Действительно, пусть $\overline{x}_2 \preceq \overline{x}_1$. Тогда по определению
1) если $\|\overline{x}_1\| > k$, то $\overline{F}_k(\overline{x}_1) = \overline{1}$ и, следовательно, $\overline{F}_k(\overline{x}_2) \preceq \overline{F}_k(\overline{x}_1)$;
2) если $\|\overline{x}_1\| \leqslant k$, то $\|\overline{x}_2\| < k$ и $\overline{F}_k(\overline{x}_2) = \overline{0}$. Следовательно, $\overline{F}_k(\overline{x}_2) \preceq \overline{F}_k(\overline{x}_1)$.

Из леммы 4 следует, что максимальный период множества $\mathbf{БД}(\overline{F}_k, n, \overline{x})$ достигается при таком $\overline{x}$, что $\|\overline{x}\| = k$, где $k = \left[\frac{n}{2}\right]$. В этом случае период равен $\mathbf{C}_n^{\left[\frac{n}{2}\right]}$.

$$\overline{G}_k(\overline{x}) = \overline{F}_k(\overline{x}) \oplus \sum_{i=1}^{\mathbf{C}_n^k - q} (\overline{c}_i \oplus \overline{F}_k(\overline{c}_i))(\mathbf{SGN}_{\overline{c}_i}(\overline{x}) \oplus \mathbf{SGN}_{\overline{F}_k^{(\mathbf{C}_n^k -)}(\overline{c}_i)}(\overline{x})),$$

где $\|\overline{c}_i\| = k, 1 \leqslant i \leqslant \mathbf{C}_n^k - q$. Вектор-функция $\overline{G}_k(\overline{x})$ по построению монотонна и $|\mathbf{БД}(\overline{G}_k, n, \overline{x})| = q$.

Положим $k = \left[\frac{n}{2}\right]$. Тогда существует $\overline{x} \neq \overline{c}_i, 1 \leqslant i \leqslant \mathbf{C}_n^k - q$, такой, что $|\mathbf{БД}(\overline{G}_{\left[\frac{n}{2}\right]}, n, \overline{x})| = q < \mathbf{C}_n^{\left[\frac{n}{2}\right]}, |\overline{x}\| = k$.

По лемме 2 для класса монотонных вектор-функций других периодов не существует.

Теорема 4 доказана.

В заключение автор пользуется случаем выразить признательность своему научному руководителю к.ф.-м.н. А.С. Строгалову за активное участие в обсуждении работы и конструктивные замечания, а также к.ф.-м.н. А.А. Ирматову за неоднократные и полезные обсуждения полученных результатов.

## Список литературы

[1] Яблонский С.В. Введение в дискретную математику. М.: Наука, 1986.

[2] Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977.

[3] Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б. Функции алгебры логики и классы Поста. М.: Наука, 1977.

# Построение классов латинских квадратов в булевой базе данных

В.А. Носов

В работе предлагается конструкция параметрических классов латинских квадратов размера $2^n \times 2^n$ над множеством булевских векторов длины $n$, которая не требует запоминания латинского квадрата. Приводится один классификационный результат для выполнения данной конструкции.

1. Напомним, что латинский квадрат над множеством $S$ есть таблица размера $n \times n$, где $n = |S|$, из элементов множества $S$, в каждой строке и в каждом столбце которой все элементы различны. Латинские квадраты широко используются в теории кодирования, планирования эксперимента, связи в секретных системах ([3, 4, 5]). В настоящее время имеются различные способы построения латинских квадратов, в том числе и с использованием алгебраических структур на множестве $S$. Однако, все эти способы предполагают, чтобы соответствующий латинский квадрат запоминался целиком, что затрудняет использование их в случае больших $S$. Целью настоящей работы является конструкция параметрических классов латинских квадратов в булевской базе данных, то есть для случая $S = E_n$ – множество булевских векторов длины $n$. При этом будем предполагать, что латинский квадрат не запоминается целиком, а определяется локальным образом с помощью функций, задающих по номеру строки и столбца значение соответствующего элемента в латинском квадрате. Другой рассмотренный вопрос – конструкция параметрического класса латинских квадратов, в которых при любом значении параметра эффективно определяется номер строки по любому номеру

столбца и элементу этого столбца. В данной конструкции это осуществляется на тех же функциях, которые определяют латинский квадрат.

Рассмотрены также классификационные вопросы, связанные с осуществлением предлагаемых конструкций.

**2.** Пусть $E_n$ – множество двоичных наборов длины $n$. В этом случае латинский квадрат над множеством $E_n$ может быть задан системой из $n$ булевых функций

$$\begin{array}{l} f_1(x_1,\ldots,x_n,y_1,\ldots,y_n) \\ f_2(x_1,\ldots,x_n,y_1,\ldots,y_n) \\ \ldots \\ f_n(x_1,\ldots,x_n,y_1,\ldots,y_n) \end{array} \qquad (1)$$

от $2n$ переменных, где $x_1,\ldots,x_n$ определяет номер строки, $y_1,\ldots,y_n$ – номер столбца, значения функций $f_1,\ldots,f_n$ определяют соответствующий элемент квадрата.

Используя результаты о регулярности системы булевых функций [7], можно доказать

**Утверждение 1.** *Система $n$ булевых функций $f_1,\ldots,f_n$ от $2n$ переменных $x_1,\ldots,x_n,y_1,\ldots,y_n$ определяет латинский квадрат тогда и только тогда, когда во всех произведениях $f_{i1}\ldots f_{ik}$, $1\leqslant i_1<\ldots<i_k\leqslant n$, $k<n$ в полиноме Жегалкина нет членов, содержащих вхождения $x_1\ldots x_n$ либо $y_1\ldots y_n$, а произведение $f_1\ldots f_n$ содержит оба таких члена и не содержит других членов, их содержащих.*

Данное утверждение не дает эффективного способа построения нужных систем булевых функций, однако позволяет сформулировать ряд достаточных условий путем рассмотрения классов используемых функций. Например, пусть дана система булевых функций вида

$$\begin{array}{l} f_1 = x_1 + y_1 + g_1(x_1,\ldots,x_n,y_1,\ldots,y_n) \\ f_2 = x_2 + y_2 + g_2(x_1,\ldots,x_n,y_1,\ldots,y_n) \\ \ldots \\ f_n = x_n + y_n + g_n(x_1,\ldots,x_n,y_1,\ldots,y_n) \end{array} \qquad (2)$$



от переменных $x_1,\ldots,x_n,y_1,\ldots,y_n$, причем функции $g_i$ не зависят от $x_i$ и $y_i$, $i\in\overline{1,n}$ и кроме того выполнено $g_i\cdot g_j\equiv 0$ при всех $i\neq j$, $i,j\in\overline{1,n}$. Тогда легко видеть, что функции $f_1,\ldots,f_n$ определяют латинский квадрат.

Далее, для системы булевых функций (2) определим два орграфа $G_1(V,E_1)$, $G_2(V,E_2)$, где $v=\{1,\ldots,n\}$ – множество вершин, а множества дуг $E_1,E_2$ определяются соотношениями:

$$\begin{array}{l} (i,j)\in E_1 \Leftrightarrow g_j \text{ существенно зависит от } x_i,\ i,j\in\overline{1,n}. \\ (i,j)\in E_2 \Leftrightarrow g_j \text{ существенно зависит от } y_i,\ i,j\in\overline{1,n}. \end{array} \qquad (3)$$

Легко показать, что если оба графа $G_1$ и $G_2$ не имеют циклов, то система булевых функций $f_1,\ldots,f_n$ (2) определяет латинский квадрат.

Неудобство данных конструкций заключается в том, что в данных классах латинских квадратов нет явно выделенного параметра.

**3.** Предложим теперь способ введения параметра в семейство латинских квадратов. Пусть дано семейство булевых функций $g=(g_1(z_1,\ldots,z_n),\ldots,g_n(z_1,\ldots,z_n))$ от $n$ переменных $z_1,\ldots,z_n$. Пусть $\pi_1(x_1,y_1),\ldots,\pi_n(x_n,y_n)$ – система булевых функций от двух переменных. Определим систему булевых функций $f_1,\ldots,f_n$ от $2n$ переменных $x_1,\ldots,x_n,y_1,\ldots,y_n$ соотношениями:

$$\begin{array}{l} f_1 = x_1 + y_1 + g_1(\pi_1(x_1,y_1),\ldots,\pi_n(x_n,y_n)) \\ f_2 = x_2 + y_2 + g_2(\pi_1(x_1,y_1),\ldots,\pi_n(x_n,y_n)) \\ \ldots \\ f_n = x_n + y_n + g_n(\pi_1(x_1,y_1),\ldots,\pi_n(x_n,y_n)) \end{array} \qquad (4)$$

Напомним (см. [1]), что семейство булевых функций $g=(g_1,\ldots,g_n)$ называют правильным, если для любых различных наборов переменных $z'=(z'_1,\ldots,z'_n)$ и $z''=(z''_1,\ldots,z''_n)$ существует $\alpha\in\overline{1,n}$ такое, что выполнено

$$z'_\alpha\neq z''_\alpha,\quad g_\alpha(z'_1,\ldots,z'_n)=g_\alpha(z''_1,\ldots,z''_n). \qquad (5)$$

**Утверждение 2.** *Система булевых функций $f_1,\ldots,f_n$ вида (4) определяет латинский квадрат для любых функций двух переменных $\pi_1,\ldots,\pi_n$ в том и только в том случае, когда семейство функций $g=(g_1,\ldots,g_n)$ является правильным.*

**Доказательство.** Пусть существуют функции $\pi_1, \ldots, \pi_n$ от двух переменных такие, что семейство $f_1, \ldots, f_n$, определенное (4), не определяет латинский квадрат. Тогда

$$\begin{gathered} f_1(x'_1, \ldots, x'_n, y_1, \ldots, y_n) = f_1(x''_1, \ldots, x''_n, y_1, \ldots, y_n) \\ \ldots \\ f_n(x'_1, \ldots, x'_n, y_1, \ldots, y_n) = f_n(x''_1, \ldots, x''_n, y_1, \ldots, y_n) \end{gathered} \tag{6}$$

для некоторых $x'_1, \ldots, x'_n, x''_1, \ldots, x''_n, y_1, \ldots, y_n$, причем $(x'_1, \ldots, x'_n) \neq (x''_1, \ldots, x''_n)$, либо

$$\begin{gathered} f_1(x_1, \ldots, x_n, y'_1, \ldots, y'_n) = f_1(x_1, \ldots, x_n, y''_1, \ldots, y''_n) \\ \ldots \\ f_n(x_1, \ldots, x_n, y'_1, \ldots, y'_n) = f_n(x_1, \ldots, x_n, y''_1, \ldots, y''_n) \end{gathered} \tag{7}$$

для некоторых $x_1, \ldots, x_n, y'_1, \ldots, y'_n, y''_1, \ldots, y''_n$, причем $(y'_1, \ldots, y'_n) \neq (y''_1, \ldots, y''_n)$.

Пусть выполнено (6), тогда, используя (4), получаем, что

$$\begin{gathered} x'_1 + g_1(\pi_1(x'_1, y_1), \ldots, \pi_n(x'_n, y_n)) = x''_1 + g_1(\pi_1(x''_1, y_1), \ldots, \pi_n(x''_n, y_n)) \\ \ldots \\ x'_n + g_n(\pi_1(x'_1, y_1), \ldots, \pi_n(x'_n, y_n)) = x''_n + g_n(\pi_1(x''_1, y_1), \ldots, \pi_n(x''_n, y_n)) \end{gathered} \tag{8}$$

Введем обозначения

$$\begin{gathered} z' = (z'_1, \ldots, z'_n), \text{ где } z'_i = \pi_i(x'_i, y_i),\ i \in \overline{1,n}, \\ z'' = (z''_1, \ldots, z''_n), \text{ где } z''_i = \pi_i(x''_i, y_i),\ i \in \overline{1,n}. \end{gathered}$$

Рассмотрим пару наборов

$$g(z') = (g_1(z'), \ldots, g_n(z')) \text{ и } g(z'') = (g_1(z''), \ldots, g_n(z'')).$$

Если для всех $\alpha \in \overline{1,n}$ выполнено $g_\alpha(z') \neq g_\alpha(z'')$, то условие правильности семейства функций $g_1, \ldots, g_n$ не выполняется на паре наборов $z'$ и $z''$. Если существует $\alpha \in \overline{1,n}$ такое, что выполнено $g_\alpha(z') = g_\alpha(z'')$, то из (8) получаем, что $x'_\alpha = x''_\alpha$ и поэтому



$\pi_\alpha(x'_\alpha, y_\alpha) = \pi_\alpha(x''_\alpha, y_\alpha)$ и, следовательно, $z'_\alpha = z''_\alpha$. Значит, в этом случае также не выполняется условие правильности семейства $g_1, \ldots, g_n$ на паре $z', z''$. Случай (7) разбирается аналогично. Таким образом, если система функций (4) не определяет латинский квадрат при некоторых функциях $\pi_1, \ldots, \pi_n$, то семейство $g_1, \ldots, g_n$ не является правильным.

Пусть теперь семейство $g_1, \ldots, g_n$ не является правильным. Это значит, что существует пара наборов $z' = (z'_1, \ldots, z'_n)$ и $z'' = (z''_1, \ldots, z''_n)$, что для всех $\alpha \in \overline{1,n}$ с условием $z'_\alpha \neq z''_\alpha$ имеем $g_\alpha(z') \neq g_\alpha(z'')$. Рассмотрим произвольные $x_1, \ldots, x_n$ и $y_1, \ldots, y_n$. Определим пару $x'_1, \ldots, x'_n$ и $x''_1, \ldots, x''_n$, где

$$\begin{aligned} x'_i &= x_i + g_i(z'),\ i \in \overline{1,n}, \\ x''_i &= x_i + g_i(z''),\ i \in \overline{1,n}. \end{aligned} \tag{9}$$

Теперь определим функции $\pi_1, \ldots, \pi_n$ так, чтобы

$$\begin{aligned} \pi_i(x'_i, y_i) &= z'_i,\ i \in \overline{1,n}, \\ \pi_i(x''_i, y_i) &= z''_i,\ i \in \overline{1,n}. \end{aligned} \tag{10}$$

Этого нельзя сделать лишь в случае, когда $x'_i = x''_i$, но $z'_i \neq z''_i$ для некоторого $i \in \overline{1,n}$. Но если $x'_i = x''_i$, то из (9) имеем $g_i(z') = g_i(z'')$ и согласно условиям выбора $z'$ и $z''$ имеем $z'_i = z''_i$. Теперь нетрудно видеть из (4), что элементы квадрата, соответствующие $(x'_1, \ldots, x'_n, y_1, \ldots, y_n)$ и $(x''_1, \ldots, x''_n, y_1, \ldots, y_n)$ равны $(x_1, \ldots, x_n)$, то есть квадрат (4) не является латинским при данных функциях $\pi_1, \ldots, \pi_n$.

Заметим, что понятие правильности семейства функций было введено в [1] в связи с изучением регулярности определенного класса булевских автоматов. Там же приведен критерий правильности и доказана $NP$-полнота задачи проверки правильности семейства булевых функций, заданного в КНФ.

4. Введем понятие равномерной обратимости латинского квадрата. Пусть $g = (g_1, \ldots, g_n)$ – правильное семейство булевых функций, $\pi_1(x_1, y_1), \pi_2(x_2, y_2), \ldots, \pi_n(x_n, y_n)$ – произвольная функция двух переменных. Тогда, согласно предыдущему, таблица над $E_n$, в которой

в строке $x_1, \ldots, x_n$ и в столбце $y_1, \ldots, y_n$ находится $x'_1, \ldots, x'_n$, где

$$\begin{aligned} x'_1 &= x_1 + y_1 + g_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ &\ldots \\ x'_n &= x_n + y_n + g_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \end{aligned} \tag{11}$$

будет латинским квадратом для всех функций $\pi_1, \ldots, \pi_n$.

Будем называть данный латинский квадрат равномерно обратимым и семейство $g = (g_1, \ldots, g_n)$ также равномерно обратимым, если из (11) следует

$$\begin{aligned} x_1 &= x'_1 + y_1 + g_1(\pi_1(\bar{x}'_1 + y_1, y_1), \ldots, \pi_n(\bar{x}'_n + y_n, y_n)) \\ &\ldots \\ x_n &= x'_n + y_n + g_n(\pi_1(\bar{x}'_1 + y_1, y_1), \ldots, \pi_n(\bar{x}'_n + y_n, y_n)). \end{aligned} \tag{12}$$

Смысл равномерной обратимости заключается в том, что номер строки произвольного элемента определяется по номеру столбца и значению элемента с помощью тех же функций $g_1, \ldots, g_n$, $\pi_1, \ldots, \pi_n$, которые участвуют в задании латинского квадрата.

Ограничимся рассмотрением правильных семейств функций $g$ вида

$$g_1 = 1,\ g_2 = g_2(z_1), \ldots, g_n = g_n(z_1, \ldots, z_{n-1}). \tag{13}$$

Будем говорить, что семейство булевых функций (13) удовлетворяет свойству $W$, если для любого $i \in \overline{2, n-1}$ и любого решения $z^*_1, \ldots, z^*_{i-1}$ уравнения

$$g_i(z_1, \ldots, z_{i-1}) = 0 \tag{14}$$

справедливо: функция $g_j(z^*_1, \ldots, z^*_{i-1}, z_i, \ldots, z_{j-1})$ не зависит от $z_i$ для любого $j > i$.

**Утверждение 3.** *Семейство функций $(g_1, \ldots, g_n)$ вида (13) равномерно обратимо тогда и только тогда, когда для него выполнено условие $W$.*



**Доказательство.** Пусть условие $W$ выполнено для семейства $g$. Покажем, что из (11) следует (12). Доказываем индукцией по $n$. Для $n = 2$ имеем

$$\begin{aligned} x'_1 &= x_1 + y_1 + 1, \\ x'_2 &= x_2 + y_2 + g_2(\pi_1(x_1, y_1)). \end{aligned}$$

Отсюда

$$\begin{aligned} x_1 &= x'_1 + y_1 + 1, \\ x_2 &= x'_2 + y_2 + g_2(\pi_1(\bar{x}'_1 + y_1, y_1)), \end{aligned}$$

и утверждение справедливо.

Пусть для $n-1$ утверждение доказано. Имеем для $x_n$ соотношение из (11)

$$x_n = x'_n + y_n + g_n(\pi_1(x_1, y_1), \ldots, \pi_{n-1}(x_{n-1}, y_{n-1})), \tag{15}$$

причем

$$\begin{aligned} x_1 &= x'_1 + y_1 + 1 \\ x_2 &= x'_2 + y_2 + g_2(\pi_1(\bar{x}'_1 + y_1, y_1)) \\ &\ldots \\ x_{n-1} &= x'_{n-1} + y_{n-1} + g_{n-1}(\pi_1(\bar{x}'_1 + y_1, y_1), \ldots, \pi_{n-2}(\bar{x}'_{n-2} + y_{n-2}, y_{n-2})) \end{aligned}$$

по предположению индукции.

Нужно доказать, что

$$x_n = x'_n + y_n + g_n(\pi_1(\bar{x}'_1 + y_1, y_1), \ldots, \pi_{n-1}(\bar{x}'_{n-1} + y_{n-1}, y_{n-1})). \tag{16}$$

В соотношениях (15) и (16) у функции $g_n$ значения первых аргументов совпадают в силу $x'_1 = x_1 + y_1 + 1$. Далее, если $g_2(\pi_1(x_1, y_1)) = 1$, то в (15) и (16) значения вторых аргументов совпадают у функции $g_n$. Если $g_2(\pi_1(x_1, y_1)) = 0$, то в силу свойства $W$, функция $g_n$ не зависит от второго аргумента при данной фиксации первого аргумента и, не меняя значения $g_n$, мы можем положить в качестве значения второго аргумента $\pi_2(\bar{x}'_2 + y_2, y_2)$. Продолжая таким образом, получаем, что соотношения (15) и (16) совпадают.

Пусть условие $W$ не выполнено для функций $g_1, \ldots, g_n$. Значит, существует набор $z_1, \ldots, z_n$ такой, что для некоторого $i \in \overline{2, n-1}$ выполнено

$$g_i(z_1, \ldots, z_{i-1}) = 0,$$

$\ldots, \bar{z}_i, \ldots, z_{j-1})$ для некоторого $j >$
$\ldots, x_n$ и $y_1 = y_2 = \ldots = y_n = 0$.
, чтобы

$z_2, \ldots, \pi_n(x_n, y_n) = z_n$.

$_n(x_n, y_n))$, $i \in \overline{1,n}$.

$z, y_2) = z_2, \ldots, \pi_i(\bar{x}'_i, y_i) = \bar{z}_i, \ldots, \pi_n(\bar{x}'_n, y_n) = z_n$.

можно сделать, так как равенство $x_i = \bar{x}'_i$ влечет $g_i = 1$, что противоречит выбору $z_1, \ldots, z_n$.

Теперь ясно, что для (11) не выполняется (12) при данных $g_1, \ldots, g_n$, $\pi_1, \ldots, \pi_n$ на индексе $j$.

Свойство $W$ позволяет строить конкретные равномерно обратимые семейства $g_1, \ldots, g_n$. Например,

$$g_1 = 1,\ g_{i+1} = g_i \cdot z_i,\ i \in \overline{1,n-1}; \quad g_1 = 1,\ g_{i+1} = \bar{g}_i \cdot z_i,\ i \in \overline{1,n-1}.$$

**5.** Установим теперь труднорешаемость рассматриваемых задач, с точки зрения теории $NP$-полноты.

**Задача 1.** Дано семейство $f_1, \ldots, f_n$ булевых функций от $2n$ переменных $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ в виде КНФ. Спрашивается, верно ли, что данное семейство определяет латинский квадрат?

**Задача 2.** Дано семейство $g_1, \ldots, g_n$ булевых функций от $n$ переменных $z_1, \ldots, z_n$ в виде КНФ. Спрашивается, верно ли, что семейство $g_1, \ldots, g_n$ является правильным?

**Задача 3.** Дано семейство $g_1, \ldots, g_n$ булевых функций вида (13) в КНФ. Спрашивается, верно ли, что данное семейство равномерно обратимо?

Аналогично [1] можно доказать следующее утверждение.

**Утверждение 4.** *Задачи 1, 2, 3 являются $NP$-трудными.*

**Следствие.** Если $P \neq NP$, то для задач 1, 2, 3 не существует разрешающего алгоритма полиномиальной сложности.



**6.** Для реализации предложенной конструкции латинских квадратов представляют интерес классификационные результаты для правильных семейств булевых функций. Заметим, что семейство функций $f = (f_1, \ldots, f_n)$, для которого граф существенной зависимости переменных не имеет циклов, является правильным. Обратное, как не трудно проверить, не является верным. Однако, для широких классов используемых функций вопрос о правильности соответствующего семейства может быть решен в терминах свойств графов, связанных с семействами.

В качестве примера возьмем класс $K_0$ булевых функций от $n$ переменных, где $K_0 = \{f(x_1, \ldots, x_n)\}$ таких, что каждая существенная переменная $x_i$ функции $f$ входит в линейную часть соответствующего полинома Жегалкина. Легко показать, что выполнено равенство

$$|K_0| = \sum_{k=0}^{n} \binom{n}{k} 2^{2^k - k}. \tag{17}$$

Для данного класса функций вопрос о правильности соответствующих семейств решается в терминах ацикличности графа существенной зависимости переменных.

Нетрудно доказать

**Утверждение 5.** *Произвольное семейство булевых функций $f = (f_1, \ldots, f_n)$, где каждая функция $f_i \in K_0$, является правильным в том и только в том случае, когда граф существенной зависимости переменных $G_f$ не имеет циклов.*

Аналогичная картина имеет место, если взять класс функций $K_1 = \{f(x_1, \ldots, x_n)\}$, где $f \in K_1$ в том и только в том случае, если для любой существенной переменной $x_i$ выполнено $f(1 \ldots x_i \ldots 1) \neq \text{const}$.

Заметим, что $|K_0| = |K_1|$.

Ясно, что линейные функции принадлежат как классу $K_0$, так и классу $K_1$.

Рассмотрим теперь класс мультиаффинных функций $M$. Напомним, что булева функция $f(x_1, \ldots, x_n)$ называется мультиаффинной, если она представляется в виде конъюнкции линейных функций.

но $g_j(z_1,\dots,z_i,\dots,z_{j-1}) \neq g_j(z_1,\dots,\bar{z}_i,\dots,z_{j-1})$ для некоторого $j > i$. Рассмотрим произвольные $x_1,\dots,x_n$ и $y_1 = y_2 = \dots = y_n = 0$. Определим функции $\pi_1,\dots,\pi_n$ так, чтобы

$$\pi_1(x_1,y_1) = z_1, \pi_2(x_2,y_2) = z_2,\dots,\pi_n(x_n,y_n) = z_n.$$

Пусть $x_i' = x_i + y_i + g_i(\pi_1(x_1,y_1),\dots,\pi_n(x_n,y_n))$, $i \in \overline{1,n}$.

Теперь положим

$$\pi_1(\bar{x}_1',y_1) = z_1,\ \pi_2(\bar{x}_2',y_2) = z_2,\dots,\pi_i(\bar{x}_i',y_i) = \bar{z}_i,\dots,\pi_n(\bar{x}_n',y_n) = z_n.$$

Это можно сделать, так как равенство $x_i = \bar{x}_i'$ влечет $g_i = 1$, что противоречит выбору $z_1,\dots,z_n$.

Теперь ясно, что для (11) не выполняется (12) при данных $g_1,\dots,g_n$, $\pi_1,\dots,\pi_n$ на индексе $j$.

Свойство $W$ позволяет строить конкретные равномерно обратимые семейства $g_1,\dots,g_n$. Например,

$$g_1 = 1,\ g_{i+1} = g_i \cdot z_i,\ i \in \overline{1,n-1};\quad g_1 = 1,\ g_{i+1} = \bar{g}_i \cdot z_i,\ i \in \overline{1,n-1}.$$

**5.** Установим теперь труднорешаемость рассматриваемых задач, с точки зрения теории $NP$-полноты.

**Задача 1.** Дано семейство $f_1,\dots,f_n$ булевых функций от $2n$ переменных $x_1,\dots,x_n$, $y_1,\dots,y_n$ в виде КНФ. Спрашивается, верно ли, что данное семейство определяет латинский квадрат?

**Задача 2.** Дано семейство $g_1,\dots,g_n$ булевых функций от $n$ переменных $z_1,\dots,z_n$ в виде КНФ. Спрашивается, верно ли, что семейство $g_1,\dots,g_n$ является правильным?

**Задача 3.** Дано семейство $g_1,\dots,g_n$ булевых функций вида (13) в КНФ. Спрашивается, верно ли, что данное семейство равномерно обратимо?

Аналогично [1] можно доказать следующее утверждение.

**Утверждение 4.** *Задачи 1, 2, 3 являются $NP$-трудными.*

**Следствие.** Если $P \neq NP$, то для задач 1, 2, 3 не существует разрешающего алгоритма полиномиальной сложности.



**6.** Для реализации предложенной конструкции латинских квадратов представляют интерес классификационные результаты для правильных семейств булевых функций. Заметим, что семейство функций $f = (f_1,\dots,f_n)$, для которого граф существенной зависимости переменных не имеет циклов, является правильным. Обратное, как не трудно проверить, не является верным. Однако, для широких классов используемых функций вопрос о правильности соответствующего семейства может быть решен в терминах свойств графов, связанных с семействами.

В качестве примера возьмем класс $K_0$ булевых функций от $n$ переменных, где $K_0 = \{f(x_1,\dots,x_n)\}$ таких, что каждая существенная переменная $x_i$ функции $f$ входит в линейную часть соответствующего полинома Жегалкина. Легко показать, что выполнено равенство

$$|K_0| = \sum_{k=0}^{n} \binom{n}{k} 2^{2^k-k}. \tag{17}$$

Для данного класса функций вопрос о правильности соответствующих семейств решается в терминах ацикличности графа существенной зависимости переменных.

Нетрудно доказать

**Утверждение 5.** *Произвольное семейство булевых функций $f = (f_1,\dots,f_n)$, где каждая функция $f_i \in K_0$, является правильным в том и только в том случае, когда граф существенной зависимости переменных $G_f$ не имеет циклов.*

Аналогичная картина имеет место, если взять класс функций $K_1 = \{f(x_1,\dots,x_n)\}$, где $f \in K_1$ в том и только в том случае, если для любой существенной переменной $x_i$ выполнено $f(1\dots x_i\dots 1) \neq \text{const}$.

Заметим, что $|K_0| = |K_1|$.

Ясно, что линейные функции принадлежат как классу $K_0$, так и классу $K_1$.

Рассмотрим теперь класс мультиаффинных функций $M$. Напомним, что булева функция $f(x_1,\dots,x_n)$ называется мультиаффинной, если она представляется в виде конъюнкции линейных функций.

Пусть семейство $f$ состоит из мультиаффинных функций. Это значит, что $f = (f_i)$, $i \in \overline{1,n}$ имеет вид

$$\begin{aligned} f_1 &= \prod_{i=1}^{k_1} l_i^1(x_1 \dots x_n) \\ f_2 &= \prod_{i=1}^{k_2} l_i^2(x_1 \dots x_n) \\ &\dots \\ f_n &= \prod_{i=1}^{k_n} l_i^n(x_1 \dots x_n) \end{aligned} \tag{18}$$

где $k_i$ $(i \in \overline{1,n})$ – число перемножаемых линейных функций в $f_i$, $l_i^t(x_1 \dots x_n) = a_1^t x_1 + \dots + a_n^t x_n + b_t$ – линейная функция над $F_2$, $1 \leqslant t \leqslant n$.

Определим ориентированный граф $G_f^0$ вхождения переменных в семейство $f$, полагая $G_f^0 = (V, E)$, где $V = \{1, 2, \dots, n\}$, $(i,j) \in E \Leftrightarrow \exists s|$ функция $l_s^j$ содержит $x_i$ (то есть $a_s^j = 1$).

Заметим, что граф $G_f^0$ вхождения переменных содержит в качестве подграфа граф $G_f$ существенной зависимости переменных семейства $f$. Построение графа $G_f^0$ просто, построение графа $G_f$ представляет собой нетривиальную задачу. Для многих классов функций установлена $NP$-трудность задачи проверки существенности переменной [2].

Простым элементарным циклом орграфа $G$ будем называть цикл, никакое собственное подмножество вершин которого не образует цикл.

**Утверждение 6.** *Семейство мультиаффинных булевых функций $f = (f_i)$, $i \in \overline{1,n}$ является правильным тогда и только тогда, когда для любого простого элементарного цикла $C$ графа вхождения $G_f^0$ семейства $f$ выполнено условие*

$$\prod_{i \in C} f_i(x_1 \dots x_n) \equiv 0. \tag{19}$$



**Доказательство.** Пусть существует простой элементарный цикл $C$ графа $G_f$ такой, что условие (19) не выполнено, то есть

$$\prod_{i \in C} f_i(x_1 \dots x_n) \neq 0. \tag{20}$$

Для определенности пусть $C = \{i_1 \dots i_s\}$, $i_k \in \overline{1,n}$. Это значит, что функция $f_{i_1}$ содержит вхождение переменной $x_{i_2}$ и не содержит вхождения переменных $x_{i_1}, x_{i_3}, \dots, x_{i_s}$.

Аналогичное высказывание справедливо о функциях $f_{i_2}, \dots, f_{i_s}$. Представим функции $f_{i_1}, \dots, f_{i_s}$ в виде

$$\begin{aligned} f_{i_1} &= (\dots + x_{i_2} + \dots) \dots (\dots + x_{i_2} + \dots) \varphi_{i_1}(x_1 \dots x_n) \\ &\dots \\ f_{i_s} &= (\dots + x_{i_1} + \dots) \dots (\dots + x_{i_1} + \dots) \varphi_{i_s}(x_1 \dots x_n) \end{aligned} \tag{21}$$

Здесь $\varphi_{i_1}$ – мультиаффинная функция, не содержащая вхождений $x_{i_2}$. Сомножители у $\varphi_{i_1}$ отвечают линейным функциям, содержащим вхождение $x_{i_2}$. Аналогично, $\varphi_{i_s}$ – мультиаффинная функция, не содержащая вхождений $x_{i_1}$, сомножители у $\varphi_{i_s}$ отвечают линейным функциям, содержащим вхождение $x_{i_1}$.

Согласно (20) существует двоичный набор $x = (x_1^0 \dots x_n^0)$ такой, что $\prod\limits_{i \in C} f_i(x_1^0, \dots, x_n^0) = 1$.

Следовательно, имеем

$$f_{i_1}(x_1^0 \dots x_n^0) = \dots = f_{i_s}(x_1^0 \dots x_n^0) = 1. \tag{22}$$

Рассмотрим двоичный набор $\tilde{x} = (x_1^0 \dots \bar{x}_{i_1}^0 \dots \bar{x}_{i_s}^0 \dots x_n^0)$, полученный из $x = (x_1^0, \dots, x_n^0)$ отрицанием переменных с индексами из $C$.

Тогда на основании (21) получаем, что на данном наборе выполнено

$$f_{i_1}(\tilde{x}) = f_{i_2}(\tilde{x}) = \dots = f_{i_s}(\tilde{x}) = 0. \tag{23}$$

Из соотношений (22) и (23) следует, что семейство $f$ не является правильным, то есть для него не выполнено условие правильности на наборах $x = (x_1^0, \dots, x_n^0)$ и $\tilde{x} = (x_1^0 \dots \bar{x}_{i_1}^0 \dots \bar{x}_{i_s}^0 \dots x_n^0)$. Обратно,

пусть теперь для любого простого элементарного цикла $C$ графа $G_f^0$ выполнено условие (19).

Для семейства $f = (f_i)$, $i \in \overline{1,n}$ рассмотрим семейство функций $\check{f} = (\check{f}_i)$, $i \in \overline{1,n}$, положив

$$\check{f}(x_1 \dots x_n) = x_i + f_i(x_1 \dots x_n), \ \forall i \in \overline{1,n}. \tag{24}$$

Пусть $I \subset \overline{1,n}$ – множество индексов, $\varepsilon_I = (\varepsilon_\alpha)$, $\alpha \in I$, $\varepsilon_\alpha \in \{0,1\}$ – семейство констант. Для произвольной функции $g(x_1 \dots x_n)$ положим

$$g^{\varepsilon_I}((x_i), i \in CI) = g(x_1 \dots x_n)|_{x_\alpha = \varepsilon_\alpha, \alpha \in I},$$

то есть переменные с индексами из $I$ замещены константами $\varepsilon_I$, $CI$ – дополнение $I$ в $\overline{1,n}$. Известно (см. [1], лемма 2), что $f$ – правильное семейство в том и только в том случае, когда семейство $\check{f}^{\varepsilon_I} = (\check{f}_i^{\varepsilon_I})$, $i \in CI$ регулярно при всех $I \neq \overline{1,n}$ и всех $\varepsilon_I$. Для установления регулярности произвольного семейства булевых функций $g = (g_1, \dots, g_t)$ от переменных $x_1, \dots, x_t$ будем пользоваться критерием Хаффмена (см. [6]), согласно которому семейство $g = (g_1, \dots, g_t)$ регулярно тогда и только тогда, когда для любых индексов $1 \leqslant i_1 < \dots < i_k \leqslant t$ произведение $g_1 \dots g_t$ не содержит члена $x_1 \dots x_t$ в полиноме Жегалкина при $k \leqslant t-1$, а произведение $g_1 \dots g_t$ содержит такой член. Пусть $I = \emptyset$. Покажем регулярность семейства $\check{f} = (\check{f}_i)$, $i \in \overline{1,n}$.

Имеем

$$\check{f}_1 \dots \check{f}_n = x_1 \dots x_n + \sum \prod_{i \in p_1} x_i \prod_{j \in p_2} f_j. \tag{25}$$

Суммирование производится по всем разбиениям $(p_1, p_2)$ множества $\overline{1,n}$, где $p_2 \neq \emptyset$. Покажем, что $\prod\limits_{i \in p_1} x_i \prod\limits_{j \in p_2} f_j$ при любых $(p_1, p_2)$, $p_2 \neq \emptyset$, не содержит члена $x_1, \dots, x_n$. Если, напротив, для некоторого $(p_1, p_2)$, $p_2 \neq \emptyset$ имеется член $x_1, \dots, x_n$, то выполнено $f_j \neq 0$ при $j \in p_2$ и $\prod\limits_{j \in p_2} f_j(x_1 \dots x_n)$ содержит член $\prod\limits_{j \in p_2} x_j$.

Рассмотрим подграф $H_f(p_2)$ графа $G_f$, содержащий вершины множества $p_2$. Из предыдущего следует, что из каждой вершины выходит по крайней мере одна дуга. Легко видеть, что в этом случае



$H_f(p_2)$ содержит простой элементарный цикл $C$ и тогда по условию должно быть $\prod\limits_{j \in C} f_j(x_1 \dots x_n) \equiv 0$. Но $p_2$ содержит вершины $C$ в качестве подмножества. Тогда $\prod\limits_{j \in p_2} f_j(x_1 \dots x_n) \equiv 0$. Значит, член $\prod\limits_{i \in p_1} x_i \prod\limits_{j \in p_2} f_j$ при $p_2 \neq \emptyset$ не содержит члена $x_1, \dots, x_n$ и, следовательно, по (25) произведение $\check{f}_1 \dots \check{f}_n$ содержит такой член.

Пусть теперь существуют $k < n$ и индексы $1 \leqslant i_1 < \dots < i_k \leqslant n$ такие, что произведение $\check{f}_{i_1} \dots \check{f}_{i_k}$ содержит член $x_1 \dots x_n$.

Имеем

$$\check{f}_{i_1} \dots \check{f}_{i_k} = x_{i_1} \dots x_{i_k} + \sum \prod_{i \in p_1} x_i \prod_{j \in p_2} f_j. \tag{26}$$

Суммирование по всем разбиениям $(p_1, p_2)$, $p_2 \neq \emptyset$ множества $\{i_1, \dots, i_k\}$. Это значит, что существует $(p_1, p_2)$, $p_2 \neq \emptyset$, такое, что $\prod\limits_{i \in p_1} x_i \prod\limits_{j \in p_2} f_j$ содержит член $x_1, \dots, x_n$. Отсюда следует, что $\prod\limits_{j \in p_2} f_j$ содержит член $\prod\limits_{i \in Cp_1} x_i$, где $Cp_1$ – дополнение множества $p_1$ в $\overline{1,n}$.

Рассмотрим подграф $H_f(p_2)$ с вершинами множества $p_2$. Поскольку функции с индексами из $p_2$ дают член $\prod\limits_{i \in Cp_1} x_i$, то по определению графа $G_f$ из каждой вершины $Cp_1$ выходит по крайней мере одна дуга с концом в $p_2$. По условию имеем $p_2 \subset Cp_1$. Следовательно, граф $H_f(p_2)$ содержит цикл, поэтому, аналогично предыдущему, имеем $\prod\limits_{j \in p_2} f_j(x_1 \dots x_n) \equiv 0$ и член $x_1, \dots, x_n$ появиться в (26) не может. Таким образом, $\check{f}_1 \dots \check{f}_n$ – регулярное семейство согласно критерию Хаффмена.

Пусть $I \subset \overline{1,n}$ – собственное подмножество, $\varepsilon_I$ – произвольное семейство констант. Регулярность семейства $f^{\varepsilon_I} = (f_i^{\varepsilon_I})$, $i \in CI$ (от переменных $(x_i)$, $i \in CI$) устанавливается повторением предыдущих рассуждений. Это возможно потому, что при замещении переменных константами мультиаффинная функция остается мультиаффинной и условие (19) также сохраняется при замене переменных константами. Тем самым утверждение доказано.

Данный критерий определяет следующий алгоритм проверки

правильности заданного семейства $f$ мультиаффинных функций.

а) Строим граф вхождения переменных $G_f$.

б) Порождаем список простых элементарных циклов графа $G_f$.

в) Для каждого такого контура $C$ проверяем условие (19).

**Замечания:** 1. Проверка условия (19) для мультиаффинных функций по сложности совпадает со сложностью проверки совместности системы линейных уравнений над $F_2$. Для многих классов функций установлена $NP$-трудность проверки выполнимости условия (19) [2].

2. Известно, что каждый элементарный цикл графа представляется через так называемые фундаментальные циклы (см. [8]). Список фундаментальных циклов для графа с $m$ дугами и $n$ вершинами может быть порожден за $O(mn)$ действий [8].

## Список литературы


[1] Носов В.А. Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные Системы. М., 1998. Т. 3. Вып. 3–4. С. 269–280.

[2] Алексеев В.Б., Носов В.А. $NP$-полные задачи и их полиномиальные варианты. Обзор // Обозрение промышленной и прикладной математики. 1997. Т. 4. Вып. 2. С. 165–193.

[3] Белоусов В.Д., Белявская Г.Б. Латинские квадраты, квазигруппы и их приложения. Кишинев, 1989.

[4] Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. М., 1963. С. 333–369.

[5] Denes J., Keedwell A.D. Latin squares and their applications. Budapest, 1974.

[6] Huffman D.A. Canonical forms for information lossless finite-state logical machines // IRE Trans. Circ. Theory. 1959. V. 6. P. 41–59.

[7] Клосс Б.М., Мальшев В.А. Определение регулярности автомата по его каноническим уравнениям // Докл. АН СССР. 1967. Т. 172. №3. С. 543–546.

[8] Липский В. Комбинаторика для программистов. Москва, 1988.


# О свойствах графа гиперболического произведения групп

А.Е. Панкратьев

## 1. Введение

Гиперболические пространства были введены М. Громовым в работе [1] следующим образом. Пусть $x, y, t$ – точки метрического пространства $X$. Обозначим $(x \cdot y)_t = \frac{1}{2}(|x-t| + |y-t| - |x-y|)$.

**Определение 1.** Метрическое пространство $X$ называется *$\delta$-гиперболическим* ($\delta \geqslant 0$) если для любых четырех точек $x, y, z, t \in X$ выполнено неравенство

$$(x \cdot y)_t \geqslant \min((x \cdot z)_t, (y \cdot z)_t) - \delta.$$

Пространство называется *гиперболическим*, если оно $\delta$-гиперболическое для некоторого $\delta \geqslant 0$.

Рассмотрим свободное произведение $F = \underset{i \in I}{*} G_i$ конечного числа групп $G_i$ [3]. Наложим на $F$ конечное множество $R$ дополнительных соотношений и обозначим полученную группу через $H = \langle F|R\rangle$. Над группой $H$ с системой образующих $\mathcal{B} = \bigcup_{i \in I} G_i$ построим граф Кэли $\Gamma(H)$: вершины графа соответствуют элементам группы $H$, причем две вершины, соответствующие элементам $u$ и $v$, соединены ориентированным ребром с меткой $h = u^{-1}v$ в том и только том случае, когда $u^{-1}v \in \mathcal{B}$. Каждое ребро снабдим метрикой отрезка $[0,1]$ и примем за расстояние $|t_1 - t_2|$ между двумя точками $t_1$, $t_2$ графа $\Gamma(H)$ минимум длин путей, их соединяющих.

**Замечание 1.** Пространство $\Gamma(H)$, очевидно, является геодезическим.