On some group properties of the functional presentation of information

Anatolii M Kukartsev¹, Alexander A Kuznetsov¹, and Anna I Kuklina¹

¹Reshetnev Siberian State University of Science and Technology
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation
E-mail: amkukarcev@yandex.ru

Abstract. The paper provides an overview of research results on processing the information represented as Boolean functions. Actions of the hyperoctahedral group (or the Jevons group) are set on these functions. Information objects transformed by such actions have special frequency (entropy) characteristics. Such actions can be used to generate information messages with equal frequency and / or entropy characteristics. Preservation of the frequency characteristics of informational messages also allows us to solve one of the problems of classifying Boolean functions with respect to the Jevons group action. This problem has existed since the Harvard catalog was created and it has not been solved until the results of the studies covered in the paper were applied. Additionally, the possibilities of optimizing the calculation of actions tens and hundreds of times due to the properties of the elements of the Jevons group and modern processors are highlighted. This optimization allows the construction of information processing algorithms using the Jevons transformations for real data (commensurate with 1 MiB).

1. Introduction
Digital information is represented mainly in two ways: a combinational one and a functional one. The first way considers information as a combination of symbols of some alphabet, and the second one – as a set of values of a certain discrete function. Combinational methods of presenting information and the corresponding algorithms for its processing began to develop in the early twentieth century. These ways of presenting are usually associated with the works of K. Shannon [1], R.V. Hamming [2] and many other researchers. Functional methods of information presentation began to appear at the end of the 20th century in connection with the development of information technologies and natural need for qualitatively new methods of information processing. A series of JPEG [3] graphic data compression algorithms is an example of such an information processing method. Digital information is mapped to some function of two arguments. Further, the function is transformed and its parameters (Fourier coefficients) are rounded, coded, and their codes are compressed using combination methods.

Boolean functions (hereinafter – BF) [4] are naturally suitable for the functional representation of digital binary information. It is possible to injectively associate any binary vector (hereinafter – BV) consisting of zeros and / or units with a BV of length that is a multiple of two. The latter can be mutually associated with some Boolean function. For this, it is important to unambiguously order the domain of the definition of BF. This can be done by fixing the order of its arguments and by arranging, for example, lexicographically, its definition.
area accordingly. The BF itself can be described by the functional elements implementing it or by the formula [5].

The property of reducing the volume of information when using algorithms for graphic compression of the JPEG series is not the only advantage of functional presentation methods. Some transformations of information presented in the form of BF have special entropic properties, and also allow solving a number of complex mathematical problems related to the classification of BF with respect to the action of algebraic groups.

Two special groups can be distinguished among the various groups of actions on the set of BF: the set of negations and the set of permutations of the BF arguments, forming the Jevons group [6] or the hyperectahedral group [7]. The specified action is remarkable because it is neutral, that is, it does not affect the connections between functional elements of BF and does not change its formula. The Jevons-equivalent BF will have the same CNF and DNF [5].

Studying the functional presentation of information allows us to develop qualitatively new information processing algorithms. This paper aims to review the works in researching the properties of transformations associated with functional presentation of information. It covers the following tasks:

1. constructive presentation of the Jevons group for the development of information processing algorithms;
2. definition of actions of the Jevons group on sets of BF and BV as well as the analysis of their properties;
3. the use of functional information representation for solving the problem of BF classification regarding the action of Jevons group elements.

2. Definitions and notation
Hereinafter let \( n \) be a nonnegative integer, \( k = 2^n \), \( i, j \) are nonnegative integer indices (counters) not exceeding \( k \).

We define \( E = \{0, 1\} \) as a set consisting of two elements. We define the Cartesian product of this set by itself as \( E^n = E \times \cdots \times E \). BV will be an element of such a set. For its coordinates we will use the numeric L2R notation (left to right), i.e. larger coordinates are to the left. We denote an arbitrary element of the set as \( x \in E^n \), \( x = \{x_{n-1}, \ldots, x_i, \ldots, x_0\} \). For BF argument vectors we will also use the L2R notation.

The Boolean function of \( n \) arguments \( f(x_{n-1}, x_{n-2}, \ldots, x_1, x_0) \) implements the mapping \( E^n \to E \) [4]:

\[
y_f = \{f(11\ldots11), f(11\ldots10), \ldots, f(00\ldots01), f(00\ldots00)\} \\
(y_f)_j = f(x_{n-1}, x_{n-2}, \ldots, x_1, x_0), \quad j = \sum_{i=n-1}^0 x_i \cdot 2^i
\]

Let BF be given through the truth table [4]. If we unambiguously determine the order of the arguments, then each BF can be associated with a binary vector \( y_f \) (1) of length \( k \) (column of values).

We denote the variable inversion group (or the linear shift group [4]) by \( E_n = (E^n, \oplus) \). Variable permutation group (the symmetric group) is denoted by \( S_n \). The Jevons group is denoted as \( D_n = E_n \rtimes S_n \) [7]. Due to the specifics of the targets, we agree that the symmetric group acts on the set of numbers \( [0; n-1] \).

The set of Boolean functions of \( n \) arguments will be denoted as \( B^n \).

3. Constructive representation of the Jevons group for actions on sets of BV and BF
When developing information processing algorithms using the actions of the Jevons group on BV and BF there appear two problems:
1) non-unique specification of the action of the symmetric group on the BV set;
2) the specification of the homomorphism of the external semidirect product of the Jevons group.
In [8] and [9] these problems are addressed and their solutions are suggested.
It is important to distinguish between the group operation in the symmetric group and its action on BV. It is empirically shown that for tasks of the Jevons group action on BF it is convenient to define the homomorphism of the external semi direct product of the Jevons group from the symmetric group to the group of automorphisms of the variables inversion group through the very action of the element on BF. Such an action may not be specified in the only way. It is empirically shown that two sets of actions can be distinguished: type A and type B. Both types of actions are expressed through each other. When the action of a Jevons group element takes place on BV, type A is preferable [8], but when it takes place on BF then type B is preferable [8]. It is therefore impossible to single out one type of action as the main one, and the second as reducible to it. At the same time the developers can choose the type of action at their discretion depending on the problem to be solved.

The operation of A type of an element of the group \( \pi \in S_n \) on BV \( x \in E^n \) will be called the calculation of the result \( x' \in E^n \): \( x' = x^\pi \) according to the following rule: "old" indexes are in the top substitution line, and "new" indexes are at the bottom one, or in a symbolic form:

\[
x'_{\pi(i)} = x_i. \tag{1.A}
\]

The operation of B type of an element of the group \( \pi \in S_n \) on \( x \in E^n \) will be called the calculation of the result \( x' \in E^n \): \( x' = x^\pi \) according to the following rule: "new" indexes are in the top substitution line, and "old" indexes are at the bottom one, or in a symbolic form:

\[
x'_i = x_{\pi(i)}. \tag{1.B}
\]

The second problem is the very way of setting the Jevons group. It is that the external semidirect product of groups can be set in many ways and as a result can give different (non-isomorphic, for example, direct product) groups [4]. In [8] it is proposed to isomorphically embed the Jevons group into a substitution subgroup \( \beta_n < S_k \) acting on the set of rows of the truth table of BF. Such a group is decomposed into an inner semidirect product, whose homomorphism is set in a natural way by conjugations. From where we get two representations of Jevons group for \( z_0, z_1 \in E_n \) and \( \pi_0, \pi_1 \in S_n \):

\[
(z_0 \pi_0)(z_1 \pi_1) = (z_0 z_1^{\pi_0^{-1}} \pi_0 \pi_1) \tag{2.A}
\]

\[
(z_0 \pi_0)(z_1 \pi_1) = (z_0 z_1^{\pi_1^{-1}} \pi_1 \pi_0) \tag{2.B}
\]

All necessary evidence and examples are given in [8] and [9].

4. Frequency properties of the action of the Jevons group on BF
The frequency characteristics of BV specifically depend on the actions of the Jevons group elements on the corresponding Boolean functions. These properties can form the basis of the message generation methods possessing the same frequency and spectral distributions in all their allowable alphabets simultaneously. We present the necessary series of definitions from [10].

**Definition 1.** The alphabet \( A_i \) is a set constructed as a Cartesian product \( E^{2^i} \).

**Definition 2.** An alphabet symbol is an element of the alphabet \( A_i \) encountered in the vector \( y_f \).

BV \( y_f \) can be divided into characters in any of the alphabets \( A_i \), where \( i \) runs through all the values of \([0; n]\). In this case, the division starts from the first value of the vector \( y_f \) and the
The length of the BV \( y_f \) (the number of characters) in each of the alphabets is calculated as \( l_i = 2^{n-i} \).

**Definition 3.** Symbol frequency is the number of times that a given symbol has been encountered from the \( A_i \) alphabet in the \( y_f \) vector.

**Definition 4.** The frequency distribution of the BV \( y_f \) (spectrum) over the alphabet \( A_i \) is the ratio \( Q_i(y_f) \subset A_i \times [0;k] \), i.e. a set of symbol – frequency pairs.

**Definition 5.** The spectral distribution of the BV \( y_f \) over the alphabet \( A_i \) is the ratio \( R_i(y_f) \subset [0;k] \times [0;k] \) (the derived set from \( Q_i(y_f) \)), the elements of which show how often the frequencies in the vector \( y_f \) are repeated. First the frequency from \( Q_i(y_f) \) and then the number of various characters with this frequency in the vector \( y_f \) is indicated in the relationship element.

We define \( c_{n-1}, \ldots, c_0 \in E^n \) – the generating set of the group \( E_n \), and each \( c_i \) has the value 1 at the position of \( i \), and the value 0 on the other positions.

**Theorem 1.** (On the invariance of frequency spectra under the action of \( E_n \)) If the element \( c_i \) acts on the BF \( f \in B(n) \), then the frequency distributions of the BV \( y_f \) are invariant with respect to this action for the alphabets \( A_i \) : \( i' \leq i, i \in [0;n-1] \), and the spectral distributions of the BV \( y_f \) are invariant with respect to the same action for the alphabets \( A_i \).

**Theorem 2.** (On the invariance of frequency spectra under the action of \( S_n \)) If the transposition \( (i,j) \in S_n, i, j \in [0;n-1] : i < j \) acts on \( f \in B(n) \), the frequency distributions of BV \( y_f \) are invariant with respect to this action for alphabets \( A_i \) : \( i' \leq i \), and the spectral distributions of BV \( y_f \) are invariant with respect to the same action for alphabets \( A_i' \) and \( A_j' : j' > j \).

Entropy is a function that depends only on frequencies, and not on frequency distribution symbols. The value of frequencies and their number are determined by the spectral distribution, so the following consequences are true.

**Corollary 1.** The entropy of BV \( y_f \) is invariant in all alphabets \( A_i, i \in [0;n-1] \) with respect to the action of any element \( E_n \) over BF \( f \).

**Corollary 2.** The entropy of BV \( y_f \) is invariant for alphabets of indices up to \( i \) inclusive and greater than \( j \) with respect to the action of the transposition \( (i,j), i, j \in [0;n-1] : i < j \) of group \( S_n \) over BF \( f \).

In [10] all the necessary descriptions and proofs of the theorems are given and specific decompositions are introduced: a monotone decomposition of an element of a substitution group and a canonical decomposition of an element of the Jevons group.

5. **Solution of the problem of BF classifying with respect to the Jevons group action**

Let \( f,g \in B(n) \). We denote the negation of the arguments by \( z \in E_n \) and the permutation of the arguments by \( \pi \in S_n \). Both the negation and \( f \) or permutation of the arguments are denoted by \( (z\pi) \in D_n \), then the basic equation of the action of a Jevons group element on a BF with respect to the unknown \( (z\pi) \) is denoted as:

\[
f^{(z\pi)} = g
\]

Equation (3) describes the problem of classifying the BF with respect to the Jevons group action. The specified task is set in [11]. It admits a trivial solution with complexity \( O(2^n \cdot n!) \), but such a solution is already inefficient for \( n > 4 \). The solution of this problem is closely related to the notion of an invariant of the group acting on the set BF [4]. S. Golomb proposed the full invariant [12], but the complexity of its calculation as well as the trivial solution is
exponential. E.A. Yakubaytis also proposed the invariant [13], but it is not complete. As a result the formulated problem is difficult to solve. Due to lack of solutions, besides the trivial transformation of information by negation and \( f \) or permutations of BF arguments, it is used as a cryptographic primitive for encrypting information by algorithms based on controlled operations in which an element of the Jevons group is the encryption key [14].

Consideration of the specified in (3) BFs as information objects allows us to construct an algorithm for solving equation (2) in polynomial time \( O(n^2 + n) \). The correctness of the algorithm is proved by the following theorem, described in [15].

**Theorem 3.** (On calculating the zero action) The set \( H_0 \) coincides with the set of all solutions of the equation \( f(zw) = g \) and can be calculated as \( H_{i+1}' = \left\{ j_1 < n \bigcup_{j_i = i} (e_E(i, j_i)) H_i \bigcup_{j_i = i} (c_i(i, j_i)) H_i \right\} \) in \( n \) steps in series for \( 0 \leq i < n \) and \( H_{i+1} = \left\{ h \in H_{i+1}' \mid Q_{i+1}(f) = Q_{i+1}(g) \right\} \), starting with \( H_0 = \{(e_E \varepsilon S)\} \).

Modern PCs are mainly focused on processing computer words, rather than individual bits. Jevons transformations are remarkable in that their action can be localized in a machine word. In fact, this means speeding up the computational process equal to the number of bits in a machine word. So some extensions of Intel processors have 512 bit registers. This allows increasing optimization hundreds of times. In [16] such methods for optimizing calculations with the necessary evidence are described.

**References**

[1] Shannon K 1963 *Works on information theory and cybernetics: Trans. from English* ed. R. L. Dobrushkin and O. B. Lapunova. From prev. A. N. Kolmogorov (Moscow: Publishing house of foreign literature) – 829 p. (In Russ)

[2] Hamming R V 1983 *Coding Theory and Information Theory: Trans. from English* (Moscow: Radio and communication) – 176 p. (In Russ)

[3] Salomon D 2004 *Compression of data, images and sound. Trans. from English* V.V. Chepyzhov (Moscow: Technosphere) – 368 p. (In Russ)

[4] Logachev O A, Salkinov A A, Yasnchenko V V 2004 *Boolean functions in coding theory and cryptology* (Moscow: ICMNO) – 470 p. (In Russ)

[5] Yablonsky S V 1986 *Introduction to discrete mathematics: textbook for universities. – 2 ed., correct. and add* (Moscow: Science. Ch. ed. Phys.-Mat. lit.) – 384 p. (In Russ)

[6] Jevons S 1881 *Fundamentals of Science* (Saint-Petersburg)

[7] Young A A 1930 *Quantitative substitutional analysis* Proc. London Math. Soc. 31 273–388

[8] Kukartsev A M, Kuznetsov A A 2015 *Constructive Representation of the Jevons Group for Engineering Solutions of Information Processing Software Engineering* 11 (Moscow: New Technology) 25–33 (In Russ)

[9] Kukartsev A M, Kuznetsov A A 2016 *On the actions of the Jevons group on sets of binary vectors* and *Boolean functions for engineering information processing solutions Software Engineering* 7 (Moscow: New Technology) 29–36 (In Russ)

[10] Kukartsev A M 2016 *On the frequency properties of actions of the Jevons group on Boolean functions Software Engineering* 7 (Moscow: New Technology) 515–521 (In Russ)

[11] Glukhov M M, Remizov A. B., Shaposhnikov V. A. 1988 *Review on the theory of k-valued functions. Part 1. Reference book. Ed. N.P. Yemelyanov.* Order number 163f (Moscow: Typography of military unit 33965, 125040, Moscow A–40) – 153 p. (In Russ)

[12] Golomb S W 1959 *On classification of Boolean functions IRE, Trans.circuit theory. Spec.Suppl.* 6 176–186

[13] Yaubaytis E A 1974 *Subclasses and classes of Boolean functions* (Riga: Zinatne) 1–8 (In Russ)

[14] Shnipirov A N 2008 *Synthesis and analysis of high-speed symmetric cryptosystems based on managed operations* Information Technology 137 (Moscow: Information Technology) 36–41 (In Russ)

[15] Kukartsev A M, Kuznetsov A A 2017 On the effective algorithm for solving the equation of the Jevons group action on Boolean functions *Software Engineering* 8 (Moscow: New Technology) 76–87 (In Russ)

[16] Kukartsev A M, Kuznetsov A A 2017 *On the Equimorphic Computation of the Jevons Group Element Action over Boolean Functions, Software Engineering* 8 (Moscow: New Technology) 300–309 (In Russ)