Yashunsky A. D.

On probability distribution sets preserved by finite field operations

Recommended form of bibliographic references: Yashunsky A. D. On probability distribution sets preserved by finite field operations // Keldysh Institute Preprints. 2014. No. 51. 20 p. URL: http://library.keldysh.ru/preprint.asp?id=2014-51&lg=e

Ордена Ленина
ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
имени М.В. Келдыша
Российской академии наук

A. D. Yashunsky

On probability distribution sets preserved by finite field operations

Москва — 2014

Яшунский А. Д.

О множествах распределений вероятностей, сохраняемых операциями конечного поля

Рассматриваются распределения случайных величин над конечным полем, получаемых с помощью операций поля из независимых случайных величин, имеющих заданные распределения. Строятся подмножества распределений, которые сохраняются операциями сложения и умножения в конечном поле.

Ключевые слова: случайная величина, конечное поле, выразимость, сохраняемое множество

Alexey Dmitrievich Yashunsky

On probability distribution sets preserved by finite field operations

We consider distributions of random variables over a finite field, obtained as results of field operations on independent random variables with given distributions. We construct subsets of distributions that are preserved by finite field addition and multiplication.

Key words: random variable, finite field, expressibility, preserved set

The work is supported by the Russian fund for basic research (project N 14–01–00598) and the Mathematics department of RAS Fundamental research program ,,Algebraic and combinatorial methods of mathematical cybernetics and information systems of a new generation" (project ,,Optimal control systems synthesis").

Contents

Problem statement

Consider a finite field $\mathcal{F}$ with k elements that are, for the sake of convenience, further denoted by $\{0, 1, 2, \ldots, k-1\}$. For elements $i, j \in \mathcal{F}$ the addition $i + j$ and multiplication $i \cdot j$ operations are defined. The element $0 \in \mathcal{F}$ is further considered to be the ,,zero" of multiplication (i. e. $0 \cdot i = i \cdot 0 = 0$) and the neutral element of addition (i. e. $0 + i = i + 0 = i$).

The properties of other elements from the field $\mathcal{F}$ are not essential for the forthcoming results, the only important conditions being that for non-zero $i, j \in \mathcal{F}$ the inequality $i \cdot j \neq 0$ holds and the equation $i \cdot j = m$ has unique solutions both with respect to i and j. We shall denote $i = m/j$ and $j = m/i$.

For the addition operation for any $i, j, m \in \mathcal{F}$ the equation $i + j = m$ has unique solutions both with respect to i and j: $i = m - j$, $j = m - i$.

We consider random variables over the field $\mathcal{F}$. The distribution of a random variable X is treated as a vector with k coordinates $P(X) = u = (u_0, u_1, \ldots, u_{k-1})$, where u_i the value of the probability $\mathcal{P}\{X = i\}$. Naturally, for all $i \in \mathcal{F}$ the inequality $u_i \geq 0$ holds and we have

$$u_0 + u_1 + u_2 + \ldots + u_{k-1} = 1.$$

For two independent random variables X_1 and X_2 over the field $\mathcal{F}$ one can consider the sum $X_1 + X_2$ and the product $X_1 \cdot X_2$, that are also random variables over the field $\mathcal{F}$. Let $P(X_1) = u$, $P(X_2) = v$. Denote the probability distributions $P(X_1 + X_2)$ and $P(X_1 \cdot X_2)$ by $u + v$ and $u \cdot v$ respectively. Their components are given by the following equations:

$$(u + v)_i = \sum_{j \in \mathcal{F}} u_j v_{i-j}, \tag{1}$$

$$(u \cdot v)_0 = u_0 + v_0 - u_0 v_0, \tag{2}$$

$$i \neq 0 : (u \cdot v)_i = \sum_{j \in \mathcal{F} \setminus \{0\}} u_j v_{i/j}. \tag{3}$$

We consider the problem of obtaining various probability distributions as distributions of read-once formulas over the field $\mathcal{F}$ whose variables are independent identically distributed random variables over $\mathcal{F}$, all having a given ,,initial" distribution $p = (p_0, p_1, \ldots, p_{k-1})$.

Previously in [3] family of distributions that can be obtained by read-once formulas from an arbitrary initial distribution with positive components was constructed. The present work contains results of a restricting nature: we construct sets of probability distributions that are preserved by field operations. Consequently, if the initial distribution p is contained in one of the preserved

sets, no distribution outside the set can be expressed by a read-once formula over independent random variables having distribution p.

Naturally, the preserved sets contain the distributions from the previously constructed family of expressible distributions.

Geometry of the distribution space

The set of distributions on elements of the field $\mathcal{F}$ may be interpreted geometrically as a $(k-1)$-dimensional simplex in a k-dimensional space with coordinates $(u_0, u_1, \ldots, u_k)$, defined by the relations:

$$u_0 \geq 0, u_1 \geq 0, \ldots, u_{k-1} \geq 0, u_0 + u_1 + \ldots + u_{k-1} = 1.$$

The vertices of this simplex are points with coordinates $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots$ $\ldots, 0)$,..., $(0, \ldots, 0, 1)$. They correspond to degenerate distributions with the probability of one of the field elements equal to 1. The uniform distribution $\left(\frac{1}{k}, \ldots, \frac{1}{k}\right)$ corresponds to the center of mass of the simplex. The fig. 1 represents the set of distributions for a three-element field.

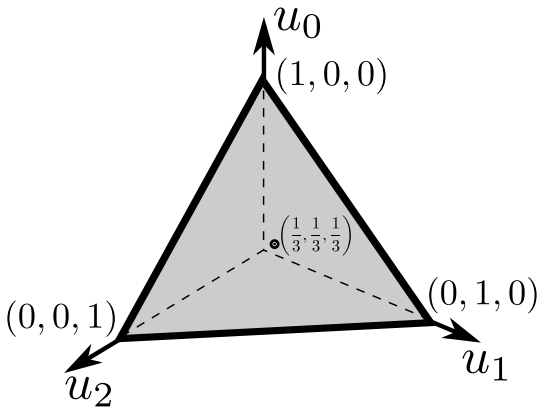

Figure 1

For our further constructions it is convenient to describe the distributions by a set of values expressed through components $u_0, \ldots, u_{k-1}$. *De facto*, we consider an alternative coordinate system in the k-dimensional space. For a point u with coordinates $(u_0, u_1, \ldots, u_{k-1})$ define:

$$\varepsilon(u) = 1 - u_0, \quad \delta_1(u) = u_1 - \frac{\varepsilon(u)}{k-1}, \ldots, \quad \delta_{k-1}(u) = u_{k-1} - \frac{\varepsilon(u)}{k-1}.$$

The set of values $(\varepsilon(u), \delta_1(u), \ldots, \delta_{k-1}(u))$ is actually the set of coordinates of the point u in a different basis; if one supposes that initially $(u_0, \ldots, u_{k-1})$ were the coordinates in an othonormal basis, the alternative basis is no longer an orthonoral one (see fig. 2 for three dimensions).

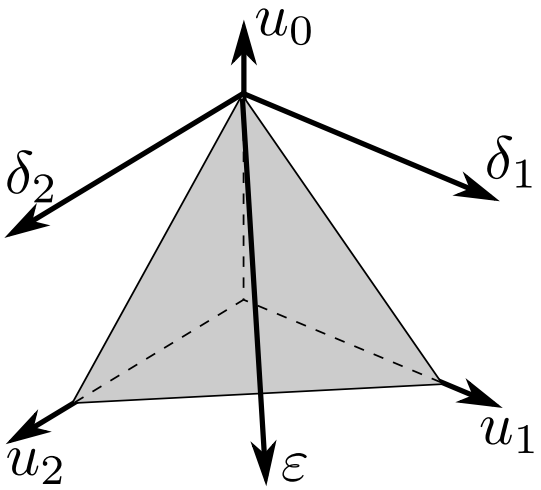

Figure 2

The coordinates of new basis vectors in the original basis are:

$$\left(-1, \frac{1}{k-1}, \ldots, \frac{1}{k-1}\right),$$
$$(0, 1, 0, \ldots, 0),$$
$$\ldots,$$
$$(0, \ldots, 0, 1),$$

i. e., with the exception of the first basis vector, they coincide with vectors from the original basis. It is easily seen that this change of coordinates is affine. Henceforth we shall operate on coordinates $(\varepsilon(u), \delta_1(u), \ldots, \delta_{k-1}(u))$, keeping in mind that all results can be easily transferred back to the original coordinates by the inverse affine transformation.

Substantially, the values $(\varepsilon(u), \delta_1(u), \ldots, \delta_{k-1}(u))$ have the following meaning for probability distributions. The value $\varepsilon(u)$ shows how much the probability of the element $0 \in \mathcal{F}$ differs from probability 1, while the values $\delta_i(u)$ show how much the conditional distribution, for a fixed probability of the element $0 \in \mathcal{F}$ equal to $1 - \varepsilon(u)$, differs from uniform on the set $\mathcal{F} \setminus \{0\}$.

For the sake of convenience we shall consider the set of values $(\varepsilon(u), \delta_1(u), \ldots$ $\ldots, \delta_{k-1}(u))$ as a set of coordinates in some orthonormal basis.

The relations defining the probability distribution simplex in the new coordinate system take the form

$$\varepsilon(u) \leq 1, \delta_1 \geq -\frac{\varepsilon}{k-1}, \ldots, \delta_{k-1} \geq -\frac{\varepsilon}{k-1},$$
$$\delta_1 + \ldots + \delta_{k-1} = 0.$$

These relations also define a simplex in coordinates $(\varepsilon, \delta_1, \ldots, \delta_{k-1})$. The point of origin $(0, \ldots, 0)$ is one of the simplex vertices. The point with coordinates $(1, 0, \ldots, 0)$ lies on a face of the simplex; the points with coordinates

$(0,1,0,\ldots,0)$,...,$(0,\ldots,0,1)$ lie outside the simplex. Thus the axis ε passes through the simplex, while the axes δ_1,...,δ_{k-1} pass outside.

The simplex is easily seen to be contained within a $(k-1)$-dimensional hyperplane (further denoted D), orthogonal to the vector with coordinates $(0,1,\ldots,1)$. The vector $\vec{e}_i = (0,\ldots,0,1,0,\ldots,0)$ can be represented as a sum:

$$\vec{e}_i = \frac{1}{k-1}(0,1,\ldots,1) + \frac{1}{k-1}(0,-1,\ldots,-1,k-2,-1,\ldots,-1),$$

hence the projection of the vector $\vec{e}_i$ onto the hyperplane D equals

$$\vec{e}'_i = \frac{1}{k-1}(0,-1,\ldots,-1,k-2,-1,\ldots,-1).$$

Fig. 3 represents a three-dimensional simplex (for a four-element field), the basis vector $\vec{e}_0$ and the projections of basis vectors $\vec{e}'_1$, $\vec{e}'_2$, $\vec{e}'_3$.

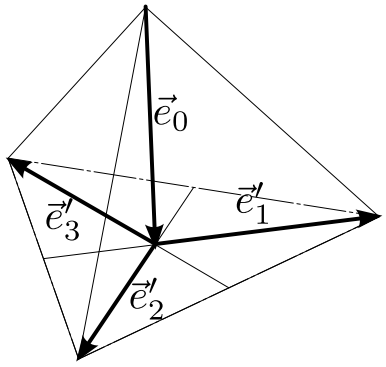

Figure 3

The position vector $\vec{w} = (\varepsilon, \delta_1, \ldots, \delta_{k-1})$ of a point in space satisfies the equality:

$$\vec{w} = \varepsilon\vec{e}_0 + \delta_1\vec{e}_1 + \ldots + \vec{e}_{k-1}.$$

For a point within the hyperplane D under projection into D this equality becomes

$$\vec{w} = \varepsilon\vec{e}_0 + \delta_1\vec{e}'_1 + \ldots + \vec{e}'_{k-1}.$$

Taking the dot product of both sides with $\vec{e}'_i$ $(i > 0)$, due to $(\vec{e}'_i, \vec{e}'_i) = \frac{k-2}{k-1}$ and $(\vec{e}'_j, \vec{e}'_i) = -\frac{1}{k-1}$ for $i \neq j$, we obtain:

$$\begin{aligned}(\vec{w}, \vec{e}'_i) &= \varepsilon(\vec{e}_0, \vec{e}'_i) + \delta_1(\vec{e}'_1, \vec{e}'_i) + \ldots + (\vec{e}'_{k-1}, \vec{e}'_i) = \\ &= \delta_i(\vec{e}'_i, \vec{e}'_i) + \sum_{j\neq 0,i} \delta_j(\vec{e}'_j, \vec{e}'_i) = \delta_i\frac{k-2}{k-1} + \sum_{j\neq 0,i} \delta_j\left(-\frac{1}{k-1}\right) = \\ &= \delta_i\frac{k-2}{k-1} + \delta_i\frac{1}{k-1} - \frac{1}{k-1}\sum_{j\neq 0}\delta_j = \delta_i.\end{aligned}$$

Let l_i be the length of the vector's $\vec{w}$ projection onto vector $\vec{e}'_i$, then:

$$(\vec{w}, \vec{e}'_i) = l_i|\vec{e}'_i| = \frac{l_i}{|\vec{e}'_i|}(\vec{e}'_i, \vec{e}'_i) = \frac{l_i}{|\vec{e}'_i|}\frac{k-2}{k-1}.$$

Thus we obtain $\delta_i = \frac{k-2}{k-1} \cdot \frac{l_i}{|\vec{e}'_i|}$. Consequently, for obtaining the coordinate δ_i of a point in space, one needs only to find the ratio between the length of its position vector's projection onto the vector $\vec{e}'_i$ and the length of the vector $\vec{e}'_i$. This observation shall be further used to describe subsets of the simplex.

The sets that are further constructed, are intersections of sets, each of which is defined by inequalities, relating one of the coordinates δ_i to the coordinate ε. Due to such structure, consideration of these sets is more convenient in terms of their projection onto a two-dimensional plane, defined by vectors $\vec{e}_0$ and $\vec{e}'_i$.

Sums and products of random variables

When passing from distributions $u = (u_0, \ldots, u_{k-1})$ and $v = (v_0, \ldots, v_{k-1})$ to their corresponding values $(\varepsilon(u), \delta_1(u), \ldots)$ and $(\varepsilon(v), \delta_1(v), \ldots)$, we naturally have to transform the formulas (1)–(3). Since $\varepsilon(u) = 1 - u_0$ and $\varepsilon(v) = 1 - v_0$, formula (2) becomes:

$$\varepsilon(u \cdot v) = \varepsilon(u) \cdot \varepsilon(v). \tag{4}$$

Expressing u_i in terms of $\delta_i(u)$, $\varepsilon(u)$, and v_i in terms of $\delta_i(v)$ and $\varepsilon(v)$, after the necessary simplifications we obtain:

$$\delta_i(u \cdot v) = \sum_{j \in \mathcal{F} \setminus \{0\}} \delta_j(u)\delta_{i/j}(v). \tag{5}$$

For the distribution of a sum instead of the relation (1) we have two equalities:

$$\varepsilon(u + v) = \varepsilon(u) + \varepsilon(v) - \frac{k}{k-1}\varepsilon(u)\varepsilon(v) - \sum_{j \in \mathcal{F} \setminus \{0\}} \delta_j(u)\delta_{-j}(v), \tag{6}$$

$$\begin{aligned}\delta_i(u + v) = &\left(1 - \frac{k}{k-1}\varepsilon(u)\right)\delta_i(v) + \left(1 - \frac{k}{k-1}\varepsilon(v)\right)\delta_i(u) + \\ &+ \sum_{j \in \mathcal{F} \setminus \{0,i\}} \delta_j(u)\delta_{i-j}(v) + \frac{1}{k-1}\sum_{j \in \mathcal{F} \setminus \{0\}} \delta_j(u)\delta_{-j}(v).\end{aligned} \tag{7}$$

The obtained formulas (4)–(7) may be simply regarded as transformations in the space with coordinates $(\varepsilon, \delta_1, \ldots, \delta_{k-1})$, than can also be applied *outside* the simplex whose points correspond to probability distributions over the field $\mathcal{F}$.

Further on we shall name the point $u \cdot v$, obtained according to the formulas (4), (5) the product of points u and v (possibly located outside the probability distribution simplex), and the point $u + v$, obtained according to the formulas (6), (7) — the sum of points u and v.

It follows from the formula (4) that a product of several independent random variables produces a distribution that tends to the distribution with $\varepsilon = 0$ (and, consequently, $\delta_1 = \ldots = \delta_{k-1} = 0$) as product length grows.

Since addition in the field is a group (and, hence, a quasigroup) operation, the results of [2] imply that a sum of several independent random variables with positive distribution components produces a distribution that approaches the uniform distribution on the field's elements as sum length grows. It has $\varepsilon = \frac{k-1}{k}$ and $\delta_1 = \ldots = \delta_{k-1} = 0$. The value $\frac{k-1}{k}$ is used in further constructions and henceforth denoted by h.

The results of [3] for distributions of finite fields allow a geometric representation. Let $E = \{0 \leq \varepsilon \leq h, \delta_1 = \ldots = \delta_{k-1} = 0\}$ be a segment in the probability distribution space. For an arbitrary initial distribution π with positive components and an arbitrary point $a \in E$ there exists a read-once formula consisting of additions and multiplications over the field $\mathcal{F}$, such that substituting independent random variables with distribution π into the formula, one obtains a distribution arbitrarily close to the point a. Fig. 4 represents the segment E for the case of a four-element field.

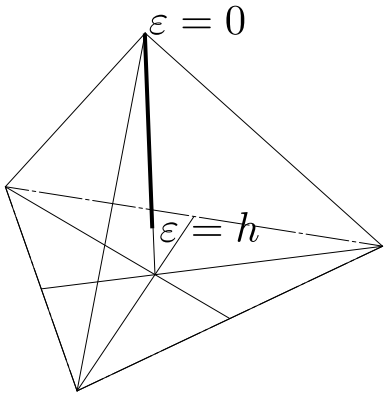

Figure 4

Multiplication-preserved sets

Let us define a subset H_α in the distribution space:

$$H_\alpha = D \cap \left\{ (\varepsilon, \delta_1, \ldots, \delta_{k-1}) : \max_{i \neq 0} |\delta_i| \leq \frac{\varepsilon^\alpha}{k-1} \right\} = D \cap \left(\bigcap_{i \neq 0} \left\{ |\delta_i| \leq \frac{\varepsilon^\alpha}{k-1} \right\} \right).$$

Let us alse define $H_{\alpha,b} = H_\alpha \cap \{(\varepsilon, \delta_1, \ldots, \delta_{k-1}) : \varepsilon \le b\}$. One can easily see from the definition of the set $H_{\alpha,1}$, that its projection onto a two-dimensional plane of the vectors $\vec{e}_0$, $\vec{e}\,'_i$ is of the form presented in fig. 5.

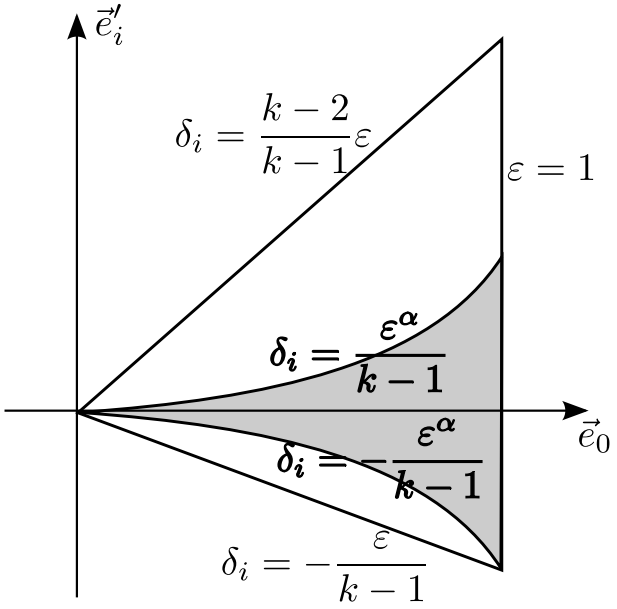

Figure 5

The set $H_{\alpha,1}$ for a four-element filed is represented in fig. 6. Its sections by planes with constant values of ε are figures defined by inequalities $\max\limits_i |\delta_i| \le d$ with d depending on ε. For $k = 3$ the section is a hexagon. The sections of other sets defined further have a similar structure.

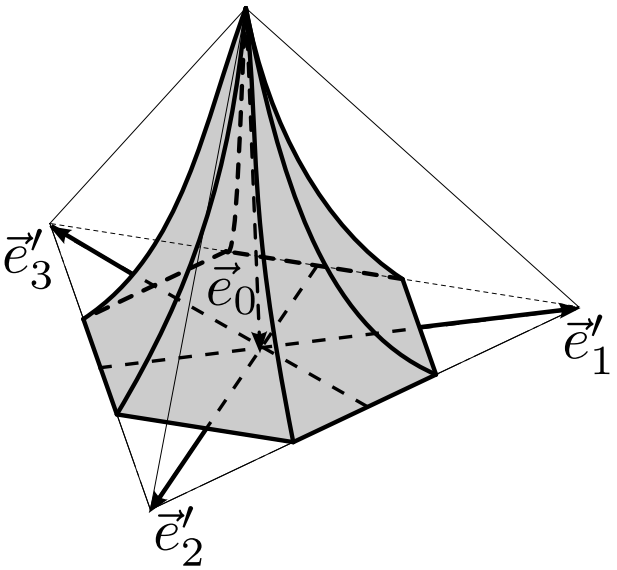

Figure 6

Lemma 1. *Let $\alpha \ge 1$, $b_1, b_2 \ge 0$, $u \in H_{\alpha,b_1}$, $v \in H_{\alpha,b_2}$. Then $u \cdot v \in H_{\alpha,b_1 b_2}$.*

Proof. For $u \in H_{\alpha,b_1}$, $v \in H_{\alpha,b_2}$ we have $\varepsilon(u) \le b_1$, $\varepsilon(v) \le b_2$, hence due to (4) we obtain $\varepsilon(u \cdot v) \le b_1 b_2$.

Consider now $\delta_i(u \cdot v)$ for an arbitrary $i \ne 0$. According to (5):

$$|\delta_i(u \cdot v)| = \left| \sum_{j \ne 0} \delta_j(u) \delta_{i/j}(v) \right| \le \sum_{j \ne 0} |\delta_j(u)| \cdot |\delta_{i/j}(v)| \le \sum_{j \ne 0} \frac{(\varepsilon(u))^\alpha}{k-1} \cdot \frac{(\varepsilon(v))^\alpha}{k-1} =$$
$$= (k-1) \cdot \frac{(\varepsilon(u) \cdot \varepsilon(v))^\alpha}{(k-1)^2} = \frac{(\varepsilon(u \cdot v))^\alpha}{k-1}.$$

Hence, $u \cdot v \in H_{\alpha,b_1 b_2}$. The lemma is proved.

Addition-preserved sets

Note that the formulas (6) and (7) are linear both in $\varepsilon(u)$, $\delta_j(u)$ for a fixed v, and in $\varepsilon(v)$, $\delta_j(v)$ for a fixed u. An easy corollary is that for a fixed v a convex set of distributions u is transformed by (6) and (7) into a convex set (and for a fixed u a convex set of distributions v becomes a convex set). These observations eventually allow to prove that the operation $u + v$ preserves some convex sets.

Let a, b, c be some positive real numbers. Consider the set of points $(\varepsilon, \delta_1, \dots$ $\dots, \delta_{k-1})$ from the hyperplane D satisfying the inequations:

$$|\delta_i| \le a - \frac{a}{b}(\varepsilon - h), \quad |\delta_i| \le a + \frac{a}{c}(\varepsilon - h), \quad i = 1, \dots, k-1. \tag{8}$$

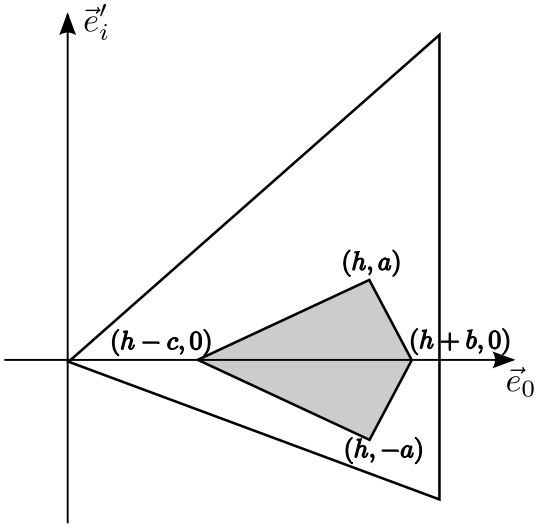

Figure 7

Denote this set of points by $K_{a,b,c}$. Thus

$$K_{a,b,c} = D \cap \left(\bigcap_{i \neq 0} \left\{ |\delta_i| \leq a - \frac{a}{b}(\varepsilon - h), |\delta_i| \leq a + \frac{a}{c}(\varepsilon - h) \right\} \right).$$

The set $K_{a,b,c}$ is easily seen to be convex. The projection of the set $K_{a,b,c}$ onto the two-dimensional plane of the vectors $\vec{e}_0$, $\vec{e}'_i$is represented in fig. 7.

The set $K_{a,b,c}$ may be regarded as the solution for the following system

$$\begin{cases} \frac{a}{b}\varepsilon + \delta_1 \leq a + \frac{a}{b}h \\ \frac{a}{b}\varepsilon - \delta_1 \leq a + \frac{a}{b}h \\ -\frac{a}{c}\varepsilon + \delta_1 \leq a - \frac{a}{c}h \\ -\frac{a}{c}\varepsilon - \delta_1 \leq a - \frac{a}{c}h \\ \dots \\ \delta_1 + \ldots + \delta_{k-1} \leq 0 \\ -\delta_1 - \ldots - \delta_{k-1} \leq 0 \end{cases}, \tag{9}$$

containing $4(k-1)+2$ inequations.

The set of solutions to this system forms a convex polyhedron, which is a convex hull of its vertices (extreme points), see [1]. The vertices are the solution of the system of equations, obtained from (9) by replacing non-strict inequalities either by strict ones, or by equalities in such a way that the subsystem containing only equalities has exactly rank k.

The last two inequations are easily seen to always become equations. For an arbitrary i consider four inequations, containing δ_i and ε. Among the various possibilities for changing inequalities to equalities only four are consistent, they define the vertices of the set represented in fig. 7:

1. $\varepsilon = h - c$, $\delta_i = 0$;
2. $\varepsilon = h$, $\delta_i = a$;
3. $\varepsilon = h$, $\delta_i = -a$;
4. $\varepsilon = h + b$, $\delta_i = 0$.

The choice of either $\varepsilon = h - c$ or $\varepsilon = h + b$ transforms two inequalities in each quadruple of inequations into equalities, binding one of the δ_j with ε, the resulting equations being linearly dependent, hence adding only 1 (and not 2)

to the system's rank. These equations lead to $\delta_j = 0$. The total rank of the equations' system is $2 + 1 \cdot (k-2) = k$.

The choice of $\varepsilon = h$ leads to two of the four inequations binding one of the δ_j with ε becoming inequations $\delta_j \le a$ while the two others become $\delta_j \ge -a$. Consequently, only two inequations out of four can become equations, and the resulting pair of equations adds only 1 to the system's rank. Generally speaking, it is possible that none of the inequations binding δ_j with ε become equations.

After choosing some δ_i one has freedom to choose $k-3$ independent equations defining the values for various δ_j. For defining the last undefined δ_j we complete the system with the equation $\delta_1 + \ldots + \delta_{k-1} = 0$. It is clearly independent of other equations and allows to define the remaining δ_j. The resulting system rank is $2 + 1 \cdot (k-3) + 1 = k$.

Hence, we conclude that the vertices of the convex set $K_{a,b,c}$ are:

1. the point $(h - c, 0, \ldots, 0)$;
2. the point $(h + b, 0, \ldots, 0)$;
3. points of the form $(h, d_1, \ldots, d_{k-1})$, where $d_1 + \ldots + d_{k-1} = 0$ and all d_i, with possibly one exception belong to the set $\{a, -a\}$ (and if $d_i \ne \pm a$, it is zero).

All of these points, naturally belong to the hyperplane D, but, strictly speaking, are not necessarily inside the simplex that corresponds to probability distributions.

Let us show that a certain relation between the parameters a, b, c guarantees that the set $K_{a,b,c}$ is preserved by transformations defined by (6) and (7).

Lemma 2. *Let* $0 < a \le \frac{1}{k}$, $k(k-1)a^2 \le b \le c \le h$. *Let* $u, v \in K_{a,b,c}$. *Then* $u + v \in K_{a,b,c}$.

Proof. By convexity of the set $K_{a,b,c}$ and bilinearity of the $u + v$ transform it suffices to prove that for any pair of vertices u, v of the set $K_{a,b,c}$ the resulting $u + v$ belongs to $K_{a,b,c}$. Let us consider all the possible pairs.

Let first $u = (h + x, 0, \ldots, 0)$, $v = (h + y, 0, \ldots, 0)$. Then by (6), (7) we obtain:

$$\begin{aligned} \varepsilon(u+v) &= (h+x) + (h+y) - \frac{1}{h}(h+x)(h+y) = h - \frac{xy}{h}, \\ \delta_i(u+v) &= 0. \end{aligned} \tag{10}$$

Using these relations we find $\varepsilon(u+v)$ for the following combinations of vertices:

1. $u = (h - c, 0, \ldots, 0)$, $v = (h - c, 0, \ldots, 0)$: $\varepsilon(u + v) = h - \frac{c^2}{h}$.

2. $u = (h - c, 0, \ldots, 0)$, $v = (h + b, 0, \ldots, 0)$: $\varepsilon(u + v) = h + \frac{bc}{h}$.

3. $u = (h + b, 0, \ldots, 0)$, $v = (h + b, 0, \ldots, 0)$: $\varepsilon(u + v) = h - \frac{b^2}{h}$.

Since under the lemma's conditions the inequations $b \le c \le h$ hold, we have $\frac{bc}{h} \le b$, $\frac{c^2}{h} \le c$ and $\frac{b^2}{h} \le c$. Hence, in all of the considered combinations we have $u + v \in K_{a,b,c}$.

Let now $u = (h + x, 0, \ldots, 0)$, $v = (h, d_1, \ldots, d_{k-1})$. Then by (6), (7) we obtain:

$$\begin{aligned} \varepsilon(u + v) &= (h + x) + h - \frac{1}{h}(h + x)h = h, \\ \delta_i(u + v) &= \left(1 - \frac{1}{h}(h + x)\right) d_i = -\frac{x}{h} d_i. \end{aligned} \tag{11}$$

Both in the case of $u = (h - c, 0, \ldots, 0)$ and in the case of $u = (h + b, 0, \ldots, 0)$, by inequations $b \le c \le h$ we have:

$$|\delta_i(u + v)| \le |d_i| \le a,$$

which easily implies that $u + v \in K_{a,b,c}$.

Finally, let us consider $u = (h, d'_1, \ldots, d'_{k-1})$ and $v = (h, d''_1, \ldots, d''_{k-1})$. Then by (6), (7) we obtain:

$$\varepsilon(u + v) = h + h - \frac{1}{h}h^2 - \sum_{j \ne 0} d'_j d''_{-j} = h - \sum_{j \ne 0} d'_j d''_{-j},$$

$$\delta_i(u + v) = \sum_{j \ne 0, i} d'_j d''_{i-j} + \frac{1}{k-1} \sum_{j \ne 0} d'_j d''_{-j}.$$

The obtained relations imply inequations $|\varepsilon(u + v) - h| \le (k - 1)a^2$ and

$$|\delta_i(u + v)| \le (k - 2)a^2 + \frac{1}{k-1}(k - 1)a^2 = (k - 1)a^2.$$

Thus, the point $u + v$ is located inside the convex set defined by inequations:

$$\begin{gathered} h - (k - 1)a^2 \le \varepsilon \le h + (k - 1)a^2, \\ -(k - 1)a^2 \le \delta_i \le (k - 1)a^2, \quad i = 1, \ldots, k - 1. \end{gathered}$$

The projection of this set onto the two-dimensional plane of the vectors $\vec{e}_0$, $\vec{e}'_i$ is represented in fig. 8.

Let us show that this entire set lies within $K_{a,b,c}$. For this it suffices to show that its vertices are located inside $K_{a,b,c}$, i. e. satisfy the inequations (8).

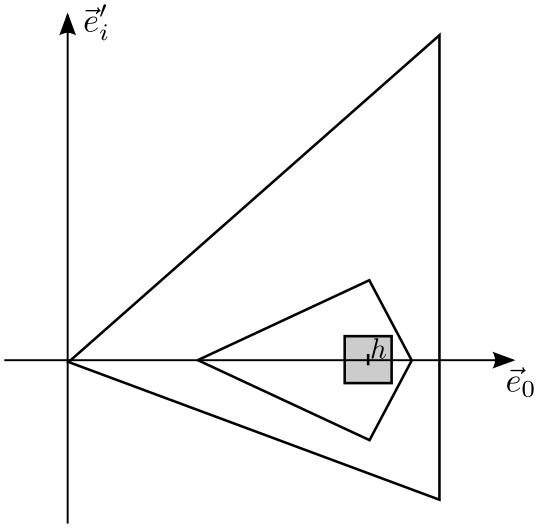

Figure 8

For the considered vertex points we have $\varepsilon = h \pm (k-1)a^2$, hence $\varepsilon - h = \pm(k-1)a^2$. Besides, these points have $|\delta_i| = (k-1)a^2$. Consequently, we have to show that the following inequations hold:

$$(k-1)a^2 \le a \pm \frac{a}{b}(k-1)a^2, \quad (k-1)a^2 \le a \pm \frac{a}{c}(k-1)a^2.$$

By positivity of a, b, c, the inequations

$$(k-1)a^2 \le a + \frac{a}{c}(k-1)a^2 \text{ and } (k-1)a^2 \le a + \frac{a}{b}(k-1)a^2$$

follow from

$$(k-1)a^2 \le a - \frac{a}{c}(k-1)a^2 \text{ and } (k-1)a^2 \le a - \frac{a}{b}(k-1)a^2.$$

By lemma's conditions $b, c \ge k(k-1)a^2$, wherefrom we obtain $\frac{a}{b}(k-1)a^2 \le \frac{a}{k}$ and $\frac{a}{c}(k-1)a^2 \le \frac{a}{k}$. Hence

$$a - \frac{a}{b}(k-1)a^2 \ge a - \frac{a}{k} = \frac{a}{k}(k-1),$$
$$a - \frac{a}{c}(k-1)a^2 \ge a - \frac{a}{k} = \frac{a}{k}(k-1).$$

Together with the inequation $a \le \frac{1}{k}$ provided by lemma's conditions, this leads to the necessary inequations. The lemma is proved.

Lemma 3. *Let* $K_1 = K_{a,k(k-1)a^2,c}$, $K_2 = K_{a',k(k-1)a'^2,c'}$, *where* $0 < a, a' \le \frac{1}{k}$, $k(k-1)a^2 \le c \le h$, $k(k-1)a'^2 \le c' \le h$. *Then for any* $u, v \in K_1 \cup K_2$ *holds* $u + v \in K_1 \cup K_2$.

Proof. Without loss of generality, let us consider $a \geq a'$. If, besides that, we have $c' \leq c$, then $K_2 \subseteq K_1$, $K_1 \cup K_2 = K_1$ and the lemma's statement follows directly from lemma 2. Further we suppose $c' > c$. The projections of the sets K_1 and K_2 onto the two-dimensional plane of the vectors $\vec{e}_0$, $\vec{e}'_i$ in this case are represented in fig. 9.

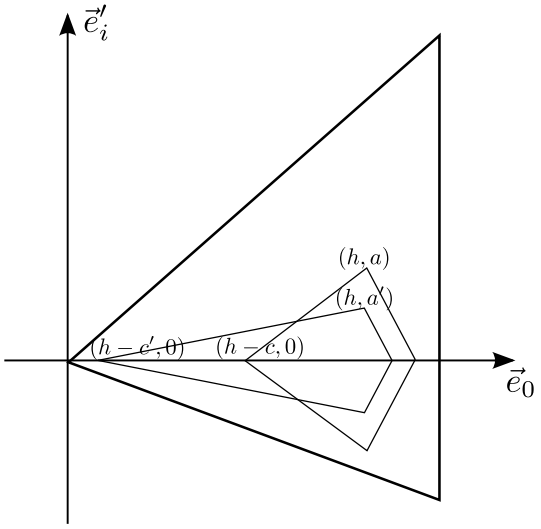

Figure 9

Let $u, v \in K_1 \cup K_2$. Supposing that moreover $u, v \in K_1$ (respectively, $u, v \in K_2$), we obtain by lemma 2 that $u + v \in K_1$ (respectively, $u + v \in K_2$) holds, which implies the lemma's statement. Thus the only remaining cases to consider are the ones with $u \in K_1$, $v \in K_2$.

Let us show that for any fixed $u \in K_1$ and all possible $v \in K_2$ the sum $u + v$ belongs to K_1. By convexity of the sets K_1 and K_2 it suffices to show that all possible combinations with u being a vertex of K_1 and v being a vertex of K_2 lead to $u + v \in K_1$.

Due to the relations $a \geq a'$ and $c < c'$ between the parameters of the sets K_1 and K_2, all of the vertices of K_2 with the exception of $(h - c', 0, \ldots, 0)$ are located within K_1, thus having $u + v \in K_1$ by virtue of lemma 2. Let us show that for $v = (h - c', 0, \ldots, 0)$ we also have $u + v \in K_1$ for all vertices u of the set K_1.

The relations (10) and the inequation $c' \leq h$ imply that for vertices $u = (h - c, 0, \ldots, 0)$ and $u = (h + k(k-1)a^2, 0, \ldots, 0)$ we have $u + v \in K_1$.

For $u = (h, d_1, \ldots, d_{k-1})$ the relations (11) and the inequation $c' \leq h$ imply that $u + v \in K_1$. Thus, the lemma is proved.

Preservation theorems

Theorem 1. *Let* $0 < a \leq \frac{1}{k}$. *Then for any* $u, v \in K_{a,k(k-1)a^2,h} \cap \{\varepsilon \leq 1\}$ *we have* $u \cdot v, u + v \in K_{a,k(k-1)a^2,h} \cap \{\varepsilon \leq 1\}$.

Proof. By virtue of lemma 2 under the theorem's conditions $u+v \in K_{a,k(k-1)a^2,h}$, thus it suffices to prove that $u \cdot v \in K_{a,k(k-1)a^2,h}$.

Let us consider some $u, v \in K_{a,k(k-1)a^2,h}$ and, without loss of generality, let $\varepsilon(u) \leq \varepsilon(v)$. Define:

$$d = \max_i \{|\delta_i| : (\varepsilon(u), \delta_1, \ldots, \delta_{k-1}) \in K_{a,k(k-1)a^2,h}\}.$$

Due to $a \leq \frac{1}{k}$ one may chose such an α that $d = \frac{(\varepsilon(u))^\alpha}{k-1}$, namely $\alpha = \frac{\ln(k-1)d}{\ln \varepsilon(u)} \geq 1$ (see fig. 10).

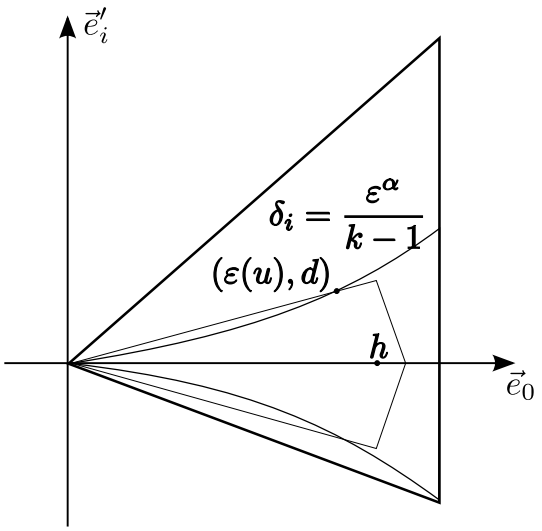

Figure 10

By choice of d and α we obtain that $H_{\alpha,\varepsilon(u)} \subset K_{a,k(k-1)a^2,h}$. Besides that, $u \in H_{\alpha,\varepsilon(u)}$, $v \in H_{\alpha_0,\varepsilon(v)}$. Hence, by virtue of lemma 1 and due to $\varepsilon(u), \varepsilon(v) \leq 1$ we obtain:

$$u \cdot v \in H_{\alpha,\varepsilon(u)\varepsilon(v)} \subseteq H_{\alpha,\varepsilon(u)} \subset K_{a,k(k-1)a^2,h}.$$

The inequations $\varepsilon(u \cdot v) \leq 1$ and $\varepsilon(u + v) \leq 1$ are an easy implication of the theorem's conditions. The theorem is proved.

Theorem 2. *For any* $k \geq 3$ *there exists such an* $\alpha_0(k)$ *that for all* $\alpha \geq \alpha_0(k)$ *the sets*

$$I_\alpha = (H_{\alpha,h} \cup K_{a,k(k-1)a^2,k(k-1)a^2}) \cap \{\varepsilon \leq 1\},$$

where $a = \frac{h^\alpha}{k-1}$, *are preserved by both addition and multiplication, i. e. for any* $u, v \in I_\alpha$ *we have* $u \cdot v, u + v \in I_\alpha$.

Proof. Given the relation $a = \frac{h^\alpha}{k-1}$, let us consider the reciprocal location of the set H_α and the set $K_{a,k(k-1)a^2,k(k-1)a^2}$. We shall show that for big enough values of α we have

$$K_{a,k(k-1)a^2,k(k-1)a^2} \subset H_\alpha.$$

Consider the projections of those sets onto the two-dimensional plane of the vectors $\vec{e}_0$, $\vec{e}_i'$ (see fig. 11). The point with $\varepsilon = h$ and $\delta_i = \frac{h^\alpha}{k-1}$ is easily seen to lie exactly on the boundary of both sets.

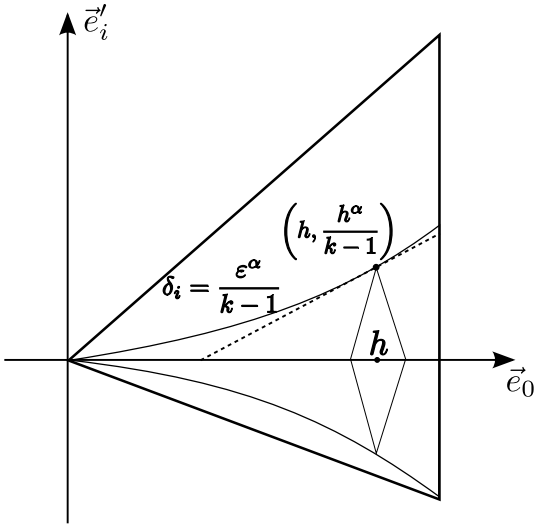

Figure 11

The points from the set $K_{a,k(k-1)a^2,k(k-1)a^2}$ satisfy the inequation

$$|\delta_i| \leq a + \frac{a}{k(k-1)a^2}(\varepsilon - h).$$

We further consider only points with $\delta_i \geq 0$ (for $\delta_i \leq 0$ the argument is analoguos).

The points of the set H_α satisfy the inequation $\delta_i \leq \frac{\varepsilon^\alpha}{k-1}$. Let us consider the tangent to the graph of the function $\frac{\varepsilon^\alpha}{k-1}$ at the point $\varepsilon = h$. The function is convex downward, hence the points that are below the tangent are also below the function's graph.

The tangent intersects the line $a + \frac{a}{k(k-1)a^2}(\varepsilon - h)$ at the point $\varepsilon = h$. If the tangent's slope is smaller than the line's slope then all of the points from the set $K_{a,k(k-1)a^2,k(k-1)a^2}$ with $\varepsilon \leq h$ lie below the tangent, and consequently within the set H_α. Also the points from the set $K_{a,k(k-1)a^2,k(k-1)a^2}$ with $\varepsilon \geq h$ obviously belong to the set H_α.

Let us write the relation between slopes as an inequation:

$$\frac{\alpha h^{\alpha-1}}{k-1} \leq \frac{a}{k(k-1)a^2}.$$

Since $a = \frac{h^\alpha}{k-1}$, it is equivalent to $\alpha h^{2(\alpha-1)} \leq 1$. Because $\lim\limits_{\alpha\to\infty} \alpha h^{2(\alpha-1)} = 0$ holds, there exists such an α_0 (depending on h and, consequently, on k), that for any $\alpha \geq \alpha_0$ the inequation is satisfied. For those values of α the inclusion $K_{a,k(k-1)a^2,k(k-1)a^2} \subset H_\alpha$ holds.

Let now $u, v \in I_\alpha$, where $\alpha \geq \alpha_0$.

If $\varepsilon(u) \leq h$ or $\varepsilon(v) \leq h$, then $u \cdot v \in H_{\alpha,h} \subset I_\alpha$. If, otherwise, $\varepsilon(u), \varepsilon(v) > h$, then there exists such an $\alpha' \geq \alpha$, that

$$u, v \in H_{\alpha',\max\{\varepsilon(u),\varepsilon(v)\}} \subset I_\alpha.$$

Hence $u \cdot v \in H_{\alpha',\max\{\varepsilon(u),\varepsilon(v)\}} \subset I_\alpha$.

Let us now show that $u + v \in I_\alpha$. If $u \in K_{a,k(k-1)a^2,k(k-1)a^2}$, let $K_1 = K_{a,k(k-1)a^2,k(k-1)a^2}$. Otherwise let us choose for K_1 such a set $K_{a',k(k-1)a'^2,c}$, that:

1. $\frac{a'}{c} = \frac{\alpha(\varepsilon(u))^\alpha}{k-1}$,

2. $\max\limits_i\{\delta_i : (\varepsilon(u), \delta_1, \ldots, \delta_{k-1}) \in K_1\} = \frac{(\varepsilon(u))^\alpha}{k-1}$,

i. e. that is tangent to the boundary of the set H_α at the point $\varepsilon = \varepsilon(u)$. It is easily seen that $u \in K_1 \subset I_\alpha$. Similarly, let us choose K_2 according to the location of v. Then $u, v \in K_1 \cup K_2$, and by virtue of lemma 3 we obtain that $u + v \in K_1 \cup K_2 \subset I_\alpha$.

The theorem is proved.

Theorems 1 and 2 allow us to construct a series of nested subsets of the probability simplex, each of which is preserved by both addition and multiplication. Projected to the plane of the vectors $\vec{e}_0$, $\vec{e}'_i$, these sets are represented in fig. 12.

Complementary remarks

Besides addition and multiplication operations in the field $\mathcal{F}$, one may consider their inverse operations of subtraction and division. From the point of view of probability distribution transformation it is equivalent to considering unary operations of negation and inversion.

For a finite field the operation of negation is, in fact, a permutation on the set of the field's elements, and it is a permutation that preserves the element $0 \in \mathcal{F}$. It is easily seen that all of the above-constructed sets, preserved by both multiplication and addition, are also preserved by permutations of the field's elements, that preserve the element 0, hence they are preserved by the unary negation operation.

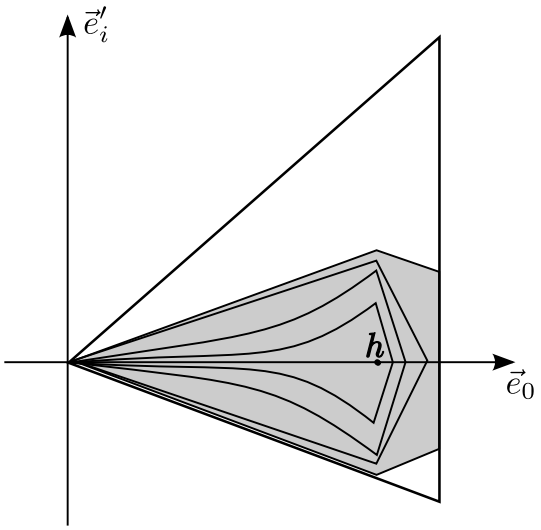

Figure 12

The inversion operation x^{-1} is not defined for $0 \in \mathcal{F}$, yet we can extend the definition by letting $0^{-1} = 0$, which will make x^{-1} also a permutation of the field's elements that preserves zero and, therefore preserves all of the sets constructed above.

It is worth noting, that the proved theorems do not require all of the field properties in the structure $\mathcal{F}$. The constructs remain valid if instead of $\mathcal{F}$ one considers a set with a quasigroup operation of ,,addition" having a neutral element $0 \in \mathcal{F}$, and an operation of ,,multiplication" which is a quasigroup on $\mathcal{F} \setminus \{0\}$ and satisfies $0 \cdot x = x \cdot 0 = 0$ for all $x \in \mathcal{F}$. Such structures, in particular, may contain an arbitrary finite number of elements k (not necessarily a power of a prime, as in the case of a field). By analogy with quasigroups, R. V. Goncharov in a private communication suggested to name these structures ,,quasifields".

The sets constructed in theorems 1 and 2 do not cover the entire simplex of probability distributions. Only in the special case of $k = 3$ for every point of the simplex there exists a preserved set containing this given point. Already for $k = 4$ one may explicitly indicate points of the simplex that do not belong to any of the constructed sets. Moreover, as k grows infinitely, the fraction of the constructed preserved sets' volume in the simplex volume tends to zero.

The author expresses his gratitude to O. M. Kasim-Zade for the attention to this work and fruitful discussions.

References

[1] Ashmanov S. A. Linear programming. — M.: Nauka, 1981. — 340 p.

[2] Yashunsky A. D. On transformations of probability distributions by read-

once quasigroup formulae // Diskretnaya matematika. — 2013. — V. 25, N 2. — P. 149–159. [English translation: Discrete Mathematics and Applications. Volume 23, Issue 2, P. 211–223.]

[3] Yashunsky A. D. On a family of probability distributions, generated by read-once formulae over finite fields // Proceedings of the IX young scientist school on discrete mathematics and its applications (Moscow, September 16–21, 2013). — M.: KIAM RAS, 2013. — P. 127–130.