Об одной линейной последовательной машине без входов

А.В. Матвеев

1. Введение

При описании объектов предметного мира мы сталкиваемся со многими различными задачами, одной из которых является задача описания объекта без избыточности или с возможно наименьшей избыточностью. Это требование, например, возникает естественным образом из ограниченности вычислительных ресурсов. Другой часто встречающейся задачей является описание зависимостей между свойствами этого объекта.

Одним из примеров решения задач такого рода является создание теории баз данных.

База данных — это совокупность наборов данных, объединенных в целях создания информационной модели объекта, используемой при обработке информации.

Создание баз данных преследует две основные цели: понизить избыточность данных и повысить их надежность. Один из способов формализации априорных знаний об абстрактной базе данных — установление зависимостей между данными.

Предположим, что база данных конечна, и что известны условия на зависимости между данными. Первое предположение возникает, как уже было сказано выше, из-за ограниченности вычислительных ресурсов. Второе предположение означает, что мы владеем информацией о структуре объекта.

2. Постановка задачи и результаты

Рассмотрим $f(\overline{x})$ — булева функция от n переменных, то есть $f : \mathbf{E}_2^n \to \mathbf{E}_2$, где $\mathbf{E}_2 = \{0, 1\}$.

Известно [3], что каждая функция $f(\overline{x})$ из класса $\mathbf{P}_2$ может быть однозначно представлена полиномом Жегалкина: $f(\overline{x}) = c_1 \oplus c_2 x_1 \oplus \cdots c_{n+1} x_n \oplus c_p x_1 x_2 \cdots x_n$, 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.

Последовательность n булевых функций $f(\overline{x})$ от n переменных с фиксированным порядком в ней называется вектор-функцией $\overline{F}(\overline{x})$ класса $\mathbf{P}_2^n(\mathbf{E}_2^n)$. Таким образом, определено отображение $\overline{F} : \mathbf{E}_2^n \to \mathbf{E}_2^n$. Это отображение можно интерпретировать также как функциональную зависимость в некоторой базе данных.

Рассмотрим задачу вывода базы данных. Эта задача заключается в построении множества $\{\overline{x}_0, \overline{F}(\overline{x}_0), \overline{F}(\overline{F}(\overline{x}_0)), \cdots\}$ по некоторым начальным данным $\overline{x}_0$ и заданной функциональной зависимости $\overline{F}$.

В общем виде, поскольку $\mathbf{E}_2^n$ конечно, множество выглядит так: $\{\overline{x}_0, \overline{F}(\overline{x}_0), \overline{F}(\overline{F}(\overline{x}_0)), \cdots, \underbrace{\overline{F}(\cdots(\overline{F}(\overline{x}_0))\cdots)}_{k \text{ штук}} = \overline{x}_k, \underbrace{\overline{F}(\cdots(\overline{F}(\overline{x}_k))\cdots)}_{p \text{ штук}} = \overline{x}_k\}$. Далее будем обозначать $\underbrace{\overline{F}(\cdots(\overline{F}(\overline{x}_0))\cdots)}_{k \text{ штук}}$ как $\overline{F}^{(k)}(\overline{x}_0)$.

Число $(p-k)$ назовем периодом базы данных. Число k остальных элементов называется предпериодом.

Эту задачу можно также проинтерпретировать следующим образом.

Рассмотрим структурный автомат с n входами и n выходами, где n — некоторое натуральное число (рис. 1). Этот автомат состоит из набора функциональных элементов, реализующего вектор-функцию $\overline{F}$, и системы задержек. В начальный момент времени автомат находится в состоянии $\overline{x}_0$ и реализует итеративный процесс построения множества булевских векторов длины n.

Другими словами, задан инициальный конечный автомат

$$(\varnothing, \mathbf{E}_2^n, \mathbf{E}_2^n, \phi(q(t), x(t)), \psi(q(t), x(t)), q_0 = q(0)).$$

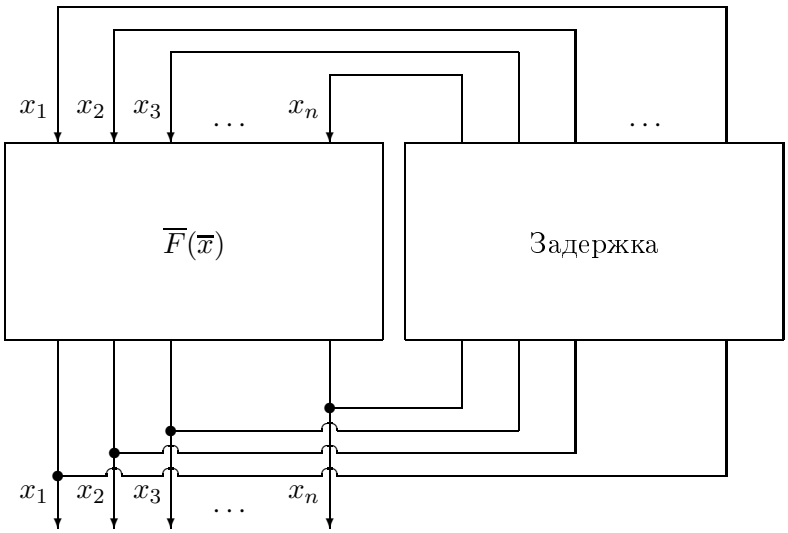

Рис. 1. Автономный автомат, реализующий вектор-функцию $\overline{F}(\overline{x})$.

Этот автомат имеет каноническое уравнение

$$\begin{cases} q(0) = \overline{x}_0, \\ q(t+1) = \overline{F}(q(t)), \\ \overline{x}(t) = q(t). \end{cases}$$

Класс таких автоматов описывает все множества, которые можно получить при помощи итерационной процедуры применения вектор-функции к результату ее действия, начиная с любого булевского вектора длины n.

Пусть множество имеет вид $\mathbf{БД}(\overline{F}, n, \overline{x}_0) = \{\overline{x}_0, \overline{F}(\overline{x}_0), \overline{F}^{(2)}(\overline{x}_0), \ldots, \overline{F}^{(p)}(\overline{x}_0) = \overline{x}_0\}$.

Очевидно, такое множество однозначно с точностью до циклической перестановки строится по вектор-функции $\overline{F}$ и любому вектору, содержащемуся в нем. Формально это можно получить, если положить период базы данных $p = \min\{t > 0 | \overline{F}^{(t)}(\overline{x}_0) = \overline{x}_0\}$.

Если $\overline{x}_\alpha \in \mathbf{БД}(\overline{F}, n, \overline{x}_\beta)$, то существует такое натуральное число k, что $\overline{x}_\alpha = \overline{F}^{(k)}(\overline{x}_\beta)$, и все глубины суперпозиций берутся по модулю p. Если же задано множество различных векторов, то тем самым задан класс вектор-функций.

Была поставлена задача оценить период базы данных $p = |\ \mathbf{БД}(\overline{F}, n, \overline{x}_0)\ |_M$ при некотором начальном векторе $\overline{x}_0$, если известно, что вектор-функция $\overline{F}$ принадлежит некоторому классу вектор-функций M, а размерность пространства — n.

В статье [7] были исследованы периоды для вектор-функций следующих классов над $\mathbf{P}_2$:

1)$\overline{\mathbf{T}}_{\overline{c}} = \{\overline{F} | \overline{F}(\ \overline{c}\ ) = \overline{c}\}$ — класс вектор-функций, сохраняющих константу $\overline{c}$.

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

3) $\overline{M} = \{\overline{F} | f_i \in M, 1 \leqslant i \leqslant n\}$ — *класс монотонных вектор-функций.*

Исследуем эту же задачу для $\overline{L} = \{\overline{F} | f_i \in L, 1 \leqslant i \leqslant n\}$ — *класса линейных вектор-функций.*

Задача оценки периода для линейной рекуррентной последовательности была рассмотрена во многих работах (см., например, [8]). Там были оценки вида q^k и $q^k - 1$, что совпадает с оценками настоящей статьи при $q = 2$ и $k = n$.

Этот факт является следствием того, что в этих работах рассматриваются конечные поля. Однако, в случае класса линейных вектор-функций автору не удалось обнаружить процедуру, которая для любого натурального числа n дает способ построения линейной рекуррентной последовательности порядка n, на которой верхняя оценка достижима.

Для линейных вектор-функций получены следующие результаты:

Теорема 1. *Пусть существует матрица C, такая что при любом векторе $\overline{x} \neq \overline{0}$ выполнено $C\overline{x} \neq \overline{0}$. Обозначим $\overline{F}_{\overline{q}}(\overline{x}) = C\overline{x} \oplus \overline{q}$. Пусть для некоторого вектора $\overline{q}$ выполнено равенство $|\ \mathbf{БД}(\overline{F}_{\overline{0}}, n, \overline{q})\ | = p$. Тогда $|\ \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0})\ | \geqslant p$.*

Эта теорема позволяет для $p \leqslant 2^n - 1$ получать четные периоды

$| \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0}) | = 2p$, если $\sum\limits_{j=0}^{p-1} C^j \overline{q} \neq \overline{0}$.

Но какой максимальный период можно получить? На этот вопрос частично дает ответ

Теорема 2. *1. Если $n \geqslant 3$, то для любой вектор-функции* $| \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0}) | < 2^n$.
2. Если $n < 3$, то существует вектор-функция $\overline{F}_{\overline{q}}$, для которой $| \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0}) | = 2^n$.

При $n \geqslant 3$ наша задача эквивалентна задаче о нахождении максимального периода на множестве вектор-функций $\overline{F}_{\overline{0}}(\overline{x}) = C\overline{x}$, сохраняющих нулевой вектор.

В самом деле, пусть для некоторого натурального числа n мы нашли вектор-функцию $\overline{F}_{\overline{q}}$, такую что $| \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{x}) | = 2^n - 1$ при любом $\overline{x} \neq \overline{x}_q$.

Ясно, что $\overline{F}_{\overline{q}}(\overline{x}_q) = \overline{x}_q$. Иначе существует вектор, отличный от $\overline{x}_q$, который сохраняет вектор-функция $\overline{F}_{\overline{q}}$ — противоречие с условием. Значит, $\overline{q} = \overline{x}_q \oplus C\overline{x}_q$. $\overline{F}_{\overline{0}}(\overline{x}) = C\overline{x} = \overline{F}_{\overline{q}}(\overline{x}) \oplus \overline{q} = \overline{F}_{\overline{q}}(\overline{x}) \oplus \overline{x}_q \oplus C\overline{x}_q = \overline{F}_{\overline{q}}(\overline{x} \oplus \overline{x}_q) \oplus \overline{x}_q$.

$\overline{F}^{(i)}_{\overline{0}}(\overline{x}) = \overline{F}_{\overline{q}}(\overline{F}^{(i-1)}_{\overline{q}}(\overline{x} \oplus \overline{x}_q)) \oplus \overline{x}_q \oplus \overline{x}_q) \oplus \overline{x}_q = \overline{F}^{(i)}_{\overline{q}}(\overline{x} \oplus \overline{x}_q) \oplus \overline{x}_q$. Поэтому $| \mathbf{БД}(\overline{F}_{\overline{0}}, n, \overline{x} \oplus \overline{x}_q) | = | \mathbf{БД}(C, n, \overline{y}) | = 2^n - 1$ для любого $\overline{x} \neq \overline{x}_q$ $(\overline{y} \neq \overline{0})$.

Обратно, поскольку $| \mathbf{БД}(C, n, \overline{y}) | = 2^n - 1$ для любого $\overline{y} \neq \overline{0}$, то найдутся такие $\overline{z} \neq \overline{0}$ и $s > 0$, что $\overline{z} \oplus C\overline{z} = \overline{t}$ и $C^s(\overline{t}) = \overline{r}$. Положим $\overline{x}_r = C^s(\overline{z})$. Тогда $\overline{F}_{\overline{r}}(\overline{y}) = C\overline{y} \oplus \overline{r} = C\overline{y} \oplus \overline{x}_r \oplus C\overline{x}_r = C(y \oplus \overline{x}_r) \oplus \overline{x}_r$. Таким образом, $\overline{F}_{\overline{r}}(\overline{x}) = \overline{F}_{\overline{q}}(\overline{x} \oplus \overline{x}_q \oplus \overline{x}_r) \oplus \overline{x}_q \oplus \overline{x}_r$. Следовательно, $| \mathbf{БД}(\overline{F}_{\overline{r}}, n, \overline{x}) | = 2^n - 1$ для любого $\overline{x} \neq \overline{x}_r$.

Это означает, что если существует вектор-функция $\overline{F}_{\overline{q}}$, такая что $| \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{x}) | = 2^n - 1$ при любом $\overline{x} \neq \overline{x}_q$ и некотором n, то для любого r существует $\overline{x}_r$, такое что $| \mathbf{БД}(\overline{F}_{\overline{r}}, n, \overline{x}) | = 2^n - 1$ при любом $\overline{x} \neq \overline{x}_r$.

Поскольку при $n \geqslant 3$ максимальный период $| \mathbf{БД}(C, n, \overline{x}) | = 2^n$ не достижим, логично предположить, что может быть достигнут максимальный период $| \mathbf{БД}(C, n, \overline{x}) | = 2^n - 1$ для любого $\overline{x} \neq \overline{0}$. Для всех $n \leqslant 11$ эта гипотеза подтвердилась.

Более того, если эта гипотеза верна, то она верна и для линейных вектор-функций, которые можно представить в виде $\overline{F}(\overline{x}) = C\overline{x}$, где матрица C из следующей теоремы.

Теорема 3. *Пусть A — матрица размера $(n-1)\times(n-1)$, и при $\overline{x'} \neq \overline{0}$ выполнено равенство: $|\,\mathbf{БД}(A, n-1, \overline{x'})\,| = 2^{n-1}-1$. Построим матрицу C размера $n \times n$ следующим образом:*

$C = \begin{pmatrix} A & A\overline{b} \\ (A\overline{b})^T & d \end{pmatrix}$, *где $d = (\overline{b}^T A\overline{b} \oplus 1)$ и $\overline{b} \neq \overline{0}$.*

Тогда никакой вектор $\overline{x}$ не лежит в предпериоде $\mathbf{БД}(C, n, \overline{x})$, то есть все вектора при помощи матрицы C переходят в себя.

Эту теорему можно усилить:

Теорема 4. *Пусть A — матрица размера $(n-1)\times(n-1)$, A не обладает предпериодом, и $C = \begin{pmatrix} A & A\overline{b} \\ (A\overline{b})^T & d \end{pmatrix}$. Матрица C не обладает предпериодом тогда и только тогда, когда $d = (\overline{b}^T A\overline{b} \oplus 1)$.*

Теперь, благодаря теореме 3, можно задать рекурсивный алгоритм построения матриц, дающих период $\mathbf{БД}(C, n, \overline{x}) = 2^n - 1$. Для этого необходимо задать вектор $\overline{b}$.

Ограничение на этот вектор накладывает

Утверждение 1. *Пусть $C = \begin{pmatrix} A & A\overline{b} \\ (A\overline{b})^T & d \end{pmatrix}$, где $d = (\overline{b}^T A\overline{b} \oplus 1)$ и $|\,\mathbf{БД}(A, n, \overline{b})\,| = 2^n - 1$. Если $(\overline{b}^T)(A \oplus E)^{-1} A\overline{b} = 1$, то ни один вектор $\begin{pmatrix} \overline{x_1} \\ y_1 \end{pmatrix} \neq \overline{0}$ не переходит в себя.*

3. Доказательство теорем 1 и 2

Пусть $\mathbf{БД}(C, n, \overline{q}) = \{\overline{q}, C\overline{q}, C^2\overline{q}, \cdots, C^{p-1}\overline{q}\}$, где $\overline{q} \neq \overline{0}$. Пусть $\sum\limits_{j=0}^{L} C^j\overline{q} = \overline{0}, L < 2p-1$. Тогда $C^{L+1}\overline{q} = C(C^L\overline{q}) = C(\sum\limits_{j=0}^{L-1} C^j\overline{q}) =$

$\sum\limits_{j=0}^{L} C^j\overline{q} \oplus \overline{q} = \overline{q}$. Это выполнено тогда и только тогда, когда L делится на p. То есть $\sum\limits_{j=0}^{L} C^j\overline{q} \neq \overline{0}$ для любого $L < 2p-1$ и $L \neq p$.

Пусть $\sum\limits_{j=0}^{L_1} C^j\overline{q} = \sum\limits_{j=0}^{L_2} C^j\overline{q}$, $L_1 < L_2 \leqslant p-1$. Тогда $C^{|L_1-L_2|}(\sum\limits_{j=0}^{\min(L_1,L_2)} C^j\overline{q}) = \overline{0}$. Следовательно, существует $L = \min(L_1, L_2) < p-1$, такое что $\sum\limits_{j=0}^{L} C^j\overline{q} = \overline{0}$ — противоречие. Значит, для любых $L_1 < L_2 \leqslant p-1$ $\sum\limits_{j=0}^{L_1} C^j\overline{q} \neq \sum\limits_{j=0}^{L_2} C^j\overline{q}$.

Рассмотрим $\mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0}) = \{\overline{0}, \overline{q}, \cdots, \sum\limits_{j=0}^{p-1} C^j\overline{q}, \cdots\}$. Из доказанного выше следует, что все элементы этого множества различны и $|\ \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0})\ | = 2p$, если $\sum\limits_{j=0}^{p-1} C^j\overline{q} \neq \overline{0}$ и $|\ \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0})\ | = p$, иначе.

Теорема 1 доказана.

Для доказательства теоремы 2 нам понадобится следующая лемма.

Лемма 1. *$|\ \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0})\ | = 2^n$ тогда и только тогда, когда $|\ \mathbf{БД}(C, n, \overline{q})\ | = p = 2^{n-1}$ и $\sum\limits_{j=0}^{p-1} C^j\overline{q} \neq \overline{0}$.*

Доказательство. 1. Пусть $|\ \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0})\ | = 2^n$. Если $\overline{q}$ принадлежит предпериоду, то существуют такие $\overline{x} \neq \overline{y}$, что $C\overline{x} = C\overline{y}$. Тогда $\overline{F}_{\overline{q}}(\overline{x}) = \overline{F}_{\overline{q}}(\overline{y})$ — противоречие с условием. Значит, существует $p > 0$, где $C^p\overline{q} = \overline{q}$. Но тогда $\sum\limits_{j=0}^{2p-1} C^j\overline{q} = \overline{0}$. Следовательно, $p = 2^{n-1}$, и $\sum\limits_{j=0}^{p-1} C^j\overline{q} \neq \overline{0}$, так как иначе $|\ \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0})\ | \neq 2^n$.

2. Пусть $|\ \mathbf{БД}(C, n, \overline{q})\ | = p = 2^{n-1}$ и $\sum\limits_{j=0}^{p-1} C^j\overline{q} \neq \overline{0}$.

Пусть $\sum\limits_{j=0}^{L} C^j\overline{q} = \overline{0}$, $L < 2p-1$. Тогда $C^{L+1}\overline{q} = C(C^L\overline{q}) = C(\sum\limits_{j=0}^{L-1} C^j\overline{q})$ $= \sum\limits_{j=0}^{L} C^j\overline{q} \oplus \overline{q} = \overline{q}$. Это выполнено тогда и только тогда, когда L делится на 2^{n-1}. То есть $\sum\limits_{j=0}^{L} C^j\overline{q} \neq \overline{0}$ для любого $L < 2p-1$.

Пусть существует $\overline{x} \neq \overline{0}$ такой, что $C\overline{x} = \overline{0}$. Тогда по определению $\overline{z}$ и $\overline{z} \oplus \overline{x}$ не принадлежат одновременно $\mathbf{БД}(C, n, \overline{q})$ для любого $\overline{z}$. Вектора $\overline{x}$ и $\overline{0}$ по построению не принадлежат $\mathbf{БД}(C, n, \overline{q})$. Следовательно, $|\ \mathbf{БД}(C, n, \overline{q}\ )| \leqslant 2^{n-1} - 1$ — противоречие с условием. Значит, $C\overline{x} \neq \overline{0}$ для любого $\overline{x} \neq \overline{0}$.

Пусть $\sum\limits_{j=0}^{L_1} C^j\overline{q} = \sum\limits_{j=0}^{L_2} C^j\overline{q}$, $L_1 < L_2 \leqslant 2p-1$. Тогда $C^{|L_1-L_2|}(\sum\limits_{j=0}^{\min(L_1,L_2)} C^j\overline{q}) = \overline{0}$. Следовательно, существует $L = \min(L_1, L_2) < 2p-1$, такое что $\sum\limits_{j=0}^{L} C^j\overline{q} = \overline{0}$ — противоречие. Таким образом, для любого $L_1 < L_2 \leqslant 2p-1$ выполнено неравенство $\sum\limits_{j=0}^{L_1} C^j\overline{q} \neq \sum\limits_{j=0}^{L_2} C^j\overline{q}$.

Рассмотрим $\mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0}) = \{\overline{0}, \overline{q}, \cdots, \sum\limits_{j=0}^{p-1} C^j\overline{q}, \cdots\}$. По доказанному, все элементы этого множества различны и $|\ \mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0})\ | = 2^n$. Лемма доказана.

4. Доказательство теоремы 2

1. Пусть $n \geqslant 2$ и $\mathbf{БД}(\overline{F}_{\overline{q}}, n, \overline{0}) = 2^n$. По лемме $\mathbf{БД}(C, n, \overline{q}) = p = 2^{n-1}$ и $\overline{t} = \sum\limits_{j=0}^{p-1} C^j\overline{q} \neq \overline{0}$.

Очевидно, $C\overline{t} = C(\sum\limits_{j=0}^{p-1} C^j\overline{q}) = \sum\limits_{j=1}^{p-1} C^j\overline{q} \oplus C^p\overline{q} = \sum\limits_{j=0}^{p-1} C^j\overline{q} = \overline{t}$. Тогда для любого $\overline{x}$ из $\mathbf{БД}(C, n, \overline{q})$ существует $(\overline{x} \oplus \overline{t})$ из $\mathbf{БД}(C, n, \overline{q})$. Иначе,

$|\ \mathbf{БД}(C,n,\overline{q}\oplus\overline{t})\ |=p$ и $\mathbf{БД}(C,n,\overline{q})\wedge\mathbf{БД}(C,n,\overline{q}\oplus\overline{t})=\varnothing$. Но тогда $2p+2\leqslant 2^n$, или $p\leqslant 2^{n-1}-1$. Это противоречит условию $|\ \mathbf{БД}(\overline{F}_{\overline{q}},n,\overline{0})\ |=2^n$.

Таким образом, $\mathbf{БД}(C,n,\overline{q})=\{\overline{x_i},\overline{x_i}\oplus\overline{t}\},1\leqslant i\leqslant 2^{n-2}$.

$\sum\limits_{j=0}^{p-1}C^j\overline{q}=\sum\limits_{j=1}^{2^{n-2}}\overline{t}=\overline{0}\neq\overline{t}$, если $n>2$ и $\sum\limits_{j=0}^{p-1}C^j\overline{q}=\overline{t}$, если $n=2$. Следовательно, если $|\ \mathbf{БД}(\overline{F}_{\overline{q}},n,\overline{0})\ |=2^n$, то $n<3$.

2. Обратно,

$\underline{n=1}$. $|\ \mathbf{БД}(x\oplus 1,1,0)\ |=|\ \{0,1\}\ |=2$;

$\underline{n=2}$. $|\ \mathbf{БД}(\begin{pmatrix}1&0\\1&1\end{pmatrix}\overline{x}\oplus\begin{pmatrix}1\\0\end{pmatrix},2,\overline{0})|=|\ \{\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\}|=4$.

Теорема 2 доказана.

5. Доказательства теорем 3 и 4

Доказательство теоремы 3. Пусть существуют два различных вектора $\begin{pmatrix}\overline{x_1}\\y_1\end{pmatrix}$ и $\begin{pmatrix}\overline{x_2}\\y_2\end{pmatrix}$, которые переходят в один и тот же вектор. Если $\overline{x_i}=\overline{0}$, то очевидно.

Положим $A\overline{b}=\overline{q}$, $\overline{x_i}=A^{j_i}\overline{b}$, $i=1,2$. Тогда $\overline{b}^T(A^{j_1}\oplus y_1E)\overline{q}\oplus y_1=\overline{b}^T(A^{j_2}\oplus y_2E)\overline{q}\oplus y_2$ и $(A^{j_1}\oplus y_1E)\overline{q}=(A^{j_2}\oplus y_2E)\overline{q}$.

Это значит, что $(y_1\oplus y_2)\overline{b}^T\overline{q}=(y_1\oplus y_2)\overline{b}^T\overline{q}\oplus 1\leftrightarrow y_1=y_2$. Но тогда $A^{j_1}\overline{q}=A^{j_2}\overline{q}\leftrightarrow j_1=j_2\leftrightarrow\overline{x}_1=\overline{x}_2$.

Теорема 3 доказана.

Доказательство теоремы 4. Матрица M имеет предпериод тогда и только тогда, когда существует ненулевой вектор, который переходит в ноль.

1. Пусть C периодическая матрица. Тогда $C\begin{pmatrix}\overline{b}\\1\end{pmatrix}=\begin{cases}\overline{0}\\d\oplus\overline{b}^TA\overline{b}\end{cases}=\begin{pmatrix}\overline{0}\\1\end{pmatrix}$. Отсюда $d=(\overline{b}^TA\overline{b}\oplus 1)$.

2. Пусть $d=(\overline{b}^TA\overline{b}\oplus 1)$, и C обладает предпериодом. Тогда существует такой ненулевой вектор $\begin{pmatrix}\overline{x}\\y\end{pmatrix}$, что $C\begin{pmatrix}\overline{x}\\y\end{pmatrix}=$

$\left\{ \begin{array}{l} A(\overline{x} \oplus y\overline{b}), \\ \overline{b}^T A\overline{x} \oplus y \cdot d \end{array} \right. = \left\{ \begin{array}{l} \overline{0}, \\ 0 \end{array} \right.$.

Если $y = 0$, то из первого уравнения системы следует, что и $\overline{x} = \overline{0}$. Это так, потому что A не обладает предпериодом.

Если $y = 1$, то из первого уравнения системы следует, что $\overline{x} = \overline{b}$, а из второго уравнения системы следует, что $d = \overline{b}^T A\overline{b}$.

Теорема доказана.

6. Доказательство утверждения

Пусть $C = \begin{pmatrix} A & A\overline{b} \\ (A\overline{b})^T & d \end{pmatrix} : \begin{pmatrix} \overline{x}_1 \\ y_1 \end{pmatrix} \to \begin{pmatrix} \overline{x}_1 \\ y_1 \end{pmatrix}$, или $\left\{ \begin{array}{l} A\overline{x}_1 \oplus y_1 \cdot A\overline{b} \\ \overline{b}^T A\overline{x}_1 \oplus y_1 \cdot d \end{array} \right.$.

Умножим первое равенство на $\overline{b}^T$.

$\left\{ \begin{array}{l} \overline{x}^T A\overline{x}_1 \oplus y_1 \cdot \overline{b}^T A\overline{b} \\ \overline{x}^T A\overline{x}_1 \oplus y_1 \cdot \overline{b}^T A\overline{b} \end{array} \right. = \begin{pmatrix} \overline{b}^T \cdot \overline{x}_1 \\ 0 \end{pmatrix}$. Следовательно, $\overline{b}^T \cdot \overline{x}_1 = 0$.

Тогда

1. если $y_1 = 0$, то $\forall \overline{t} \in \mathbf{БД}(A, n, \overline{b})$ выполнено $\overline{x}_1^T \cdot \overline{t} = 0$ и $A\overline{x}_1 = \overline{x}_1$;

2. если $y_1 = 1$, то $\overline{x}_1^T \cdot \overline{b} = 0$ и $\overline{x}_1 \oplus A\overline{x}_1 = A\overline{b}$.

Действительно,

1. $\left\{ \begin{array}{l} A\overline{x}_1 \\ \overline{b}^T A\overline{x}_1 \end{array} \right. = \left\{ \begin{array}{l} \overline{x}_1 \\ 0 \end{array} \right.$.

2. $\left\{ \begin{array}{l} A\overline{x}_1 \oplus A\overline{b} \\ \overline{b}^T A\overline{x}_1 \oplus \overline{b}^T A\overline{b} \end{array} \right. = \left\{ \begin{array}{l} \overline{x}_1 \\ 0 \end{array} \right.$.

Но $|\, \mathbf{БД}(A, n, \overline{b}) \,| = 2^n - 1$. Поэтому $\left\{ \begin{array}{l} \overline{x}_1^T \cdot \overline{b} = 0, \\ \overline{x}_1 \oplus A\overline{x}_1 = A\overline{b} \end{array} \right.$.

Второе уравнение $\overline{x}_1 \oplus A\overline{x}_1 = A\overline{b}$ имеет единственное решение $\overline{x}_1 = (A \oplus E)^{-1} A\overline{b}$, так как $A \oplus E = A^{2^n} \oplus E = (A \oplus E)^{2^n}$, или $(A \oplus E)^{2^n - 1} = E$.

Подставляя $\overline{x}_1$ в первое уравнение, получаем $\overline{b}^T \cdot \overline{x}_1 = \overline{b}^T (A \oplus E)^{-1} A\overline{b} = 0$, что противоречит условию.

Утверждение доказано.

В заключение автор хотел бы выразить искреннюю благодарность своему научному руководителю к.ф.-м.н. А.С. Строгалову за активное участие в обсуждении работы, к.ф.-м.н. В.А. Носову за помощь в подборе литературы и конструктивные замечания, проф. В.Б. Кудрявцеву за неоднократные и полезные обсуждения полученных результатов и поддержку.

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.

[4] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. М.: Наука, 1985.

[5] Гилл А. Введение в теорию конечных автоматов. / Пер. с англ. Дауровой А.Т. и др. / Под ред. Пархоменко П.П. М.: Наука, 1966.

[6] Гилл А. Линейные последовательностные машины. Анализ синтез и применение. / Пер. с англ. Бернштейна А.С. / Под ред. Цыпкина Я.З. М.: Наука, 1974.

[7] Матвеев А.В. Оценки мощности некоторых итеративных множеств // Интеллектуальные системы. М., 1999. Т. 4. Вып. 3–4. С. 295–306.

[8] Лидл Р., Нидеррайтер Г. Конечные поля. / Пер. с англ. Жукова А.Е. и Петрова В.И. / Под ред. Нечаева В.И. М.: Мир, 1988. Т. 2.