[2] Haken A. The interactability of resolutions // Theoretical Computer Science. 1985. V. 39. P. 297–308. / рус. перевод: Хакен А. Трудноразрешаемость резолюций // Кибернетический сборник. №28. 1991. С. 179–194.

[3] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

Оценки мощности некоторых итеративных множеств

А.В. Матвеев

Устанавливаются точные значения числа элементов множеств, построенных с помощью начальных данных и булевых функций из конкретных замкнутых классов.

1. Введение

В работе исследуются мощности множеств, полученных итеративной процедурой из некоторого булевского вектора $\overline{x}$. В качестве компонент итеративного отображения рассматриваются булевы функции из некоторых замкнутых классов в множестве всех булевых операторов $\mathbf{P}_2^n = \underbrace{\mathbf{P}_2 \times \cdots \times \mathbf{P}_2}_{n \text{ штук}}$, где $n \in \mathbb{N}$. В одномерном случае ($n = 1$) – это классы $\mathbf{T}_0, \mathbf{T}_1, \mathbf{M}$ и $\mathbf{S}$ [1].

2. Основные понятия

Пусть $f(\overline{x})$ – булева функция от n переменных, то есть $f : \mathbf{E}_2^n \to \mathbf{E}_2$, где $\mathbf{E}_2 = \{0, 1\}$. Известно, что каждая функция $f(\overline{x})$ из класса $\mathbf{P}_2$ может быть однозначно представлена при помощи полиномов Жегалкина: $f(\overline{x}) = c_1 \oplus c_2 x_1 \oplus \cdots \oplus c_{n+1} x_n \oplus c_p x_1 x_2 \cdots x_n$, где $p = 2^n, \overline{x} = (x_1, x_2, \cdots, x_n)$ – вектор булевских переменных, $c_1, c_2, \cdots, c_p$ – набор булевских коэффициентов, а сумма понимается как сумма по модулю 2.

Упорядоченный набор из n булевых функций $f(\overline{x})$ от n переменных называется вектор-функцией $\overline{F}(\overline{x})$ класса $\mathbf{P}_2^n(\mathbf{E}_2^n)$. Таким образом, определено отображение $\overline{F} : \mathbf{E}_2^n \to \mathbf{E}_2^n$.

В [1] определены классы функций, сохраняющих константу, $\mathbf{T}_c$ ($c \in \{0,1\}$), классы $\mathbf{S}$ самодвойственных и $\mathbf{M}$ – монотонных функций из $\mathbf{P}_2$.

Эти классы функций естественным образом расширяются на декартово произведение множеств функций от n переменных:

1)$\overline{\mathbf{T}}_{\overline{c}} = \{\overline{F} | \overline{F}(\overline{c}) = \overline{c}\}$ – класс вектор-функций, сохраняющих константу $\overline{c}$. Вектор-функция $\overline{F}$ называется *сохраняющей константу* $\overline{c}$.

2) $\overline{\mathbf{S}} = \{\overline{F} | f_i \in \mathbf{S}, 1 \leqslant i \leqslant n\}$ – *класс самодвойственных вектор-функций.* Вектор-функция $\overline{F}$ называется самодвойственной.

3) $\overline{\mathbf{M}} = \{\overline{F} | f_i \in \mathbf{M}, 1 \leqslant i \leqslant n\}$ – *класс монотонных вектор-функций.* Вектор-функция $\overline{F}$ называется монотонной. Очевидно, определенные выше классы принадлежат множеству $\mathbf{P}_2^n$.

Также в классе $\mathbf{P}_2^n$ вводят понятие замыкания.

Очевидно, классы $\overline{\mathbf{T}}_{\overline{c}}, \overline{\mathbf{M}}$ и $\overline{\mathbf{S}}$ замкнуты, и поэтому понятие принадлежности вектор-функций к соответствующим классам корректно.

Задача заключается в том, чтобы построить заданное множество элементов при помощи некоторых начальных данных – элементов множества – и функциональных зависимостей в этом множестве, или показать, что это невозможно. При этом построение данного множества состоит в последовательном применении функциональной зависимости к результату его действия, то есть представляет собой итерационный процесс.

3. Постановка задачи и результаты

Множество, построенное с помощью начальных данных (вектора $\overline{x}_0$) и вектор-функций из конкретных замкнутых классов, будем называть базой данных.

Обозначим $\underbrace{\overline{F}(\cdots(\overline{F}(\overline{x}_0))\cdots)}_{k \text{ штук}}$ через $\overline{F}^{(k)}(\overline{x}_0)$, а через $|\mathbf{A}|$ – мощность множества $\mathbf{A}$.

Пусть дана вектор-функция $\overline{F}$ и начальные данные $\overline{x}_0$. Вывод базы данных заключается в построении множества

$$\{\overline{x}_0, \overline{F}(\overline{x}_0), \cdots, \overline{F}^{(k)}(\overline{x}_0), \cdots, \overline{F}^{(k+p)}(\overline{x}_0) = \overline{F}^{(k)}(\overline{x}_0)\}.$$

Число $p = |\ \mathbf{БД}(\overline{F}, n, \overline{x}_0)\ | = \min\{t > 0 | \overline{F}^{(t)}(\overline{x}_i) = \overline{x}_i$ для любого $i \leqslant k\}$, где $\overline{x}_i = \overline{F}^{(i)}(\overline{x}_0)$ – вектор нашего множества, назовем периодом базы данных.

Пусть дана вектор-функция $\overline{F}$ и начальный вектор $\overline{x}_0$. Построим множество $\mathbf{БД}(\overline{F}, n, \overline{x}_0) = \{\overline{x}_0, \overline{F}(\overline{x}_0), \overline{F}^{(2)}(\overline{x}_0), \cdots, \overline{F}^{(p)}(\overline{x}_0) = \overline{x}_0\}$. Как оценить период этой базы данных $|\ \mathbf{БД}(\overline{F}, n, \overline{x})\ | = p$, если известны некоторые свойства вектор-функции $\overline{F}$ и размерность n?

Период базы данных p изначально ограничен только числом элементов пространства булевых векторов $\mathbf{E}_2^n$. Чтобы доказать это, построим вектор-функцию $\overline{F}_A(\overline{x}) = ((a+1)(\mathrm{mod}\, 2^n))_2$, где $(a)_2 = \overline{x}$ и $0 \leqslant a \leqslant 2^n - 1$.

Теорема 1. *Для любого натурального числа n и любого начального вектора $\overline{x}$ в $\mathbf{E}_2^n$ существует такая вектор-функция $\overline{F}_A$, что период базы данных $p = |\ \mathbf{БД}(\overline{F}_A, n, \overline{x})\ | = 2^n$.*

Вектор-функция $\overline{F}_A$ позволяет получить основной результат для вектор-функций из класса, сохраняющего константу. Этот результат формулируется следующим образом.

Теорема 2. *а) Для любого натурального числа n существует вектор-функция $\overline{F}$, сохраняющая вектор $\overline{c}$ такая, что для любого начального вектора $\overline{x}$ период $|\mathbf{БД}(\overline{F}, n, \overline{x})| \leqslant 2^n - 1$;*

б) существует вектор-функция $\overline{F}_{\overline{c}}$ такая, что для любого начального вектора $\overline{x} \neq \overline{c}$ выполнено равенство $|\mathbf{БД}(\overline{F}_{\overline{c}}, n, \overline{x})| = 2^n - 1$;

в) для любого натурального n существует вектор-функция $\overline{F}_k$ из того же класса вектор-функций, что для любого натурального

$k < 2^n - 1$ существуют начальные вектора $\overline{x}$ такие, что период $|\mathbf{БД}(\overline{F}_k, n, \overline{x})| = k$.

Подобные теоремы верны также для классов самодвойственных и монотонных вектор-функций.

Теорема 3. *а) Для любого натурального числа n и любого натурального числа $k \leqslant 2^{n-1}$ существуют такие функции класса самодвойственных вектор-функций $\overline{F}_k, \overline{F}_{2k}$, что для них можно так подобрать начальные вектора $\overline{x}$, чтобы периоды принимали значения* $|\mathbf{БД}(\overline{F}_k, n, \overline{x})| = k$ *и* $|\mathbf{БД}(\overline{F}_{2k}, n, \overline{x})| = 2k$;
б) существует вектор-функция $\overline{F}_S$ из того же класса, что для любого начального вектора $\overline{x}$ выполнено равенство $|\mathbf{БД}(\overline{F}_S, n, \overline{x})| = 2n$;
в) для данного класса вектор-функций других значений периодов не существует.

Теорема 4. *а) Для любого натурального числа n и любого натурального числа $q \leqslant \mathbf{C}_n^{\left[\frac{k}{n}\right]}$ существуют вектор-функции $\overline{G}$ класса монотонных вектор-функций, что для них можно так подобрать начальные вектора $\overline{x}$, что период* $|\mathbf{БД}(\overline{G}, n, \overline{x})| = q$;
б) других значений периодов не существует.

4. Доказательства теорем 1 и 2

Доказательство теоремы 1. Для любого фиксированного $n \in \mathbb{N}$ рассмотрим отображение π вектора $\overline{x} = (x_1, x_2, ..., x_n)$ из пространства $\mathbf{E}_2^n$ в число a из $\mathbb{Z}/2^n\cdot\mathbb{Z}$ – кольца вычетов по модулю 2^n:

$$\pi(\overline{x}) = \sum_{i=1}^{n} 2^{i-1} x_i.$$

Пусть $\overline{x}_1, \overline{x}_2$ – различные вектора, то есть существует такой наибольший индекс j, что $x_{1j} \neq x_{2j}$. Без ограничения общности положим

$x_{1j} = 1$ и $x_{2j} = 0$. Тогда

$$\pi(\overline{x}_1) - \pi(\overline{x}_2) = \sum_{i=1}^{n} 2^{i-1}(x_{1i} - x_{2i}) = 2^{j-1} - \sum_{i=1}^{j-1} 2^{i-1}(x_{1i} - x_{2i}) \geqslant 1.$$

То есть для любых векторов $\overline{x}_1, \overline{x}_2$ таких, что $\overline{x}_1 \neq \overline{x}_2$ выполнено $\pi(\overline{x}_1) \neq \pi(\overline{x}_2)$. $|\mathbf{E}_2^n| = |\mathbb{Z}/2^n\cdot\mathbb{Z}| = 2^n$. Следовательно, мощность множества векторов $\{\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_p\}$ из класса $\mathbf{E}_2^n$ равна мощности множества чисел $\{\pi(\overline{x}_1), \pi(\overline{x}_2), \cdots, \pi(\overline{x}_p)\}$ кольца вычетов по модулю 2^n.

Для любых векторов $\overline{x}_1$ и $\overline{x}_2$ выполнено $x_{1j} \oplus x_{2j} = x_{1j} + x_{2j} - 2x_{1j}x_{2j}$, где x_{1j}, x_{2j} принимают значения из множества $\{0, 1\}$. Значит,

$$\pi(\overline{x}_1 \oplus \overline{x}_2) = \pi(\overline{x}_1) + \pi(\overline{x}_2) - 2\pi(\overline{x}_1\overline{x}_2).$$

$$\pi(\overline{x}_1 \oplus \overline{x}_2) = \sum_{j=1}^{n} 2^{j-1}(x_{1j} \oplus x_{2j}) = \sum_{j=1}^{n} 2^{j-1}(x_{1j} + x_{2j} - 2x_{1j}x_{2j}) =$$

$$= \sum_{j=2}^{n} 2^{j-1}(x_{1j} + x_{2j} - x_{1j-1}x_{2j-1}) + x_{11} + x_{21} - 2^n x_{1n}x_{2n}.$$

Рассмотрим вектор-функцию $\overline{F}_A(\overline{x}) = \{f_i(\overline{x}) = x_i \oplus \prod_{j=0}^{i-1} x_j, 1 \leqslant i \leqslant n;$ $x_0 = 1\}$. Положим $\overline{x}_1 = \overline{x}$, $x_{2i} = \prod_{j=0}^{i-1} x_j$, где $x_0 = 1$. Тогда

$$\pi(\overline{x}_1 \oplus \overline{x}_2) = \pi(\overline{F}_A(\overline{x})) = (\sum_{i=2}^{n} 2^{i-1}(x_i + \prod_{j=0}^{i-1} x_j - \prod_{j=0}^{i-1} x_j) + x_1 + 1) (\mathrm{mod}\, 2^n) =$$

$(\pi(\overline{x}) + 1) (\mathrm{mod}\, 2^n)$. Таким образом, $\pi(\overline{F}_A^{(k)}(\overline{x})) = (\pi(\overline{x}) + k) (\mathrm{mod}\, 2^n)$.

Следовательно, $|\mathbf{БД}(\overline{F}_A, n, \overline{x})| = |\{(\pi(\overline{x}) + k) (\mathrm{mod}\, 2^n)\}_{k=1}^{2^n}| = |\{k\}_{k=0}^{2^n-1}| = 2^n$. При этом вектор-функция $\overline{F}_A$ отображает вектора следующим образом: $(0)_2 \to (1)_2 \to \cdots \to (2^n - 1)_2 \to (0)_2$, где $\{k\}_2 = \pi^{-1}(k) = \{\overline{x} | x_i = \frac{k (\mathrm{mod}\, 2^i) - k (\mathrm{mod}\, 2^{i-1})}{2^{i-1}}$, где $1 \leqslant i \leqslant n\}$.

Теорема 1 доказана.

Доказательство теоремы 2. По условию $\overline{F}(\overline{c}) = \overline{c}$. Поэтому при любом $\overline{x} \neq \overline{c}$ выполнено неравенство $|\mathbf{БД}(\overline{F}, n, \overline{x})| \leqslant 2^n - 1$. Рассмотрим вектор-функцию $\mathbf{SGN}_{\overline{c}}(\overline{x}) = \{\mathrm{sgn}_i(\overline{x}) = (x'_j \oplus 1), 1 \leqslant i \leqslant n$, где

$\overline{x}' = \overline{x} \oplus \overline{c}\}$. $\mathbf{SGN}_{\overline{c}}(\overline{c}) = \overline{1}$, и $\mathbf{SGN}_{\overline{c}}(\overline{x}) = \overline{0}$, если $\overline{x}' \neq \overline{0}$ (то есть $\overline{x} \neq \overline{c}$).

$$\overline{F}_{\overline{c}}(\overline{x}) = \overline{F}_A(\overline{x}) \oplus (\overline{c} \oplus \overline{F}_A(\overline{c}))(\mathbf{SGN}_{\overline{c}}(\overline{x}) \oplus \mathbf{SGN}_{\overline{F}_A^{(2^n-1)}(\overline{c})}(\overline{x})).$$

По построению $\overline{F}_{\overline{c}}(\overline{c}) = \overline{c}$, $\overline{F}_{\overline{c}}(\overline{F}_A^{(2^n-1)}(\overline{c})) = \overline{F}_A(\overline{c})$ и $\overline{F}_{\overline{c}}(\overline{x}) = \overline{F}_A(\overline{x})$ для остальных $\overline{x}$. Таким образом, построена база данных с периодом $|\mathbf{БД}(\overline{F}_{\overline{c}}, n, \overline{x})| = 2^n - 1$ при $\overline{x} \neq \overline{c}$.

Возьмем произвольный набор различных векторов $\mathrm{M} = \{\overline{c}_1, \overline{c}_2, \cdots, \overline{c}_{2^n-k-1}\}$, где $0 \leqslant k \leqslant 2^n - 1$, таких, что $\overline{c} \notin \mathrm{M}$. Построим вектор-функцию $\overline{F}_k \in \overline{\mathbf{T}}_{\overline{c}}$ такую, что $|\mathbf{БД}(\overline{F}_k, n, \overline{x})| = k$. Будем действовать по следующему алгоритму:

Шаг 1. $\overline{F}_{2^n-1}(\overline{x}) = \overline{F}_{\overline{c}}(\overline{x})$; $t = 2^n - 1$.

Шаг 2. $\overline{F}_{t-1}(\overline{x}) = \overline{F}_t(\overline{x}) \oplus (\overline{c}' \oplus \overline{F}_t(\overline{c}'))(\mathbf{SGN}_{\overline{c}'}(\overline{x}) \oplus \mathbf{SGN}_{\overline{F}_t^{(t-1)}(\overline{c}')}(\overline{x}))$, где $\overline{c}' = \overline{c}_{2^n-t}$.

Шаг 3. Если $t \geqslant k+1$, переходим к **шагу 2**.

Шаг 4. Построенная вектор-функция $\overline{F}_k$ и есть искомая.

Действительно, построенная вектор-функция $\overline{F}_k$ обладает свойством сохранять вектор $\overline{c}$ и вектора из множества M, то есть $\overline{F}_k(\overline{c}) = \overline{c}$ и $\overline{F}_k(\overline{c}') = \overline{c}'$ для любого $\overline{c}' \in \mathrm{M}$. Остальные вектора образуют базу данных.

Теорема 2 доказана.

5. Доказательство вспомогательных утверждений

Лемма 1. *Если существует такая самодвойственная вектор-функция $\overline{F}_p$, что $p = |\mathbf{БД}(\overline{F}_p, n, \overline{x})| \leqslant 2^{n-1}$, то p делится на 2.*

Доказательство. Если $|\mathbf{БД}(\overline{F}_p, n, \overline{x})| = 2^{n-1}$, то $|\mathbf{БД}(\overline{F}_p, n, \overline{x})|$ делится на 2.

Пусть $|\mathbf{БД}(\overline{F}_p, n, \overline{x})| \geqslant 2^{n-1}$. Тогда существует по крайней мере одна пара двойственных векторов $\overline{y}, \neg\overline{y} \in \mathbf{БД}(\overline{F}_p, n, \overline{x})$. Это значит, что существует такое k, для которого $\overline{F}_p^{(k)}(\overline{y}) = \neg\overline{y}$. Но тогда $\overline{F}_p^{(k)}(\neg\overline{y}) = \overline{y}$, так как $\overline{F}_p \in \overline{\mathbf{S}}$. Следовательно, $\overline{F}_p^{(2k)}(\overline{y}) = \overline{y}$ и $p = |\mathbf{БД}(\overline{F}_p, n, \overline{x})| = 2k$.

Лемма 1 доказана.

Лемма 2. *Для любого n и любой вектор-функции $\overline{F}$ класса монотонных вектор-функций в базе данных $\mathbf{БД}(\overline{F}, n, \overline{x})$ не существует пары сравнимых векторов, то есть каждый вектор сравним только с собой.*

Доказательство. $\mathbf{БД}(\overline{F}, n, \overline{x}) = \{\overline{x}_0, \overline{F}(\overline{x}_0), \cdots, \overline{F}^{(k)}(\overline{x}_0), \cdots, \overline{F}^{(p)}(\overline{x}_0) = \overline{x}_0\}$, где $\overline{F}$ – монотонная вектор-функция и $|\mathbf{БД}(\overline{F}, n, \overline{x})| = p$. Если $\overline{x}_0$ сравним с $\overline{F}^{(k)}(\overline{x}_0)$, то $\overline{F}^{(l)}(\overline{x}_0)$ сравним с $\overline{F}^{(k+l)}(\overline{x}_0)$ по определению. Пусть $k = \min\{t | 0 < t \leqslant p$ и существует l, что $\overline{F}^{(l)}(\overline{x}_0)$ сравним с $\overline{F}^{(l+t)}(\overline{x}_0)\}$. Тогда положим $\overline{F}^{(l)}(\overline{x}_0)$ в качестве начального вектора $\overline{x}_0$. Следовательно, $\overline{x}_0$ сравним с $\overline{F}^{(k)}(\overline{x}_0)$.

Не ограничивая общности, положим $\overline{x}_0 \preceq \overline{F}^{(k)}(\overline{x}_0)$. Тогда выполнена система отношений

$$\overline{x}_0 \preceq \overline{F}^{(k)}(\overline{x}_0) \preceq \overline{F}^{(2k)}(\overline{x}_0) \preceq \cdots \preceq \overline{F}^{(qk)}(\overline{x}_0). \qquad (1)$$

Пусть $p = qk + r, 0 < r < k$. Тогда $\overline{F}^{((q-1)k+r)}(\overline{x}_0) \preceq \overline{F}^{(p)}(\overline{x}_0) = \overline{x}_0$. Подставляя данное отношение в систему (1), получим $\overline{F}^{((q-1)k+r)}(\overline{x}_0) \preceq \cdots \preceq \overline{F}^{((q-1)k+k)}(\overline{x}_0)$ или, с учетом транзитивности отношения частичного порядка, $\overline{F}^{((q-1)k+r)}(\overline{x}_0) \preceq \overline{F}^{(qk)}(\overline{x}_0)$.

Таким образом, существуют различные сравнимые элементы, отстоящие друг от друга на $(k-r)$ суперпозиций. Противоречие с выбором k, так как $(k-r) < k$.

Пусть $p = qk$. Тогда $\overline{x}_0 \preceq \overline{F}^{(k)}(\overline{x}_0) \preceq \cdots \preceq \overline{F}^{(p)}(\overline{x}_0) = \overline{x}_0$. Следовательно, $k = p$ (так как отношение частичного порядка транзитивно).

Лемма 2 доказана.

Лемма 3. *Множество $\mathbf{M}_k(n) = \{\overline{x} \mid \|\overline{x}\| = k\}$ состоит из попарно несравнимых векторов, где $\|\overline{x}\| = \sum_{i=1}^{n} x_i$ – вес вектора. То есть для*

любых векторов $\overline{x}$ *и* $\overline{y}$ *из множества* $\mathbf{M}_k(n)$ *не верно, что* $\overline{x} \preceq \overline{y}$. *Число векторов* $|\mathbf{M}_k(n)| = \mathbf{C}_n^k$.

Доказательство. Пусть существуют различные вектора $\overline{x}_1, \overline{x}_2 \in \mathbf{M}_k(n)$ такие, что $\overline{x}_2 \preceq \overline{x}_1$. То есть для любого i из того, что $x_{1i} = 0$ следует, что $x_{2i} = 0$. Пусть существует такое j, что из $x_{1j} = 1$ следует, что $x_{2j} = 0$. Тогда $k = \sum\limits_{i=1}^{n} x_{2i} = \sum\limits_{i:x_{2i}=1} 1 = \sum\limits_{i:x_{2i}=1} x_{1i} \leqslant \sum\limits_{i=1}^{n} x_{1i} - x_{1j} = k - 1$ – противоречие. Следовательно, для любого $j : x_{1j} = 1$ следует, что $x_{2j} = 1$ и для любого $j : x_{1j} = 0$ следует, что $x_{2j} = 0$. Это значит, что $\overline{x}_1 = \overline{x}_2$. Поэтому не существует различных $\overline{x}_1, \overline{x}_2 \in \mathbf{M}_k(n)$ таких, что $\overline{x}_2 \preceq \overline{x}_1$. Число векторов $|\mathbf{M}_k(n)| = \mathbf{C}_n^k$. Действительно, k единиц можно разместить по n ячейкам $\mathbf{C}_n^k$ способами.

Лемма 3 доказана.

Лемма 4. *В множестве* $\{\overline{\sigma}_1, \overline{\sigma}_2, \cdots, \overline{\sigma}_k\}$, *состоящем из попарно несравнимых векторов пространства* $\mathbf{E}_2^n$, *число векторов* $k \leqslant \mathbf{C}_n^{[\frac{n}{2}]}$, *и равенство достигается.*

Доказательство. Последовательность $\{\overline{x}_0, \cdots, \overline{x}_n\}$, такая что $\overline{x}_{i-1} \preceq \overline{x}_i$ и вес $\|x_i\| = i$, называется монотонно возрастающим путем из $\overline{0}$ в $\overline{1}$. Вектора $\overline{\sigma}_1, \overline{\sigma}_2$ несравнимы тогда и только тогда, когда не существует монотонно возрастающего пути из $\overline{0}$ в $\overline{1}$, проходящего через $\overline{\sigma}_1$ и $\overline{\sigma}_2$ [2]. Другими словами, все пути, содержащие $\overline{\sigma}_1$ и $\overline{\sigma}_2$ различны.

Введем функцию $\mathbf{Z}(\overline{\sigma}) = \{$число монотонно возрастающих путей из $\overline{0}$ в $\overline{1}$, проходящих через $\overline{\sigma}\}$ $= \sigma!(n-\sigma)!$, где $\sigma = \|\sigma\|$. Если $A = \{\overline{\sigma}_i \mid \overline{\sigma}_i$ попарно несравнимы$\}$, то $\mathbf{Z}(A) = \sum\limits_{i=1}^{k} \mathbf{Z}(\sigma_i), |A| = k$.

$\mathbf{Z}(\overline{0}) = \mathbf{Z}(\overline{1}) = n!$ – максимальное число путей в $\mathbf{E}_2^n$.

$\mathbf{Z}(A) = \sum\limits_{i=1}^{k} \sigma_i!(n-\sigma_i)! \leqslant n!$. Это эквивалентно неравенству $\sum\limits_{i=1}^{k} (\mathbf{C}_n^{\sigma_i})^{-1} \leqslant 1$.

Легко показать, что число $\mathbf{C}_n^{\sigma^*}$ будет максимальным при $\sigma^* = [\frac{n}{2}]$. Следовательно, $k(\mathbf{C}_n^{[\frac{n}{2}]})^{-1} \leqslant \sum\limits_{i=1}^{k} (\mathbf{C}_n^{\sigma_i})^{-1} \leqslant 1$, и $k \leqslant \mathbf{C}_n^{[\frac{n}{2}]}$. По лемме 3 при $A = \mathbf{M}_{[\frac{n}{2}]}(n)$ достигается равенство $k = \mathbf{C}_n^{[\frac{n}{2}]}$.

Лемма 4 доказана.

6. Доказательства теорем 3 и 4

Доказательство теоремы 3. Для любой функции $p(y_1, \cdots, y_n)$ выполнено следующее утверждение

$$f(y_1, \cdots, y_n, x_i) = (x_i \oplus 1)p(y_1, \cdots, y_n) \oplus x_i(p(y_1 \oplus 1, \cdots, y_n \oplus 1) \oplus 1) \in \mathbf{S}(\mathbf{E}_2^n).$$

Здесь x_i может совпадать с каким-то y_j или быть новой переменной, отличной от всех y_j.

Действительно, $f(\neg(y_1, \cdots, y_n, x_i)) = (\neg x_i \oplus 1)\ p(\neg(y_1, \cdots, y_n)) \oplus (\neg x_i)(p(y_1, \cdots, y_n) \oplus 1) = (x_i)p(\neg(y_1, \cdots, y_n)) \oplus x_i \oplus (x_i \oplus 1)p(y_1, \cdots, y_n) \oplus 1 = f(y_1, \cdots, y_n, x_i) \oplus 1$.

1) Рассмотрим вектор-функцию следующего вида: $\overline{F}_S(\overline{x}) = (f_i(\overline{x}) = x_n \oplus f_n \oplus g_i$, где $g_i(\overline{x}) = (x_n \oplus 1)p_i(\overline{x}) \oplus x_n(p_i(\neg\overline{x}) \oplus 1)$, $p_i(\overline{x}) = x_i \oplus \prod\limits_{j=1}^{i} x_j, x_0 = 1, 1 \leqslant i \leqslant n-1; f_n(\overline{x}) = x_n \oplus \prod\limits_{j=1}^{n-1} x_j \oplus \prod\limits_{j=1}^{n} x_j \oplus \prod\limits_{j=1}^{1} (x_j \oplus 1) \oplus \prod\limits_{j=1}^{n} (x_j \oplus 1)\}$.

$f_i(\overline{x})$ самодвойственная функция, так как x_n, f_n и $g_i \in \mathbf{S}$, и сумма нечетного числа самодвойственных функций есть функция самодвойственная, $1 \leqslant i \leqslant n-1$. $f_n(\overline{x}) \in \mathbf{S}$ по построению. Следовательно, $F_S \in \mathbf{S}$.

Для любого n выполняется:

Если $x_n = 0$, то $f_n = \prod\limits_{j=1}^{n-1} x_j$, и $f_i(\overline{x}) = p_i(\overline{x})$, когда существует i такое, что $x_i = 0, 1 \leqslant i \leqslant n-1$. Пусть $x_1 = \cdots = x_{n-1} = 1$. Тогда

$f_n = 1$ и $f_i(\overline{x}) = 1, 1 \leqslant i \leqslant n-1$. Положив $\overline{x} = (0)_2$, получим, что $\overline{F}_S$ отображает вектор $\overline{x}$ следующим образом: $(0)_2 \to (1)_2 \to \cdots \to (2^{n-1}-1)_2 \to (2^n-1)_2$. Далее по свойству самодвойственности получим все оставшиеся вектора: $\overline{F}_S((2^n-1-k)_2) = \overline{F}_S((k)_2) \oplus (2^n-1)_2$.

Таким образом, $|\mathbf{БД}(\overline{F}_S, n, \overline{x})| = 2^n$.

2) Возьмем произвольный набор попарно не двойственных векторов $\mathrm{M} = \{\overline{c}_1, \overline{c}_2, \cdots, \overline{c}_{2^{n-1}-k}\}$, где $0 < k < 2^{n-1}$, и зафиксируем их вместе с множеством двойственных векторов $\neg\mathrm{M} = \{\overline{c}_1 \oplus \overline{1}, \overline{c}_2 \oplus \overline{1}, \cdots, \overline{c}_{2^{n-1}-k} \oplus \overline{1}\}$ с помощью функции $\mathbf{SGN}_{\overline{c}}$ из теоремы 2:

Шаг 1. $\overline{F}_{2^n}(\overline{x}) = \overline{F}_S(\overline{x})$; $t = 2^{n-1}$; $q = 1$.

Шаг 2. $\overline{F}_{2(t-1)}(\overline{x}) = \overline{F}_{2t}(\overline{x}) \oplus (\overline{c}_q \oplus \overline{F}_{2t}(\overline{c}_q))(\mathbf{SGN}_{\overline{c}_q}(\overline{x}) \oplus \mathbf{SGN}_{\overline{F}^{(2t-1)}_{2t}(\neg\overline{c}_q)}(\overline{x}) \oplus \mathbf{SGN}_{\neg\overline{c}_q}(\overline{x}) \oplus \mathbf{SGN}_{\overline{F}^{(2t-1)}_{2t}(\neg\overline{c}_q)}(\overline{x}))$; $t = t-1$.

Шаг 3. Если $q < 2^{n-1} - k$, то $q = q+1$; переходим к **шагу 2**.

Шаг 4. Построенная вектор-функция $\overline{F}_{2k}$ и есть искомая.

Действительно, вектор-функция $\overline{F}_{2k} \in \overline{\mathbf{S}}$, так как $\overline{F}_{2k} \in \overline{\mathbf{T}}_{\overline{c}}$ и $\overline{F}_{2k} \in \overline{\mathbf{T}}_{\overline{c}}$ для любого вектора $\overline{c}$ множества M по построению, и значит, выполнено свойство $\overline{F}_{2k}(\neg\overline{c}) = \overline{F}_{2k}(\overline{c}) \oplus \overline{1}$; для остальных векторов $\overline{x}$ $\overline{F}_{2k} \in \overline{\mathbf{S}}$. Кроме того, по построению при любом начальном векторе $\overline{x} \notin \mathrm{M} \vee \neg M$ $|\mathbf{БД}(\overline{F}_{2k}, n, \overline{x})| = 2k$.

3) Рассмотрим вектор-функцию $\overline{F}(\overline{x}) = \{f_i(\overline{x}) = (x_n \oplus 1)p_i(\overline{x}) \oplus x_n(p_i(\neg\overline{x}) \oplus 1)$, где $p_i(\overline{x}) = x_i \oplus \prod_{j=0}^{i-1} x_j, 1 \leqslant i \leqslant n-1, x_0 = 1; f_n(\overline{x}) = x_n\}$.

По построению эта вектор-функция самодвойственна, и при $x_n = 0$ у нее период $|\mathbf{БД}(\overline{F}, n, \overline{x})| = 2^{n-1}$. Аналогично при $x_n = 1$. Применим к ней модифицированный алгоритм из пункта 2) доказательства:

Шаг 1. $\overline{F}_{2^{n-1}}(\overline{x}) = \overline{F}(\overline{x})$; $t = 2^{n-1}$; $q = 1$.

Шаг 2. $\overline{F}_{t-1}(\overline{x}) = \overline{F}_t(\overline{x}) \oplus (\overline{c}_q \oplus \overline{F}_t(\overline{c}_q))(\mathbf{SGN}_{\overline{c}_q}(\overline{x}) \oplus \mathbf{SGN}_{\overline{F}^{(t-1)}_t(\overline{c}_q)}(\overline{x})) \oplus \mathbf{SGN}_{\neg\overline{c}_q}(\overline{x}) \oplus \mathbf{SGN}_{\overline{F}^{(t-1)}_t(\neg\overline{c}_q)}(\overline{x}))$; $t = t-1$.

Шаг 3. Если $q < 2^{n-1} - k$, то $q = q+1$ и переходим к **шагу 2**.

Шаг 4. Построенная вектор-функция $\overline{F}_k$ и есть искомая.

По построению $|\mathbf{БД}(\overline{F}_k, n, \overline{x})| = k$ при любом начальном векторе $\overline{x} \notin \neg\,\mathrm{M} \vee \mathrm{M}$. Из леммы 1 следует, что других периодов не существует.

Теорема 3 доказана.

Следствие. Существует вектор-функция $\overline{F}^{(-1)}_A(\overline{x}) = \overline{F}^{(2^n-1)}_A(\overline{x}) = \overline{F}_A(\neg\overline{x}) \oplus \overline{1}$.

Доказательство. Рассмотрим функцию $\overline{F}_S$. При любом n выполняется:

Если $x_n = 1$, то $f_n = \prod_{j=0}^{n-1}(x_j \oplus 1)$, и $f_i(\overline{x}) = p_i(\neg\overline{x}) \oplus 1$, когда существует i такое, что $x_i = 1, 1 \leqslant i \leqslant n-1$. Положив $\overline{x} = (2^n - 1)_2$, из самодвойственности получим, что $\overline{F}_S$ отображает вектор $\overline{x}$ следующим образом: $(2^n-1)_2 \to (2^n-2)_2 \to \cdots \to (2^{n-1})_2, \overline{F}^{(-1)}_A(\overline{0}) = \overline{F}(\neg\overline{0}) \oplus \overline{1} = \overline{F}(\overline{1}) \oplus \overline{1} = \overline{1}$. Таким образом, вектор-функция $\overline{F}^{(-1)}_A(\overline{x}) = \{f_i(\overline{x}) = p_i(\neg\overline{x}) \oplus 1$, где $p_i(\overline{x}) = x_i \oplus x_j, x_0 = 1, 1 \leqslant i \leqslant n-1\}$ действует как вектор-функция, противоположная $\overline{F}_A(\overline{x})$ на множестве $\mathbf{E}^{n-1}_2$.

То есть построена $\overline{F}^{(-1)}_A(\overline{x}) = \overline{F}^{(2^n-1)}_A(\overline{x}) = \overline{F}_A(\neg\overline{x}) \oplus \overline{1}$.

Следствие доказано.

Доказательство теоремы 4. Рассмотрим функцию $\overline{F}_k(\overline{x})$ следующего вида.

$$\overline{F}_k(\overline{x}) = \begin{cases} \overline{0}, & \|\overline{x}\| < k; \\ \overline{R}_k(\overline{x}), & \|\overline{x}\| = k; \\ \overline{1}, & \|\overline{x}\| > k, \end{cases}$$

где $\overline{R}_k(\overline{x}) \in \overline{T}_{\overline{c}_i}$ для любого $\overline{c}_i \notin \mathbf{M}_k(n)$.

$$\overline{R}_k(\overline{x}) = \overline{F}_A(\overline{x}) \oplus \sum_{i=1}^{d}(\overline{c}_i \oplus \overline{F}_A(\overline{c}_i))(\mathbf{SGN}_{\overline{c}_i}(\overline{x}) \oplus \mathbf{SGN}_{\overline{F}^{(2^n-1)}_A(\overline{c}_i)}(\overline{x})),$$

где $\overline{c}_i$ – все различные вектора, не принадлежащие множеству $\mathbf{M}_k(n)$, а $d = 2^n - \mathbf{C}^k_n$.

Здесь $\mathbf{SGN}_{\overline{c}_i}(\overline{x})$ – вектор-функция из доказательства теоремы 2.

$\overline{F}_k(\overline{x}) = (\sum_{i=1}^{\mathbf{C}^k_n} \mathbf{SGN}_{\overline{c}_i}(\overline{x}))\overline{R}_k(\overline{x}) \oplus \sum_{j=1}^{b} \mathbf{SGN}_{\overline{c}_j}(\overline{x})$, где $\|\overline{c}_i\| = k, \|\overline{c}_j\| > k$ и $b = \frac{(2^n - 3\mathbf{C}^k_n - (-1)^n)}{2}$.

Таким образом, построена вектор-функция $\overline{F}_k$ такая, что при любом начальном векторе $\overline{x}, \|\overline{x}\| = k$ выполнено $\mathbf{БД}(\overline{F}_k, n, \overline{x}) = \mathbf{M}_k(n)$ для любого $k \leqslant n$. Эта вектор-функция монотонна.

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