$ is explained by the fact that the equation $X+X=A$ can sometimes have no solution (for instance, for $|A|=3, |A|=5$; or for $0\notin A$), though the equation $X+X=A$ always has a solution.

Then, for the minimal and maximal cardinality set $X\cup Y$, where $(X,Y)\in N(A)$, we get respective boundary values, which make possible to narrow the region $N(A)$, *i.e.* the region of the set of solutions of Equation (4) (we shall see this below).

It is not hard to prove that:

$$m(A)\le\bar{m}(A)\le\bar{M}(A)\le|A\cup\{0\}|\le M(A). \tag{5}$$

As every solution (X,X) of the equation $X+X=A$ is a solution for (4), then we present the following useful statement which makes possible to obtain solutions of the equation $X+X=Y$ from solutions of the Equation (4), under certain limitations.

Statement 13. *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 14. *For the subspace* $A\subseteq B^n$ *the following is valid*:

(a) $m(A)=\bar{m}(A)$;

(b) $M(A)=\bar{M}(A)=2^{\dim A}$.

Proof. It follows from (5) that it is sufficient to prove for (a) that:

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

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

$$m(A)=|X_0\cup Y_0|. \tag{6}$$

On the other hand, it follows from Statement 13 that $(X_0\cup Y_0)$ is a solution of the equation $X+X=A$ and, consequently, $|X_0\cup Y_0|\ge\bar{m}(A)$. Taking into account this and (6), we get:

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

The proof for the case (b) is analogical.

Statement 15. *The following estimations are valid*:

1. $m(A)\le 2^{\left\lceil\frac{k}{2}\right\rceil}+2^{\left\lceil\frac{k}{2}\right\rceil}-2$, *for the subspaces* $A\subseteq B^n$, *for* $\dim A=k\ge 3$;
2. $m(A)\ge\left\rceil\frac{1}{2}\left(\left(8|A|-7\right)^{\frac{1}{2}}+1\right)\right[$, *for* $A\subseteq B^n$.
3. *If* $A\subseteq B^n$ *is a subspace, then equality in* $m(A)\ge\left\rceil\frac{1}{2}\left(\left(8|A|-7\right)^{\frac{1}{2}}+1\right)\right[$ *takes place if* $\dim A=1, 2$ *or* 4.

Proof. Items 1 and 2 of this statement were proved in [1], and we prove only item 3.

Necessity. We assume that:

$$m(A)=\left\rceil\frac{1}{2}\left(\left(8|A|-7\right)^{\frac{1}{2}}+1\right)\right[, \tag{7}$$

and that the pair (X_0, Y_0) is a solution for the equation $X + Y = A$.

It follows from (7) that:

$$m(A)(m(A)-1) = 2(2^k - 1), k = \dim A. \tag{8}$$

According to the statement, we have that the set $(X_0 \cup Y_0)$ is a solution for the equation $X + X = A$, as well. We consider a Boolean matrix $n \times m(A)$, having points from $(X_0 \cup Y_0)$ in its rows. We denote by k_i the number of units in the *i*-thcolumn of this matrix. As A is a subspace, then the following equality is true: $k_i(m(A) - k_i) = 2^{k-1}$, *i.e.* $k_i = 2^{s_i}$ and $m(A) - k_i = 2^{k-1-s_i}$. Consequently, $m(A) = 2^{s_i} + 2^{k-1-s_i}$. This and (8) give:

$$2^{2(k-1-s_i)} + 2^{2s_i} = 2^k + 2^{k-1-s_i} + 2^{s_i} - 2. \tag{9}$$

For $s_i \geq 2$ and $k - 1 - s_i \geq 2$ this equation has no solution for every *k*. Consequently, $s_i \leq 1$ or $k - 1 - s_i \leq 1$. Now it is easy to find the solution of Equation (9): $k = 1, 2$ or 4.

Sufficiency. Let $\{e_1, e_2, \cdots, e_k\}$ be the basis for the space A_k. We consider the following sets:

$$X_1 = \{0, e_1\} \subseteq A_1;$$

$$X_2 = \{0, e_1, e_2\} \subseteq A_2;$$

$$X_4 = \{0, e_1, e_2, e_3, e_4, e_1 + e_2 + e_3 + e_4\} \subseteq A_4.$$

As $|X_k| \geq m(A_k) \geq \left\lceil \frac{1}{2}\left(\left(8|A_k| - 7\right)^{\frac{1}{2}} + 1 \right) \right\rceil$, then for $k \in \{1, 2, 4\}$ we have:

$$|X_k| = m(A_k) = \left\lceil \frac{1}{2}\left(\left(8|A_k| - 7\right)^{\frac{1}{2}} + 1 \right) \right\rceil.$$

The statement is proved.

Examples.

1. The pair (X_0, Y_0), where $X_0 = Y_0 = S_t^n(0)$ is a solution of the equation: $X + Y = B^n \setminus \{1^n\}$, for $n = 2t + 1$.

2. The pair (X_1, Y_1), where $X_1 = S_t^n(0), Y_1 = S_t^n(0) \cup x, x \in B^n \setminus S_t^n(0)$ is a solution of the equation: $X + Y = B^n$, for $n = 2t + 1$.

If we keep to these examples, then we can assume that there exists some monotonous dependence of the function $m(A)$ on the cardinality *A*. But one can manage to find the possible connection between the right hand side of Equation (4) and the function $m(A)$ for the case if *A* is the halfspace.

Corollary. *For the halfspace* A_1, A_2 *the inequality* $\dim A_1 \geq \dim A_2$ *is valid if* $m(A_1) \geq m(A_2)$.

The "seemingly obvious" hypothesis that the upper limit of $m(A)$ is reached for all $k = \dim A$ is refuted by the following examples.

Examples.

1. Let $A = B^5$. In this case there is no solution of Equation (4), satisfying the condition: $|X| = 9$. Consequently, since for $k = 5$ the following is valid:

$$2^{\left\lceil \frac{k}{2} \right\rceil} + 2^{\left\lceil \frac{k}{2} \right\rceil} - 2 = 10 \geq m(A),$$

$m(A) = 10$, and the upper limit is reached in this example.

2. Let $A = B^7 \cdot X$ = {(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: $X + X = A, m(A) = 22 < 24 = 2^{\left\lceil \frac{k}{2} \right\rceil} + 2^{\left\lceil \frac{k}{2} \right\rceil} - 2$. Consequently, the upper limit is not reached in this example.

Statement 16 [11]. *If* $A \setminus \{0\} \subseteq B_k^n$, *then the solution of the equation* $X + X = A$ *is an equidistant code with a distance between any two points equal k, and* $\overline{M}(A) \leq n + 1$. *At the same time* $\overline{M}(A) = n + 1$ *if there*

exists a Hadamard matrix of the order $n+1$ [12].

Consequently, the problem of constructing of an equidistant code with the distance k having the minimal cardinality can be formulated in terms of solvability of the equation $X+X=A$.

Definition. *The set* $A \in 2^{B^n}$ *is called a quadrate if the following equation*:

$$X+X=A \tag{10}$$

is solvable.

It is clear that a quadrate always contains the zero point.

Example.

1. If A is a halfspace in B^n, then, as it was mentioned above, $A+A=A$ and, therefore, A is a quadrate. If $A\setminus\{0\}\subseteq B_{2r+1}^n$, $r\in\{0,1,\cdots\}$, then A is a quadrate if $|A|=2$, *i.e.* $A=\{0,x;x\in B_{2r+1}^n\}$.

The notion of 'quadrate' is connected with problems of equivalence of additive channels [4] where description of the class of equivalence is connected with finding of all solutions of the following equation:

$$X+X=A.$$

Let:

$$M(n,d)=\max_{N(A)\neq\varnothing}\left\{\bar{M}(A);A\setminus\{0\}\subseteq\bigcup_{i=d}^{n}B_i^n\right\}.$$

We denote by $A(n,d)$ the cardinality of the maximal code with the minimal distance d [6].

Statement 17. $M(n,d)=A(n,d)$.

From this and taking into account the known estimations $A(n,d)$ (the upper limit; see [6]) we get:

Statement18.*The following inequality is valid*:

$$M(n,d)\le\frac{2^n}{\sum_{i=0}^{t}\binom{n}{i}},\ t=\left]\frac{d-1}{2}\right[.$$

At the same time equality takes place if there exists a perfect code in B^n with the minimal distance d.

Consequently, the problem of constructing the code of maximal cardinality – in particular, a perfect code – is reduced to finding the solution of maximal cardinality for Equation (10) among all quadrates of the union of layers $B_d^n\cup B_{d+1}^n\cup\cdots\cup B_n^n$.

Statement 19 [1]. *If* A,B *is a quadrate, then* $(A+B)$ *is a quadrate too*.

Corollary. *The preceding statement is valid for any number of summands*.

Now let $GL_2(n)$ be a group of invertible matrices having components in the field $F_2=\{0,1\}$.

Definition. *The set of matrices* $G_A\subseteq GL_2(n)$ *is called stabilizer of the set* $A\in 2^{B^n}$ *if all matrices in* G_A *conserve* A, *i.e.* $gA=A$, *where* $g\in G_A$.

At the same time, if $A=\{v_1,v_2,\cdots,v_m\}$, *then* $gA=\{gv_1,gv_2,\cdots,gv_m\}$.

Statement 20. *Let* G_A *be a stabilizer of the set* $A\in 2^{B^n}$ *and* $G_A=\{g\}$. *Then the pair* X,gX *is the solution of the equation* $X+X=A$, *as well*.

3. Multisets

The second definition of addition of sets from 2^{B^n} is connected with multiplicity of containing each member into the sum $A+B$ [4].

Definition. *A multisum of two sets* $A,B\in 2^{B^n}$ *is called multiset*:

$$A+B=\{\alpha*(x+y),x\in A,y\in B\}, \tag{11}$$

in which each member $(x+y)$ is counted as many times as it comes in sum (11), and α is the multiplicity of the member $(x+y)$.

Examples.

1. If $A=\{(0\,1),(1\,0)\}\in 2^{B^2}$, then $A+A=\{2*(0\,0),2*(1\,1)\}$.

2. If $A_1=B_1^3=\{(0\,0\,1),(0\,1\,0),(1\,0\,0)\}$, $A_2=B_2^3=\{(1\,1\,0),(1\,0\,1),(0\,1\,1)\}$, then

$A_1 + A_2 = \{3*(1\,1\,1), 2*(1\,0\,0), 2*(0\,1\,0), 2*(0\,0\,1)\}$.

It is clear that by definition $|A_1 + A_2| = |A_1| \cdot |A_2|$, in which the cardinality of the multiset is the sum of the multiplicities of its members.

In particular, the following expression is valid:

$$\bigcup_{x \in B^n} \{C + x\} = |C| * B^n,$$

where C is an arbitrary subset in B^n and $|C|$ is the multiplicity of the constituent $y \in B^n$.

It follows from this that:

$$\left| \bigcup_{x \in B^n} \{C + a\} \right| = |C| \cdot 2^n.$$

Let $a = |g - p|, b = g + p$.

Statement 21. *For the multiset* $B_g^n + B_p^n$ *the following formula is valid*:

$$B_g^n + B_p^n = \bigcup_{2r \le \min\{2n-b,b\}-a} \alpha(a+2r) * B_{a+2r}^n, \tag{12}$$

where $\alpha(a+2r) = \binom{a+2r}{r}\binom{n-a-2r}{\min(g,p)-r}$ *is the multiplicity of the member of the multiset* $B_p^n + B_g^n$ *with the weight* $(a+2r)$.

Proof. Let z be any member of the multiset $B_p^n + B_g^n$. Since:

$|p-g| = a \le \|z\| \le \min(2n-b, b)$ and $\|z\| - a$ is an even number, then $\|z\|$ always is presentable in the form: $\|z\| = a + 2r, r \ge 0$.

We assume (without violating generality) that:

$x = (x_1 x_2), y = (y_1 y_2), z = (z_1 z_2)$, where $x_1 \in B_{a+r}^{a+2r}, y_1 \in B_r^{a+2r}, z_1 \in B_{a+2r}^{a+2r}$, $x_2, y_2 \in B_{\min(p,g)-r}^{n-a-2r}, z_2 \in B_0^{n-a-2r}$ and $\rho(x_1, y_1) = a + 2r$, $\rho(x_2, y_2) = 0$.

Hence, we have:

$$\left|\{(x_1, y_1); x_1 + y_1 = z_1\}\right| = \binom{a+2r}{r};$$

$$\left|\{(x_2, y_2); x_2 = y_2\}\right| = \binom{n-a-2r}{\min(p,g)-r},$$

that is:

$$\left|\{(x, y); x + y = z\}\right| = \binom{a+2r}{r}\binom{n-a-2r}{\min(p,g)-r}.$$

From this, taking into account Statement 9, we get Formula (12).

Corollary. *For* $g \le p \le n$ *we have*:

a) $\binom{n}{g}\binom{n}{p} = \sum_{2r=0}^{\min\{2n-b,b\}-a} \binom{n}{a+2r}\binom{a+2r}{r}\binom{n-a-2r}{g-r}$;

b) $\binom{n}{p}\binom{n}{g} = \sum_{i=1}^{n-p} \binom{n}{p-g+2i}\binom{p-g+2i}{i}\binom{n-p+g-2i}{g-i}$;

if $p + g \ge n$, *and*:

c) $\binom{n}{p}\binom{n}{g} = \sum_{i=0}^{g} \binom{n}{p-g+2i}\binom{p-g+2i}{i}\binom{n-p+g-2i}{g-i}$;

if $p + g \le n$.

Statement 22. *For the multiset* $S_t^n(v) + B_p^n$ *the following is valid*:

$$S_t^n(v)+B_p^n=\bigcup_{2r=\max x(0,p-t)-l}^{\min(p+t,n)}\alpha(l+2r)*\left(B_{l+2r}^n+v\right),$$

where $v\in B^n$; *and at the same time*:

$$\alpha(l+2r)=\sum_{i=0}^{t}\sum_{\substack{r\\ l=|i-p|}}\binom{l+2r}{r}\binom{n-l-2r}{\min(i,p)-r}$$

is the multiplicity of the members of $\left(B_{l+2r}^n+v\right)$.

Corollary. *For* $n\geq p,t\geq 0$ *the following is valid*:

a) $\binom{n}{p}\sum_{i=0}^{t}\binom{n}{i}=\sum_{i=0}^{\min(p,t)}\sum_{r=0}^{i}\binom{n}{p+r}\binom{p+r}{i}\binom{i}{r}+\sum_{i=p+1}^{t}\sum_{r=0}^{p}\binom{n}{i+r}\binom{i+r}{p}\binom{p}{r}$;

b) $\binom{n}{p}\binom{n}{g}=\sum_{i=0}^{g}\binom{n}{p+i}\binom{p+i}{g}\binom{g}{i}$.

Statement 23. *For the multiset* $S_{t_1}^n(v_1)+S_{t_2}^n(v_2)$ *the following equality is valid*:

$$S_{t_1}^n(v_1)+S_{t_2}^n(v_2)=\bigcup_{m=0}^{t_1+t_2}\alpha_m*\left(B_m^n+(v_1+v_2)\right),$$

where $v_1,v_2\in B^n$ *and at the same time*:

$$\alpha_m=\sum_{i=0}^{t_1}\binom{m}{i}\sum_{j=0}^{\min(t_1-i,t_2-m+i)}\binom{n-m}{j}$$

is the multiplicity of the members $x\in\left(B_m^n+(v_1+v_2)\right)$.

Corollary. *For* $n\geq t_1,t_2\geq 0$ *the following equality is valid*:

$$\sum_{i=0}^{t_1}\binom{n}{i}\sum_{j=0}^{t_2}\binom{n}{j}=\sum_{m=0}^{t_1+t_2}\binom{n}{m}\sum_{i=0}^{t_1}\binom{m}{i}\sum_{j=0}^{\min(t_1-i,t_2-m+i)}\binom{n-m}{j}$$

Statement 24. *For the multiset* $B_p^n+J^k$ *the following formula is valid*:

$$B_p^n+J^k=\bigcup_{x\in B^n}\alpha(x)*x,$$

where $\alpha(x)=\binom{k}{p-\lambda_1\left(J^k+x\right)}$ *is the multiplicity of* x.

Corollary. *For* $n\geq p\geq 0$ *the following is valid*:

$$\binom{n}{p}=\sum_{i=0}^{p}\binom{n-k}{i}\binom{k}{p-i}$$

Statement 25. *For the multiset* $S_t^n(v)+J^k$ *the following formula is valid*:

$$S_t^n(v)+J^k=\bigcup_{x\in B^n}\alpha(x)*(x+v),$$

where $v\in B^n$, *and at the same time*:

$$\alpha(x)=\sum_{i=0}^{t-\lambda_1\left(J^k+x\right)}\binom{k}{i}$$

is the multiplicity of $x+v$.

Corollary. *For* $n\geq k\geq 0,n\geq t\geq 0$ *the following is valid*:

$$\sum_{i=0}^{t}\binom{n}{i}=\sum_{i=0}^{t}\binom{n-k}{i}\sum_{j=0}^{t-i}\binom{k}{j}.$$

Statement 26. *For the multiset* $J^{k_1}+J^{k_2}$ *the following is valid*:

$$J^{k_1}+J^{k_2}=\alpha\left(J^{k_1},J^{k_2}\right)*J^{k_3},$$

where $k_3=k_1+k_2-\lambda_2\left(J^{k_1}\cap J^{k_2}\right)$, J^{k_3} *is the interval with the code*: $\lambda\left(J^{k_1}+J^{k_2}\right)$, *and* $\alpha\left(J^{k_1},J^{k_2}\right)=\lambda_2\left(J^{k_1}\cap J^{k_2}\right)$ *is the multiplicity of the members of* J^{k_3}.

Finally, we define the operation "/", that is, subtraction for multisets.

Let $X=\left\{\alpha(x)*x;x\in B^n\right\},Y=\left\{\alpha(y)*y;y\in B^n\right\}$.

Definition. $X\setminus Y=\left\{\alpha(z)*z;\text{ where }\alpha(z)=\max\left\{\alpha(x)-\alpha(y),0\right\},z=x=y\in B^n\right\}$.

Example. We consider the multisets:

$$X=B_p^n+J^k=\left\{\begin{pmatrix}k\\ p-\lambda_1\left(J^k+x\right)\end{pmatrix}*x,x\in B^n\right\},$$

$$Y=B_p^n+J^k=\left\{\alpha(y)*y,y\in B^n,\alpha(y)=\begin{cases}1;\ \text{if}\begin{pmatrix}k\\ p-\lambda_1(J^k+y)\end{pmatrix}\geq 1\\ 0;\quad\text{otherwise}\end{cases}\right\}.$$

From Statements 22 and 12 we get:

$$X\setminus Y=\left\{\left(\begin{pmatrix}k\\ p-\lambda_1\left(J^k+z\right)\end{pmatrix}-1\right)*z,z\in B^n\right\}.$$

References

[1] Leontiev, V.K., Movsisyan, G.L. and Margaryan, Zh.G. (2016) Algebra and Geometry of Sets in Boolean Space. *Open Journal of Discrete Mathematics* (*OJDM*), **6**, 25-40.

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

[3] Sachkow, W.N. (1977) Combinatory Methods of Discrete Mathematics. Nauka, Moscow. (In Russian)

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

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

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

[7] Lang, S. (1968) Algebra. Moscow, Mir. (In Russian)

[8] Nigmatulin, R.G. (1991) Complexity of Boolean Functions. Nauka, Moscow, p. 240. (In Russian)

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

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

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

[12] Delsarte, P. (1973) Four Fundamental Parameters of a Code and Their Combinatorial Significance. *Information and Control*, **23**, 407-438.