Keldysh Institute • Publication search

Keldysh Institute preprints • Preprint No. 11, 2016

ISSN 2071-2898 (Print)
ISSN 2071-2901 (Online)

Yashunsky A.D.

# On convex polytopes of distributions preserved by finite field operations

***Recommended form of bibliographic references:*** Yashunsky A.D. On convex polytopes of distributions preserved by finite field operations // Keldysh Institute Preprints. 2016. No. 11. 9 p. doi:10.20948/prepr-2016-11-e
URL: http://library.keldysh.ru/preprint.asp?id=2016-11&lg=e

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

**A. D. Yashunsky**

# On convex polytopes of distributions preserved by finite field operations

Москва — 2016

**Яшунский А. Д.**

**О выпуклых многогранниках распределений, сохраняемых операциями конечного поля**

Строятся семейства многогранников в пространстве вероятностных распределений над конечным полем, обладающих свойством сохранения: при сложении или умножении независимых случайных величин, имеющих распределение из построенного множества, распределение результата также лежит в этом множестве.

***Ключевые слова:*** случайная величина, конечное поле, сохраняемое множество, выпуклый многогранник

**Alexey Dmitrievich Yashunsky**

**On convex polytopes of distributions preserved by finite field operations**

We construct families of polytopes in the space of probability distributions over a finite field, which are preserved, i.e. when adding or multiplying independent random variables with distributions from the constructed set, one obtains a result whose distribution belongs to the set as well.

***Key words:*** random variable, finite field, preserved set, convex polytope

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”).

Let us consider transformations of random variables over a finite set $E$ by applying operations from a given operation set $\mathcal{B}$ to these variables. When considering such transformations, one naturally arrives to the issue of constructing a distribution set $K$ with the following property: for any set $X_1, \ldots, X_n$ of mutually independent random variables over $E$ with distributions belonging to $K$ and any operation $f(x_1, \ldots, x_n) \in \mathcal{B}$ the distribution of the variable $f(X_1, \ldots, X_n)$ belongs to $K$ as well. In this case the set $K$ shall be referred to as *preserved* by operations from $\mathcal{B}$ (see also [1, 2]). Usually the set $K$ is constructed for some given set $G$ of *initial* distributions, so as to have $G \subseteq K$.

The present work considers a set $E$ with $k$ elements (we further let $E = \{0, 1, \ldots, k-1\}$ for the sake of convenience and denote $E \setminus \{0\}$ by $E^*$) and a set $\mathcal{B}$, containing two binary operations. The first operation, denoted by $+$, is a quasigroup operation on $E$, for which the element $0 \in E$ is the identity element[1], i.e. $0 + i = i + 0 = i$ for any $i \in E$ (for necessary definitions see [3]). The second operation, denoted by $\times$, is a quasigroup operation on $E^*$ and additionnaly satisfies the equalities $0 \times i = i \times 0 = 0$ for any $i \in E$. An example of such a set with the corresponding pair of operations is the finite field of order $k$ with $+$ and $\times$ being the finite field addition and multiplication, respectively.

The operations from $\mathcal{B}$ applied to independent random variables naturally induce operation of the random variables' distributions (stochastic vectors): tuples $(x_0, x_1, \ldots, x_{k-1})$ satisfying the conditions $x_i \geqslant 0, i \in E$ and $\sum\limits_{i \in E} x_i = 1$. The set of such vectors is a simplex that we shall further refer to as *distribution space*. Let us denote the operations induced by $+$ and $\times$ with $\oplus$ and $\otimes$. One can easily verify that for distributions $x = (x_0, x_1, \ldots, x_{k-1})$ and $y = (y_0, y_1, \ldots, y_{k-1})$ the following hold:

$$(x \oplus y)_i = \sum_{\substack{j \in E, \\ j + \ell = i}} x_j y_\ell, \ i \in E; \tag{1}$$

$$(x \otimes y)_0 = x_0 + y_0 - x_0 y_0 = x_0 + y_0(x_1 + \ldots + x_{k-1}); \tag{2}$$

$$(x \otimes y)_i = \sum_{\substack{j \in E^*, \\ j \times \ell = i}} x_j y_\ell, \ i \in E^*. \tag{3}$$

Note that due to quasigroup properties of the $+$ and $\times$ operations, the index $\ell$ in sums (1) and (3) is uniquely defined for every pair of $i$ and $j$.

In order to construct sets of distributions preserved by the $+$ and $\times$ operations we shall first prove a property of quasigroup distribution trans-

[1] Hence, $\langle E, + \rangle$ is a loop.

formations. Let $Q = \{1, 2, \ldots, q\}$ be a finite set with a binary quasigroup operation $*$, let $\backslash$ be the corresponding left division operation and $\circledast$ be the operation on distribution vectors, induced by $*$. One can easily check the equalities:

$$(x \circledast y)_i = \sum_{j \in Q} x_j y_{j\backslash i},\ i \in Q. \tag{4}$$

Note that for every $\ell \in Q$ the map $i \mapsto \ell\backslash i$ is a permutation on $Q$, let us denote it by $\sigma_\ell$. For a distribution $x = (x_1, \ldots, x_q)$ and a permutation $s$ we shall denote by $x^s$ the distribution $(x_{s(1)}, \ldots, x_{s(q)})$.

Recall, that a subset $K \subseteq \mathbb{R}^k$ is said to be *convex* if for any pair of points, belonging to the set, it contains the segment that joins them, i.e. for any $x, y \in K$ and $\alpha \in [0, 1]$ we have $\alpha x + (1 - \alpha)y \in K$.

**Lemma 1.** *Let $K$ be such a convex subset of the distribution space over $Q$ that for any $\ell \in Q$ and any $y \in K$ we have $y^{\sigma_l} \in K$. Then for any $y \in K$ and an arbitrary distribution $x$ over $Q$ we have $x \circledast y \in K$.*

*Proof.* Let us rewrite the equation (4) in matrix form:

$$((x \circledast y)_1, (x \circledast y)_2, \ldots, (x \circledast y)_q) = (x_1, x_2, \ldots, x_q) \begin{pmatrix} y_{1\backslash 1} & y_{1\backslash 2} & \cdots & y_{1\backslash q} \\ y_{2\backslash 1} & y_{2\backslash 2} & \cdots & y_{2\backslash q} \\ \vdots & & \ddots & \vdots \\ y_{q\backslash 1} & y_{q\backslash 2} & \cdots & y_{q\backslash q} \end{pmatrix}.$$

One easily notes that the matrix rows are exactly the vectors $y^{\sigma_\ell}$, $\ell \in Q$. Hence, $x \circledast y = \sum\limits_{\ell \in Q} x_\ell y^{\sigma_\ell}$.

The lemma's conditions imply that for all $\ell \in Q$ we have $y^{\sigma_\ell} \in K$. Since $\sum\limits_{\ell \in Q} x_\ell = 1$ and $x_\ell \geqslant 0$, $\ell \in Q$, the vector $\sum\limits_{\ell \in Q} x_\ell y^{\sigma_\ell}$ is a convex combination of the vectors $y^{\sigma_\ell}$ and by convexity of $K$ we have $x \circledast y \in K$. The lemma is proved. □

Lemma 1 allows us to construct sets of distributions over $E$ that are preserved by $+$, yet it cannot be applied directly for constructing sets, preserved by $\times$, since this operation is not quasigroup on the entire set $E$.

**Lemma 2.** *Let $Q = E^*$ be the quasigroup with the $\times$ operation and let $\sigma_\ell$, $\ell \in Q$ be the corresponding set of permutations on $Q$ extended to $E$ by defining $\sigma_\ell(0) = 0$. Let $K$ be such a convex subset of the distribution space over $E$ that $(1, 0, \ldots, 0) \in K$ and for any $\ell \in Q$ and any $y \in K$ we have $y^{\sigma_\ell} \in K$. Then for any $y \in K$ and an arbitrary distribution $x$ over $E$ we have $x \otimes y \in K$.*

*Proof.* Similar to lemma 1, let us write the equations (2), (3) in matrix form, in terms of permutations $\sigma_\ell$:

$$((x\otimes y)_0,(x\otimes y)_1,\dots,(x\otimes y)_{k-1})=(x_0,x_1,\dots,x_{k-1})\begin{pmatrix}1 & 0 & \dots & 0\\ y_0 & y_{\sigma_1(1)} & \cdots & y_{\sigma_1(k-1)}\\ \vdots & \vdots & \ddots & \vdots\\ y_0 & y_{\sigma_{k-1}(1)} & \cdots & y_{\sigma_{k-1}(k-1)}\end{pmatrix}.$$

Since $\sigma_\ell(0)=0$ by definition, we have:

$$((x\otimes y)_0,(x\otimes y)_1,\dots,(x\otimes y)_{k-1})=x_0(1,0,\dots,0)+\sum_{\ell\in Q}x_\ell y^{\sigma_\ell}.$$

Due to $\sum\limits_{i\in E}x_i=1$ and $x_i\geqslant 0$, $i\in E$, the vector $x\otimes y$ is a convex combination of $(1,0,\dots,0)$ and the vectors $y^{\sigma_\ell}$, $\ell\in Q$, which, by lemma's conditions, all belong to $K$. By convexity of $K$ we obtain that $x\otimes y\in K$. □

Let us now prove a theorem that describes a class of convex sets preserved by both $+$ and $\times$ operations.

**Theorem.** *Let $\sigma^{\times}_\ell$, $\ell\in E^*$ be the permutations corresponding to the quasigroup $\langle E^*,\times\rangle$, with additional definition $\sigma^{\times}_\ell(0)=0$; let $\sigma^{+}_\ell$, $\ell\in E$ be the permutations corresponding to the quasigroup $\langle E,+\rangle$. Let $G$ be such a set of distributions that for any $g\in G$ and any $\ell\in E$ we have $g^{\sigma^{\times}_\ell}\in G$, $g^{\sigma^{+}_\ell}\in G$. Let $K$ be the convex hull of $G\cup\{(1,0,\dots,0)\}$ then for any $x,y\in K$ we have $x\oplus y\in K$ and $x\otimes y\in K$.*

*Proof.* Let us show that the set $K$ is preserved by the $+$ operation. Let $K'$ be the convex hull of $G$. Then the set $K$ is the convex hull of $K'\cup\{(1,0,\dots,0)\}$.

Consider distributions $x,y\in K$. By convexity there exist such $\alpha,\beta\in[0,1]$, that $x=\alpha(1,0,\dots,0)+(1-\alpha)x'$ and $y=\beta(1,0,\dots,0)+(1-\beta)y'$, where $x',y'\in K'$. Due to the bilinearity of the operation $x\oplus y$ (see (1)), and also the equalities $(1,0,\dots,0)\oplus y'=y'$ and $(1,0,\dots,0)\oplus x'=x'$ we obtain the equation

$$\begin{aligned}x\oplus y&=(\alpha(1,0,\dots,0)+(1-\alpha)x')\oplus(\beta(1,0,\dots,0)+(1-\beta)y')=\\&=\alpha\beta(1,0,\dots,0)+\alpha(1-\beta)y'+(1-\alpha)\beta x'+(1-\alpha)(1-\beta)(x'\oplus y').\end{aligned}$$

Since the set $K'$ satisfies lemma 1 conditions, we have $x'\oplus y'\in K'$. Then $x\oplus y$ is a convex combination of vectors from $K'\cup\{(1,0,\dots,0)\}$, and hence $x\oplus y\in K$.

The preservation of the set $K$ by the operation $\times$ follows directly from lemma 2. The theorem is proved. □

Let us now consider the construction of a preserved set $K$, that contains a given initial distribution $g$. In order to use the above theorem, we need to construct a set $G$, containing the distribution $g$ and invariant under permutation of coordinates by $\sigma_\ell^+$ and $\sigma_\ell^\times$, $\ell \in E$. One can easily see that a finite set $G$ suffices.

Let $S$ be the subgroup of the symmetric group, generated by all the permutations $\sigma_\ell^+, \sigma_\ell^\times$, $\ell \in E$. Let $G = \{g^s \mid s \in S\}$. The set $G$ is easily seen to contain $g$ and satisfy the theorem's conditions. Let further $K(g)$ be the convex hull of the set $G \cup \{(1, 0, \ldots, 0)\}$. According to the theorem, $K(g)$ is preserved by the operation $+$ and $\times$. Evidently, $g \in K(g)$ and $K(g)$ is a polytope whose vertices belong to the set $G \cup \{(1, 0, \ldots, 0)\}$.

**Statement 1.** *The polytope $K(g)$ containing the given distribution $g$ has at most $|S| + 1$ vertices.*

All of the distributions $g^s$ are vertices of the so-called permutohedron. In case all components of $g$ are distinct, all distributions $g^s$ are distinct as well, and as a corollary from Rado's results [4], none of these distributions belong to the convex hull of the others [5]. In other words, the polytope $K'$ that is the convex hull of the set $G$, has exactly $|S|$ vertices and only when considering the convex hull of the set $K' \cup \{(1, 0, \ldots, 0)\}$ can the number of vertexes get less than $|S|$.

Since $S$ contains no more than $k!$ elements, the following holds:

**Statement 2.** *The polytope $K(g)$ containing the given distribution $g$ has at most $k! + 1$ vertices.*

Note that one can define $+$ and $\times$ operations in such a way that the group $S$ coincides with the entire symmetric group. We shall now demonstrate it by defining in a specific way the operation $\times$.

Since $\sigma_\ell^\times(i) = l \backslash i$, the values of $\sigma_\ell^\times(i)$, $\ell, i \in E^*$ define in fact a quasigroup operation $\backslash$, which is the left inverse for the $\times$ operation. Let us define the operation $\ell \backslash i$ on the set $E^*$ for $\ell = 1, 2$ the following way.

| $\backslash$ | 1 | 2 | 3 | 4 | ... | $k-2$ | $k-1$ |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 1 | 3 | 4 | ... | $k-2$ | $k-1$ |
| 2 | 1 | 3 | 4 | 5 | ... | $k-1$ | 2 |

Then, by virtue of Hall's theorem [6], the operation $\backslash$ can be defined for other values of $\ell \in E^*$ so that it is a quasigroup operation on $E^*$, with the corresponding operation $\times$ being quasigroup too. Besides, one can easily check that the values of $\sigma_1^\times(i)$ and $\sigma_2^\times(i)$ correspond to permutations which generate the cycles $(1\,2)$ and $(1\,2\,\ldots\,k-1)$, and, hence (see, e.g. [7]), the entire subgroup of permutations that preserve the element $0 \in E$.

Note now, that since $+$ is a quasigroup operation on the set $E$, the set of values $\sigma_\ell^+(0)$, $\ell \in E$ coincides with $E$. Consequently, for any $j \in E$ there exists such a permutation $\sigma_\ell^+$, $\ell \in E$ that $\sigma_\ell^+(0) = j$.

Let us now show that an arbitrary permutation $s$ is generated by the above defined permutations $\sigma_\ell^+, \sigma_\ell^\times$, $\ell \in E$. Let $s(0) = j$. Then there exists a permutation $\tau = \sigma_\ell^+$ for which $\tau(0) = j$. By choice of $\tau$ we therefore have $(\tau^{-1}s)(0) = 0$, and consequently $\tau^{-1}s$ is a permutation generated by the above defined permutations $\sigma_\ell^\times$. Hence $s$ is generated by the permutations $\sigma_\ell^+, \sigma_\ell^\times$, $\ell \in E$.

Thus the group $S$ can coincide with the entire symmetric group on $E$. Yet, special properties of the operations $+$ and $\times$ may significantly simplify the structure of the group $S$ and consequently of the polytope $K(g)$.

Let $+$ and $\times$ be finite field addition and multiplication. Then the quasigroups $\langle E, + \rangle$ and $\langle E^*, \times \rangle$ are actually groups of orders $k$ and $k-1$, respectively. Applying the permutations $\sigma_\ell^\times$ to an element $i \in E$ is in fact multiplication of $i$ by $\ell^{-1}$, while permutations $\sigma_\ell^+$ add $-l$ to $i$. By virtue of distributive property for multiplication over addition we easily obtain that any combination of permutations reduces to one multiplication of $i$ by an element of the field and one addition of a field element, which implies that the group $S$ contains $k(k-1)$ elements.

**Statement 3.** *Let the operations $+$ and $\times$ be the addition and multiplication in the finite field of order $k$. Then the polytope $K(g)$ containing the given distribution $g$ has at most $k^2 - k + 1$ vertices.*

In author's earlier papers [1, 2] there have been constructed other sets preserved by $+$ and $\times$ operations. We shall now compare previously constructed families of sets with the ones that are subject of the present work.

The previously constructed family of polytopes was the intersection of the distribution space with the polytopes whose vertices have the following coordinates (where $a$ is a parameter, $0 \leqslant a \leqslant \frac{1}{k}$):

1. $(1, 0, \ldots, 0)$;
2. $(1/k - k(k-1)a^2, 1/k + ka^2, \ldots, 1/k + ka^2)$;
3. $(1/k, d_1, \ldots, d_{k-1})$,

where $d_1, \ldots, d_{k-1}$ are all the tuples with one $d_i$ possibly equal to zero and the others equal to $1/k \pm a$.

These polytopes are contained one within the other and every distribution, except those lying on the boundary of the distribution space, may belong to the boundary of at most one polytope from this family. For a given

distribution $g$ without zero components, the polytope from the family that has $g$ on its boundary is the minimal polytope containing $g$ in this family.

Let us consider the mutual positioning of the preserved sets depending on the distribution $g$ they are to contain, taking e. g. distributions over a 3-element finite field. The figures below represent the $(x_0, x_1, x_2)$ distribution space projected onto the $(x_1, x_2)$ plane.

Solid black lines represent the distribution space boundaries, while the dashed black lines are symmetry axes of this space. The red polygon is the one from the "old" family, while the green one is from the "new" family and constructed for the initial distribution $g$, marked by a green circle, lying on the "old" family polygon's boundary. The green dashed lines are sides of the polygon $K'$ that are not sides of the polygon $K$.

Depending on the position of the distribution $g$, the "new" polygon may be either entirely inside the "old" one (fig. 1) or contain the entire "old" polygon (fig. 2).

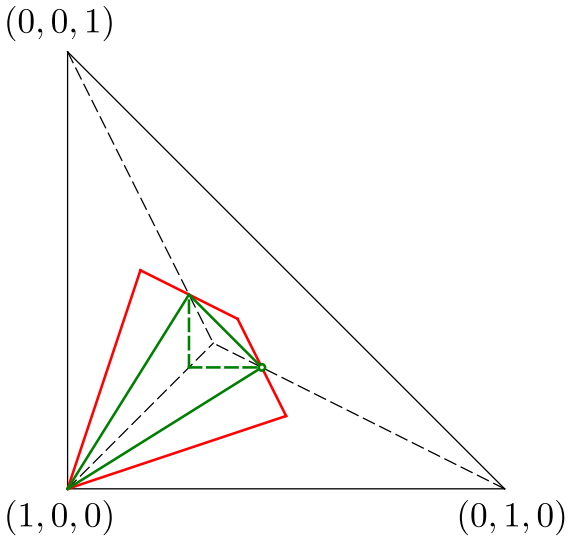


Fig. 1

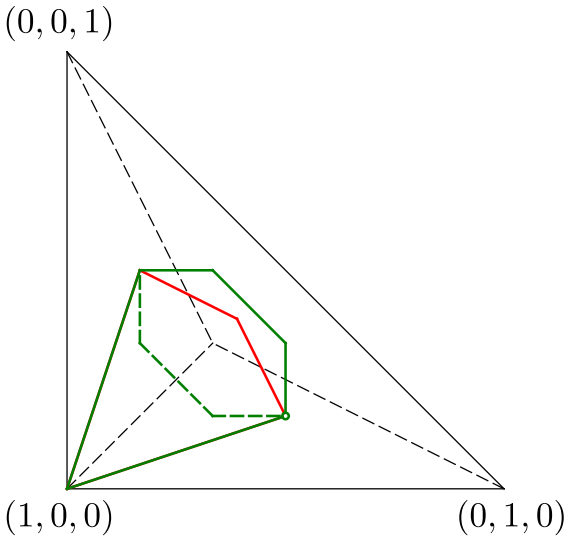


Fig. 2

Finally, for some positions of the distribution $g$ the "new" and "old" polygon have a non-empty symmetric difference (fig. 3), which, in a sense, illustrates the "independence" of the discussed preserved sets' families. Also in the case represented in fig. 3 the intersection of the "old" and "new" polygons provides another preserved set, not belonging to either of the constructed families.

Note that the previously constructed family did not cover the entire distribution space, whereas in the "new" family, for any given distribution, one finds a preserved polytope to contain it.

The author is deeply grateful to professor O. M. Kasim-Zade for fruitful discussions that contributed to writing the present paper.

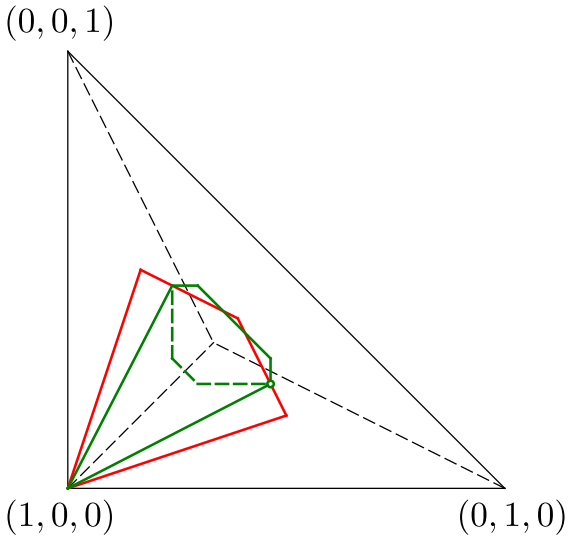


Fig. 3

# References

[1] 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

[2] Yashunsky A. D. On read-once transformations of random variables over finite fields // Discrete Mathematics and Applications. 2015. Volume 25, Issue 5. P. 311–321. http://dx.doi.org/10.1515/dma-2015-0030

[3] Belousov V. D. Foundations of the theory of quasi-groups and loops, Moscow, 1967. [In Russian]

[4] Rado R. An inequality // J. London Math. Soc. 1952. Vol. 27. P. 1–6.

[5] Yemelichev V. A., Kovalev M. M., Kravtsov M. K. Polytopes, Graphs and Optimisation. Cambridge University Press, New York, NY, USA. 1984.

[6] Hall M. An existence theorem for latin squares // Bull. Amer. Math. Soc. 1945. Vol. 51, N6. P. 387–388.

[7] Kalujnin L. A., Suschanskiy V. I. Transformations and permutations. Moscow, 1979. [In Russian]