UDC 519.711/.72

A.Ya. Beletsky, Dr. Sci. Tech.
(National Aviation University, Ukraine)

Multidimensional Gray transformations in cryptographic applications

By analogy with the discrete Fourier transform algorithms, variants of constructing the methods of discrete Gray transformations of one-dimensional (vector data transformations), two-dimensional (transformations on the plane), and three-dimensional (spatial transformations) of digital data are considered.

Gray's transformations (GT) are treated further as a generalization of the concept of Gray codes (CG). The Gray codes, proposed in 1953 in response to requests for engineering practice regarding the construction of optimum ambiguity errors in the angle-code converters [1], at the dawn of their appearance attracted the attention not only of mathematicians but also of a wide range of developers a variety of electronic equipment. A distinctive feature of the Gray codes is that in the binary system, when changing from an image of one number to an image of a neighboring higher or next minor number, the numbers (1 to 0 or vice versa) change only in one digit of the number. Such codes are referred to a group of binary codes with a single Hamming distance [2]. Gray's code is not the only one in this group, but its use in communication systems, analog-digital transformations and in other fields of science and technology became preferable for a number of reasons.

Apparently, they turned out to be out of the field of view, both for mathematicians and for developers of electronic equipment, of the possibility of constructing codes that are opposite in direction to the formation of classical CG. In the known (classical) scheme, the process of forming forward and reverse codes develops from left to right. In this case, the highest (left) digit of the converted number does not change under both forward and reverse transformations. At the same time, it is possible to construct a scheme of transformation in the general case of m-ary codes, which is inverse in the direction of formation of the classical (left-handed) PG. In this class of right-handed transformations, the value of the lower (right) digit of the converted number remains unchanged under forward and backward transformations.

The combination of left- and right-hand Gray transformations (both direct and inverse) together with the inverse code permutation operation led to the possibility of constructing combined or composite Gray codes (CGC) [3]. The application of the SKG proved to be very successful in problems of determining the structure and interrelation of symmetric systems of Walsh functions, discrete Vilenkin-Krestenson functions, cryptography, coding and other applications [4]. The simplest physical essence of classical direct GT is revealed by its structural-logic scheme, an example of which for a four-point transformation of binary data is shown in Fig. 1.

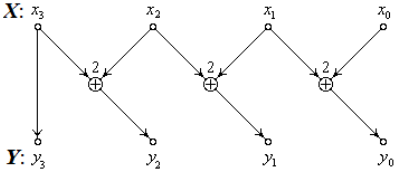


Fig. 1. Structural-logical scheme of the formation algorithm
Gray Direct Left-side Binary Code

$$\begin{aligned} y_3 &= x_3; \\ y_2 &= x_3 + x_2; \\ y_1 &= x_2 + x_1; \\ y_0 &= x_1 + x_0. \end{aligned} \qquad (1) \qquad\qquad \begin{aligned} x_3 &= y_3; \\ x_2 &= y_3 + y_2; \\ x_1 &= y_3 + y_2 + y_1; \\ x_0 &= y_3 + y_2 + y_1 + y_0. \end{aligned} \qquad (2)$$

Circuit shown in Fig. 2 displays the inverse transformations (2).

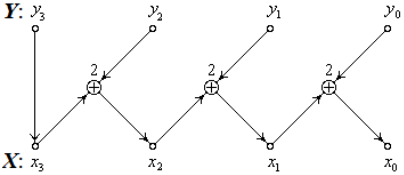
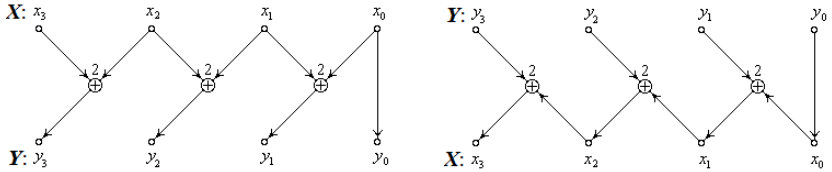


Fig. 2. Structural-logical scheme of the formation algorithm
Gray Backward Left-side Binary Code

From the systems of equations (1) - (2) it can be seen, that the GT process develops from left to right. For this reason, the classical Gray transformations are called left-handed. Alternative classical SGs are right-handed transformations, the method of formation of which is illustrated in Fig. 3.



a) direct conversion *b*) backward conversion

Fig. 3. Structural-logical scheme of the formation algorithm
Gray Right-side Binary Code

Algebraic equations corresponding to the algorithms for the formation of right side Gray codes (Fig. 3) are as follows:

$$y_3 = x_3; \qquad x_3 = y_3;$$
$$y_2 = x_3 + x_2; \qquad x_2 = y_3 + y_2;$$
$$y_1 = x_2 + x_1; \qquad x_1 = y_3 + y_2 + y_1;$$
$$y_0 = x_1 + x_0. \qquad x_0 = y_3 + y_2 + y_1 + y_0.$$

We reduce the main Gray operators to Table. 1, by adding to it a number of additional operations.

Table 1.

A group of simple Gray operators

Notation operator	The operation to be performed
0	Preservation of source data
1	Inverse permutation
2	Direct left-side GT
3	The reverse left-side GT
4	Direct right-side GT
5	The reverse right-sided GT
6	Cyclic shift one digit to the right
7	Cyclic shift one digit to the left

The matrix forms of third-order operators are shown in Table 2.

Table 2.

Matrix forms of simple Gray operators

$0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$	$4 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$	$6 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$
$1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$3 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$	$5 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$	$7 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

The operators of Gray presented in Table. 1 and 2, as well as the CGC compiled on their basis, is sufficient for constructing a complete system consisting of 28 Walsh functions $\boldsymbol{W}$ of the eighth order and objectively associated with the third-order indicator matrices (MI).

Indicator matrices $\boldsymbol{J}_w$ of systems of Walsh functions $\boldsymbol{W}$ are right-sided symmetric (0, 1)-matrices (that is, matrices symmetric with respect to the auxiliary diagonal), nondegenerate over F_2.

Any Walsh system of order N can be formed by an appropriate permutation of rows (or columns) of the Walsh-Paley matrix $\boldsymbol{P}$. The line number k_w of the system $\boldsymbol{W}$, into which the row k_p of the Paley matrix moves is found by the formula:

$$k_w = k_p \cdot \boldsymbol{J}_w, \quad k_p = \overline{0, N-1},$$

from which, as a consequence, follows:

Assertion 1: An arbitrary Walsh system $\boldsymbol{W}$ of order N is uniquely determined by its indicator matrix $\boldsymbol{J}_w$ of order n.

We formulate a number of fundamental propositions, which form the basis of the construction of the theory of GT.

Axiom 1. An arbitrary Gray code (simple or composite) is the generator of the multiplicative cyclic group.

Axiom 2. The operator $\perp$ of right-sided transposition performs a rotation of the square matrices relative to the auxiliary diagonals.

Lemma 1. The composite Gray code $\boldsymbol{G} \cdot \boldsymbol{G}^T$, where $\boldsymbol{G}$ is the matrix form of an arbitrary CGC, corresponds to a left-sided symmetric matrix.

Evidence. From that $(\boldsymbol{A} \cdot \boldsymbol{B})^T = \boldsymbol{B}^T \cdot \boldsymbol{A}^T$ it follows, that $(\boldsymbol{G} \cdot \boldsymbol{G}^T)^T = (\boldsymbol{G}^T)^T \cdot \boldsymbol{G}^T = \boldsymbol{G} \cdot \boldsymbol{G}^T$ which is true, if only $\boldsymbol{G} \cdot \boldsymbol{G}^T$ - a left-sided symmetric matrix. ▪

Lemma 2. A right-sided transposition $\perp$ of the CGC is equivalent to inversion of this code, which reduces to reversing the order of the simple Gray codes. ■

In fact, $(g_2 \cdot g_1)^{\perp} = g_2{}^{\perp} \cdot g_1{}^{\perp} = g_2 \cdot g_1$ since any simple Gray code g is symmetric with respect to the auxiliary diagonal.

Lemma 3. A symmetric matrix of a transformation corresponds to a symmetric CGC.

*Evidence***.** By definition, a symmetric composite is a code $\boldsymbol{G}_s = \boldsymbol{G} \cdot \omega \cdot \boldsymbol{G}^{\perp}$, in which $\boldsymbol{G}$ is an arbitrary SCG, and ω – a kernel that is a simple or symmetric Gray compound code. We have

$$\boldsymbol{G}_s^{\perp} = (\boldsymbol{G} \cdot \omega \cdot \boldsymbol{G}^{\perp})^{\perp} = (\boldsymbol{G}^{\perp})^{\perp} \cdot \omega^{\perp} \cdot \boldsymbol{G}^{\perp} = \boldsymbol{G} \cdot \omega \cdot \boldsymbol{G}^{\perp} = \boldsymbol{G}_s. \blacksquare$$

Assertion 2: There exist CGC, forming cyclic groups of maximal order L, (*m*-sequence), defined by the relation $L = 2^n - 1$, where is the order n of indicator matrices of simple codes, which are components of the CGC.

We say that those CGC are primitive with respect to the IM order n, the sequence of powers of which, starting with the zero degree, forms an *m*-sequence. sequences also generate individual unbalanced SCGs. As an example, we indicate the code $\boldsymbol{G} = 1 \cdot g$, in which g - one of the simple codes with identifiers, presented in Table. 2. Additional information on non-symmetric primitive compound codes is given in Table. 3.

Table 3.

Primitive Gray compound codes

$n = 16$	$n = 32$	$n = 64$	$n = 128$	$n = 256$
2224244	2225355	2252435	2425535	22533435
2225524	2225535	2433435	2433534	22534335
2252435	2244424	2435225	2435334	24334225
2255535	2255524	2522534	22524224	25224334
2433435	2442224	25224334	22533334	2222535224

By analogy with the term "discrete Fourier transforms" (DFT), we introduce the term discrete Gray transformations (DGTs), dividing them into one-dimensional, two-dimensional, and three-dimensional DGT. The most useful is still a generalization to the case of two dimensions, since it is widely used in image processing.

Like a two-dimensional DFT, a two-dimensional DGT can be calculated sequentially in two dimensions. To this end, it is sufficient to define one-dimensional DGTs of all image lines, and then calculate the one-dimensional DGT s of all columns in the resulting "image". In this case, the results of one-dimensional DGTs should be written down to the place of the initial data for these DGTs.

Conclusions

Despite more than half a century (1953) history of its discovery, Gray's codes are still far from complete. The additions of the classical Gray codes proposed in this paper by the so-called right-handed and composite codes significantly extend the boundaries of the application of Gray's transformations in many fields of science and technology.

References

1. Gray F. Pulse code communication. — Pat. USA, # 2632058, 1953.
2. Hamming R. V. Coding and Information Theory. Prentice-Hall, 1980. — 176 p.
3. Белецкий А. Я. Коды Грея. — К.: Изд-во «КИТ», 2002. — 150 с.
4. Белецкий А. Я. Комбинаторика кодов Грея. — К.: Изд-во «КВИЦ», 2003. – 508 с.