БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
BELARUSIAN STATE UNIVERSITY

ОБЪЕДИНЕННЫЙ ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК БЕЛАРУСИ
UNITED INSTITUTE OF PROBLEMS OF INFORMATICS
OF NATIONAL ACADEMY OF SCIENCE OF BELARUS

НАУЧНО-ТЕХНОЛОГИЧЕСКАЯ АССОЦИАЦИЯ «ИНФОПАРК»
SCIENTIFIC AND TECHNOLOGICAL ASSOCIATION «INFOPARK»

ЕВРАЗИЙСКАЯ АССОЦИАЦИЯ УНИВЕРСИТЕТОВ
EUROASIAN UNIVERSITIES ASSOCIATION

МЕЖДУНАРОДНЫЙ КОНГРЕСС ПО ИНФОРМАТИКЕ: ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Материалы международного научного конгресса

**Республика Беларусь,
Минск, 24–27 октября 2016 г.**

INTERNATIONAL CONGRESS ON COMPUTER SCIENCE: INFORMATION SYSTEMS AND TECHNOLOGIES

Proceedings of the International Scientific Congress

**Republic of Belarus,
Minsk, October 24–27, 2016**

**МИНСК
БГУ
2016**

УДК 37:004(06)

Международный конгресс по информатике: информационные системы и технологии = International Congress on Computer Science: Information Systems and Technologies [Электронный ресурс] : материалы междунар. науч. конгресса, Республика Беларусь, Минск, 24–27 окт. 2016 г. / редкол.: С. В. Абламейко (гл. ред.), В. В. Казаченок (зам. гл. ред.) [и др.]. – Минск : БГУ, 2016.
ISBN 978-985-566-369-1.

Представлены материалы международного научного конгресса, в которых рассматриваются следующие темы: аэрокосмические информационные и телекоммуникационные системы и технологии; биоинформатика и приложения; высокотехнологичная образовательная среда (педагогические аспекты); геоинформационные системы; защита информации и компьютерный анализ данных; интеллектуальные информационные системы; информационно-коммуникационные системы; цифровые медиа технологии; информационные системы и технологии обеспечения научно-образовательной среды; компьютерные технологии в приборостроении; параллельная и распределенная обработка данных, вычислительные системы и сети; программная инженерия; распознавание образов, информационные системы управления; теоретическая информатика.

УДК 37:004(06)

ISBN 978-985-566-369-1

ПОСТРОЕНИЕ ОБРАТИМЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ С КООРДИНАТАМИ, ЗАВИСЯЩИМИ ОТ ЗАДАННОГО ЧИСЛА ПЕРЕМЕННЫХ

И. А. Панкратова

Томский государственный университет
Томск, Россия
e-mail: *pank@isc.tsu.ru*

Предлагается алгоритм построения обратимых векторных булевых функций, каждая координата которых существенно зависит от заданного числа переменных.

Ключевые слова: векторная булева функция; обратимая функция.

CONSTRUCTION OF INVERTIBLE VECTORIAL BOOLEAN FUNCTIONS WITH COORDINATES DEPENDING ON GIVEN NUMBER OF VARIABLES

I. A. Pankratova

Tomsk State University
Tomsk, Russia

An algorithm for constructing invertible vectorial Boolean functions, any coordinate of which essentially depends exactly on a given number of variables, is proposed.

Keywords: vectorial Boolean functions; invertible function.

INTRODUCTION

For constructing cryptosystems, we often need vectorial Boolean functions that have to be invertible. Particularly such functions are used in symmetric iterative block ciphers SIBCiphers [1]. These functions must be effectively calculated. For this purpose, a restriction is often imposed on the number of essential variables of their coordinates.

For integers n, m, and k, let $\boldsymbol{F}_{n,\,m,\,k}$ be the set of all invertible functions F: $\{0, 1\}^n \to \{0, 1\}^m$, where $F = (f_1 \dots f_m)$ and any coordinate function f_i: $\{0, 1\}^n \to \{0, 1\}$, $i = 1, \dots, m$, essentially depends exactly on k arguments, $1 \le k \le n$.

The following simple properties hold [2].

1. If $\boldsymbol{F}_{n,\,m,\,k}$ is not empty, then $m \ge n$.

2. If $F \in \boldsymbol{F}_{n,\,n,\,k}$, then F is a bijection on $\{0, 1\}^n$, and all its coordinate functions are balanced.

3. If $F = (f_1 \dots f_i \dots f_m) \in \boldsymbol{F}_{n,\,m,\,k}$, then $F' = (f_1 \dots \neg f_i \dots f_m) \in \boldsymbol{F}_{n,\,m,\,k}$ for any $i = 1, \dots, m$.

4. If $\boldsymbol{F}_{n,\,m,\,k}$ is not empty, then $\boldsymbol{F}_{n,\,t,\,k}$ is not empty for any $t \ge m$.

5. $\boldsymbol{F}_{n,\,n,\,2}$ is empty for any $n \geq 2$.
6. If $\boldsymbol{F}_{n,\,m,\,k}$ is not empty, then $\boldsymbol{F}_{n+1,\,m+1,\,k}$ is not empty.
7. $\boldsymbol{F}_{n,\,m,\,2}$ is not empty for any $m > n \geq 2$.
8. $\boldsymbol{F}_{n,\,m,\,3}$ is not empty for any $m \geq n \geq 3$.

CONSTRUCTING FUNCTIONS FROM $\boldsymbol{F}_{n,n,n}$

Let us consider a method for constructing bijections on the set $\{0, 1\}^n$ with coordinates essentially depending on all n variables (i. e., functions from the class $\boldsymbol{F}_{n,\,n,\,n}$). There are some useful statements.

Statement 1. Let $f(x_1, ..., x_n)$ be a Boolean function essentially depending only on x_i, that is, $f = x_i$ or $f = \neg x_i$. Then, if we invert two values $f(a)$ and $f(b)$ where a and b differ only in i-th component, we will obtain the function g essentially depending on all n variables.

Proof. Clearly, the new function g essentially depends on x_i.

Take any j in $\{1, \ldots, n\}\backslash\{i\}$. For definiteness, let $j < i$, $a = (a_1 \ldots a_j \ldots a_i \ldots a_n)$, $b = (a_1 \ldots a_j \ldots \neg a_i \ldots a_n)$. Due to equality $f(a_1 \ldots a_j \ldots a_i \ldots a_n) = f(a_1 \ldots \neg a_j \ldots a_i \ldots a_n)$, we have the following:

$$g(a_1 \ldots a_j \ldots a_i \ldots a_n) = \neg f(a_1 \ldots a_j \ldots a_i \ldots a_n) = \neg f(a_1 \ldots \neg a_j \ldots a_i \ldots a_n) = \neg g(a_1 \ldots \neg a_j \ldots a_i \ldots a_n).$$

It implies the essential dependence of function g on its j-th variable. The statement is proved.

The following algorithm is based on this statement.

Algorithm for constructing some function from $\boldsymbol{F}_{n,\,n,\,n}$

1. Let F be the identity permutation on the set $\{0, 1\}^n$, i. e. $F(a) = a$ for any a in $\{0, 1\}^n$;

   $M := \{0, 1\}^n$.

2. For $i = 1, 2, \ldots, n$:
   2.1. choose a pair of tuples a, b in M, differing only in the i-th component;
   2.2. swap the values $F(a)$ and $F(b)$;
   2.3. $M := M\backslash\{a, b\}$.

3. Return F.

Prove the algorithm performance.

Statement 2. For any $n > 2$, in step 2.1 of the algorithm we always can choose a proper pair of tuples.

Proof. Let $M' = \{0, 1\}^n\backslash M$. Notice, that after i iterations in step 2 we have $|M'| = 2i$, $|M| = 2^n - 2i$. Suppose there are not tuples in M differing only in the $(i+1)$ – th component. Then, for any a in M, its neighbor (differing from a) by the $(i+1)$ – th component is in M', which implies $|M| \leq |M'|$, i. e. $2^n \leq 4i$, that is impossible for any $n > 3$ and $i < n$.

It remains to consider the case $n = 3$.

Suppose that in the first iteration the tuples $a = cde$ and $b = \neg cde$ were chosen for some c, d, e in $\{0, 1\}$. Then in the second iteration we may choose $a = cd\neg e$, $b = c\neg d\neg e$ (and $M = \{\neg c\neg de,\ \neg cd\neg e,\ \neg c\neg d\neg e,\ cd\neg e\}$) or $a = \neg cd\neg e$, $b = \neg c\neg d\neg e$ (and $M = \{\neg c\neg de,$ $cd\neg e,\ c\neg d\neg e,\ c\neg de\}$). In both cases we have the pair of tuples in M differing only in the third component; $a = \neg c \neg de$, $b = \neg c \neg d \neg e$ in the first case and $a = c \neg d \neg e$, $b = c \neg de$ in the second case. The statement is proved.

Thus, we have the following: $\boldsymbol{F}_{n,\,n,\,n}$ is not empty for any $n > 2$. Hence, taking into account the properties 4 and 6, we get

Statement 3. The class $\boldsymbol{F}_{n,\,m,\,k}$ is not empty for any n, m, k, such that $m \geq n \geq k \geq 3$.

Statement 3 and property 7 give the complete decision of the existence problem for functions in class $\boldsymbol{F}_{n,m,k}$.

Unfortunately, the algorithm does not possess the completeness property, i. e. it can not costruct all fuctions in $\boldsymbol{F}_{n,\,n,\,n}$, even if we change the step 1 to the following more general one.

1'. Let F be a permutation on the set $\{0, 1\}^n$, such that any coordinate function of F essentially depends only on one variable (not obligatorily the i-th coordinate – on the i-th variable; but, of course, F depends on all n variables).

For example, the function F: $\{0, 1\}^3 \to \{0, 1\}^3$ with the value vector $F = (0, 1, 2, 6, 7, 4, 5, 3)$ having coordinate functions $f_1 = x_1 + x_2x_3$, $f_2 = x_1 + x_2 + x_1x_3$, $f_3 = x_1 + x_3 + x_2x_3$, is in $\boldsymbol{F}_{3,\,3,\,3}$ and can not be built by the algorithm above, because it is an even permutation (obtained from identity permutation by four transpositions (011,110), (011,101), (011,100), (011,111)), while the algorithm for $n = 3$ produces only odd permutations.

Notice, that the change of step 1 by 1' does not affect the permutation parity, because the invertion of i-th variable of n-ary function F is achieved by 2^{n-1} transpositions of value vector: for example, for $i = 1$, we need to exchange values $F(0, a_2, ..., a_n)$ and $F(1, a_2, ..., a_n)$ for any $(a_2, ..., a_n)$ in $\{0, 1\}^{n-1}$. The swapping of variables x_i and x_j is achieved by 2^{n-2} transpositions: for $i = 1$, $j = 2$, we need to exchange values $F(0, 1, a_3, ..., a_n)$ and $F(1, 0, a_3, ..., a_n)$ for any $(a_3, ..., a_n)$ in $\{0, 1\}^{n-2}$. Both numbers (2^{n-1} and 2^{n-2}) are even for $n > 2$.

Direction for further research are the building an algorithm that can construct any function in $\boldsymbol{F}_{n,\,m,\,k}$ and the investigation of cryptographic properties of functions constructed with the algorithm, such as correlation and algebraic immunity, nonlinearity, propagation criterion, and so on.

LITERATURE

1. Agibalov G. P. SIBCiphers – symmetric iterative block ciphers composed of Boolean functions depending on small number of variables // Prikladnaya Diskretnaya Matematika. Supplement. 2014. № 7. P. 43–48.
2. Pankratova I. A. On the invertibility of vector Boolean functions // Prikladnaya Diskretnaya Matematika. Supplement. 2015. № 8. P. 35–37.