МИКРОЭЛЕКТРОНИКА, 2020, том 49, № 1, с. 3–17

КВАНТОВАЯ ИНФОРМАТИКА

УДК 621.382

О СВЯЗИ БУЛЕВОЙ АЛГЕБРЫ С КВАНТОВОЙ ИНФОРМАТИКОЙ

© 2020 г. Ю. И. Богданов[a, b, c, *], Н. А. Богданова[a, b], Д. В. Фастовец[a, b, **], В. Ф. Лукичев[a]

[a] *Физико-технологический институт имени К.А. Валиева Российской АН, Нахимовский проспект, 36, корп. 1, Москва, 117218 Россия*

[b] *Национальный исследовательский университет МИЭТ, пл. Шокина, 1, Зеленоград, Москва, 124498 Россия*

[c] *Национальный исследовательский ядерный университет МИФИ, Каширское ш., 31, Москва, 115409 Россия*

**e-mail: bogdanov_yurii@inbox.ru*

***e-mail: fast93@mail.ru*

Поступила в редакцию 14.06.2019 г.
После доработки 25.07.2019 г.
Принята к публикации 25.07.2019 г.

Рассматривается фундаментальная взаимосвязь между квантовой физикой и дискретной математикой. Описан метод представления булевых функций в виде унитарных преобразований. Рассмотрен вопрос о связи полиномов Жегалкина, определяющих алгебраическую нормальную форму булевой функции, с квантовыми схемами. Показано, что квантово-информационный язык предоставляет простой алгоритм построения полинома Жегалкина на основе таблицы истинности. Разработанные методы и алгоритмы обобщены на случай произвольной булевой функции с многобитовой областью определения и многобитовым множеством значений, а также на случай многозначных (k-значных) логик, когда $k = p$-простое число. Разработанный подход имеет существенное значение для реализации квантовых компьютерных технологий и является основой для перехода от классической машинной логики к квантовому аппаратному обеспечению.

DOI: 10.31857/S0544126920010044

1. ВВЕДЕНИЕ

Дискретная математика – важный раздел математики, который исследует свойства различных дискретных объектов: графы [1], булевы функции [2, 3], конечные автоматы и т.д. Методы дискретной математики успешно применяются в различных областях, включая реализацию логических элементов электронных устройств, оптимизацию транспортных путей сообщения, построение бизнес-моделей и т.д.

Свойства булевых функций находят широкое применение в вопросах информационной безопасности [4–6]. Все аппаратно-программные средства, предназначенные для обеспечения безопасности передаваемой информации, должны обладать рядом криптографических свойств. Особенности используемых средств защиты находят свое отражение в булевых математических моделях в виде ряда специфических свойств используемых булевых функций (или систем булевых функций).

В настоящее время все большее внимание исследователей привлекают перспективы применения квантовых методов обработки информации к задачам криптографии [7–12].

Дискретные системы также активно исследуются в рамках квантовой механики и квантовой теории информации. Понятия дискретизации и квантования аналогичны по содержанию. Однако, долгие годы, дискретная математика развивалась без видимой связи с квантовой теорией – истинной наукой о дискретных объектах.

Такой важный объект дискретной математики, как полином Жегалкина [13] находит интересное и важное применение при построении квантовых схем. Оказывается, что множество всех полиномов Жегалкина и набор квантовых схем, состоящих из гейта X и его условных аналогов, связаны посредством инъективного отображения. Другими словами, любому полиному Жегалкина можно поставить в соответствие квантовую схему. Этот факт подробно описан ниже в тексте данной статьи. Важной особенностью является простота построения схемы. Кроме того, нами продемонстрирован эффективный метод построения полинома Жегалкина по таблице истинности исходной функции.

Наличие гейтов X, $CNOT$, $CCNOT$ и т.д. в схемах, построенных по полиномам Жегалкина, объясняется тем фактом, что в классической логике существуют аналогичные преобразования [14]. Квантовая механика предоставляет, кроме того, ресурсы в виде унитарных операций, которые не только позволяют построить квантовые аналоги классических схем, но и обобщить их,

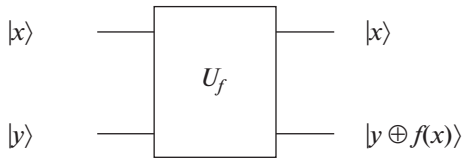


Рис. 1. Схема реализации квантового аналога булевой функции $f(x)$.

например, введя обратное преобразование, соответствующее булевой функции, а также рассматривая квантовые суперпозиции базисных состояний. Таким образом, квантовые булевы функции являются более совершенными объектами по сравнения с классическими битовыми функциями. Заметим также, что сами квантовые булевы функции являются только подмножеством гораздо более широкого класса квантовых преобразований.

Основная современная инфраструктура информационного сообщества основана на принципах булевой алгебры и методах дискретной математики. Информационные технологии являются основным драйвером мировой экономики, начиная с середины 20-го столетия по сей день. В настоящее время становится все более очевидным, что в ближайшие годы и десятилетия драйвером развития самих информационных технологий должны стать квантовые информационные технологии. Таким образом, необходима интеграция методов дискретной математики и квантовой информатики.

2. ПРЕДСТАВЛЕНИЕ БУЛЕВОЙ ФУНКЦИИ НА ЯЗЫКЕ УНИТАРНЫХ ПРЕОБРАЗОВАНИЙ

В теории квантовой информации доказано, что любую булеву функцию $f(x)$ можно представить в виде квантового преобразования [15, 16]:

$$|x, y\rangle \xrightarrow{f} |x, y \oplus f(x)\rangle. \quad (1)$$

Здесь символом x обозначен регистр из n кубитов—регистр области определения булевой функции (еще его называют регистром данных или регистром запроса). Символом y обозначен регистр множества значений, который может быть как однокубитовым, так и многокубитовым. Символ $\oplus$ означает сложение по модулю 2.

Графическое представление формулы (1) показано на рис. 1. Многокубитовый гейт U_f осуществляет преобразование, задаваемое булевой функцией $f(x)$.

Следует заметить, что, если на вход квантовой схемы подается регистр $|y\rangle$ в нулевом состоянии, то на выходе мы получим регистр значений, содержащий значения функции $f(x)$. Данное преобразование представляет собой частный случай (1):

$$|x, 0\rangle \xrightarrow{f} |x, f(x)\rangle.$$

В настоящем разделе мы будем считать что регистр запроса состоит из n кубитов, а регистр значений – из одного кубита. В этом случае матрица, соответствующая гейту U_f, будет иметь размер $2^{n+1} \times 2^{n+1}$. В разделе 4 мы представим обобщение на булевы функции с многобитовым множеством значений.

Рассмотрим вначале простейший случай – булеву функцию $f(x)$ с однобитовыми областью определения и множеством значений. Всего существует 4 таких функции, и все они представлены в табл. 1.

В булевой алгебре приняты следующие обозначения: $f_0 = 0$, $f_3 = 1$ – постоянные функции, а $f_1 = x$, $f_2 = x \oplus 1$ – переменные функции. На основе определения (1) легко построить четыре унитарных матрицы, реализующие квантовые аналоги этих четырех функций:

$$U_0 = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}, U_1 = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}, U_2 = \begin{pmatrix} X & 0 \\ 0 & I \end{pmatrix}, U_3 = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}, \quad (2)$$

Таблица 1. Таблица истинности однобитовых функций

x	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

где $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ – единичная матрица, а $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ – матрица, соответствующая операции логического отрицания. Стоит также заметить, что представленный в матрице ноль – это матричный ноль $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Все представленные матрицы (2) име-

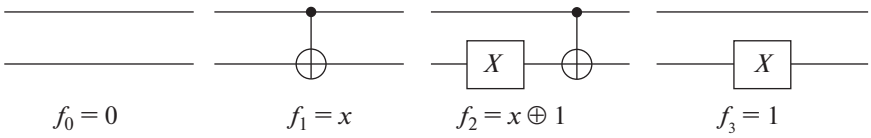


Рис. 2. Квантовые схемы для однобитовых булевых функций.

ют блочно-диагональный вид и принцип их построения очень прост: нулю в таблице истинности сопоставляется матрица I, а единице – матрица X. Математически это можно представить в следующем виде:

$$U_f = \mathrm{diag}\left(fX + \bar{f}I\right), \tag{3}$$

где $\mathrm{diag}(x)$ – функция, возвращающая матрицу, с элементами вектора x на главной диагонали. В данной формуле под символом f подразумевается вектор выходных значений, соответствующих рассматриваемой булевой функции $f(x)$. Запись $\bar{f}$ означает логическое отрицание над каждым элементом двоичного вектора f. Также отметим, что в этой формуле, под символами I и X понимаются именно блоки матрицы U_f, то есть, с ними следует оперировать как с числами.

Аналогичный принцип построения булевых функций сохраняется и для многобитовых булевых функций. При этом матрица преобразования U_f для n-битовой булевой функции будет состоять из 2^n блоков, каждый из которых есть либо I, либо X. Сформулируем данный принцип построения в виде общего утверждения:

Утверждение 1 (о блочно-диагональном характере булевых преобразований)
Унитарная матрица, отвечающая булевой функции, имеет блочно-диагональный вид, причем, значениям функции $f(x) = 0$ соответствует матрица I, а значениям функции $f(x) = 1$ соответствует матрица X. Предполагается, что значения аргумента x для n-битовой функции упорядочены в порядке возрастания от 0 до $2^n - 1$.

Из булевой алгебры известно, что всего существует 2^{2^n} n-битовых булевых функций. Этот факт также напрямую следует из Утверждения 1. Следует заметить, что формула (3), введенная для однобитовых функций, также справедлива и для n-битовых функций. Таким образом, формула (3) – есть математическое описание Утверждения 1.

Квантовые преобразования удобно представлять в виде графических схем. Квантовые схемы для четырех рассмотренных выше однобитовых булевых функций представлены на рис. 2.

Функции $f_0 = 0$, соответствующей тождественному преобразованию, отвечают просто два “голых” квантовых провода. Функции $f_3 = 1$ соответствует действие на нижний кубит (регистр результатов) безусловного оператора отрицания X (NOT). Функции $f_1 = x$ отвечает очень важный для квантовых вычислений логический элемент условного отрицания CNOT – так называемое управляемое (условное) – НЕ (Controlled-Not) преобразование. Наконец, функции $f_2 = x \oplus 1$ отвечает последовательное действие операторов CNOT и X (NOT).

Сложение (по модулю два) двух булевых функций-столбцов, в соответствии с Утверждением 1, сводится к умножению двух блочно-диагональных унитарных матриц. При этом матричное тождество $I \cdot I = I^2 = I$ соответствует булеву тождеству $0 + 0 = 0$; матричное соотношение $I \cdot X = X \cdot I = X$ соответствует булеву соотношению $0 + 1 = 1 + 0 = 1$; наконец матричное тождество $X \cdot X = X^2 = I$ соответствует булеву тождеству $1 + 1 = 0$. Здесь и далее в тексте, под знаком суммы мы подразумеваем сложение по модулю 2.

Обозначим область определения x однобитовой булевой функции через одноименный вектор-столбец $x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Этот вектор будем рассматривать в качестве базисного вектора e_1 двумерного векторного пространства $e_1 = x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. В качестве второго базисного вектора будет выступать вектор-столбец $e_0 = x + 1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Булевой функции, соответствующей вектору e_0, отвечает полином $1 + x = 1 \cdot x^0 + 1 \cdot x^1$, коэффициенты которого образуют вектор-столбец $p_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Здесь

$x^0 = \begin{pmatrix}1\\1\end{pmatrix}$, $x^1 = \begin{pmatrix}0\\1\end{pmatrix}$ – нулевая и первая степени вектора $x = \begin{pmatrix}0\\1\end{pmatrix}$. А булевой функции, соответствующей вектору e_1, отвечает полином $x = 0 \cdot x^0 + 1 \cdot x^1$, коэффициенты которого образуют вектор-столбец $p_1 = \begin{pmatrix}0\\1\end{pmatrix}$. Выражение для базисных функций e_0 и e_1 мы трактуем, прежде всего, как функции-столбцы, отвечающие некоторым полиномам от векторного аргумента $x = \begin{pmatrix}0\\1\end{pmatrix}$. Само выражение $e_0 = x + 1$ можно трактовать, одновременно, и традиционно, как числовую функцию: $e_0 = 1$ при $x = 0$ и $e_0 = 0$ при $x = 1$. Удобство векторной записи в том, что она представляет рассматриваемую логическую функцию целиком, как единый объект. Удобство векторов-столбцов p_0 и p_1 в том, что они представляют в качестве единых объектов коэффициенты рассматриваемых полиномов. Как мы увидим ниже, представленные элементарные соображения для однобитовых логических функций позволят нам легко получать нетривиальные результаты в многобитовом случае, фактически обеспечив автоматизацию соответствующих вычислений.

Базисные векторы-столбцы e_0 и e_1, объединенные вместе, образуют единичную матрицу

$$I = [e_0\ e_1] = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}.$$

Аналогично, векторы-столбцы p_0 и p_1, объединенные вместе, образуют следующую матрицу:

$$P = [p_0\ p_1] = \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}.$$

Базисные векторы e_0 и e_1, так же как и векторы-столбцы p_0 и p_1, введенные нами для описания однобитовых функций, составляют основу и для представления многобитовых функций. Такое рассмотрение мы проведем с использованием полиномов Жегалкина и соответствующих им квантовых схем. Мы увидим, что использование базисных векторов e_0 и e_1 позволяет нам просто и наглядно выписать полином Жегалкина в аналитическом виде. В свою очередь, использование векторов-столбцов p_0 и p_1 позволяет очевидным образом автоматизировать весь процесс нахождения коэффициентов полинома Жегалкина, избавив нас от громоздкой процедуры раскрытия скобок и приведения подобных слагаемых.

3. ПРЕДСТАВЛЕНИЕ ПОЛИНОМА ЖЕГАЛКИНА В ВИДЕ КВАНТОВОЙ СХЕМЫ

Перейдем к рассмотрению двухбитовых булевых функций ($n = 2$). Развивая описание на языке вектор-столбцов, логично определить двухбитовые базисные векторы через тензорное произведение однобитовых векторов, например:

$$e_{00} = e_0 \otimes e_0 = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}.$$

С другой стороны $e_0 = 1 + x_1$ для первого бита и $e_0 = 1 + x_2$ для второго бита, поэтому получаем сразу следующий полином Жегалкина:

$$e_{00} = (1 + x_1)(1 + x_2) = 1 + x_2 + x_1 + x_1x_2 = x_1^0x_2^0 + x_1^0x_2^1 + x_1^1x_2^0 + x_1^1x_2^1.$$

Справа мы представили полином Жегалкина в лексикографическом порядке по показателям степени (00, 01, 10, 11).

Используя, введенные ранее, вектор-столбцы коэффициентов получаем тот же результат для коэффициентов полинома Жегалкина:

$$p_{00} = p_0 \otimes p_0 = \begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1\\1\\1\\1\end{pmatrix}.$$

Таким образом, вектору e_{00} соответствует столбец

$$e_{00} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

в таблице истинности и, одновременно, полином Жегалкина

$$e_{00} = 1 + x_2 + x_1 + x_1x_2 = x_1^0x_2^0 + x_1^0x_2^1 + x_1^1x_2^0 + x_1^1x_2^1,$$

коэффициенты которого есть

$$p_{00} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Трехкубитовая квантовая схема, отвечающая данному полиному, представлена на рис. 3 слева. Два верхних кубита отвечают области определения функции, третий кубит – множеству значений. Слагаемому x_1x_2 отвечает гейт CCNOT (два верхних кубита управляют нижним); слагаемому x_1 отвечает гейт CNOT, в котором верхний кубит управляет нижним; слагаемому x_2 отвечает гейт CNOT, в котором средний кубит управляет нижним; наконец слагаемому 1 отвечает однокубитовый гейт X (NOT), который действует на нижний кубит. Аналогично, для трех оставшихся базисных векторов получаем следующие выражения:

$$e_{01} = e_0 \otimes e_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = (1 + x_1)x_2 = 0 \cdot x_1^0x_2^0 + 1 \cdot x_1^0x_2^1 + 0 \cdot x_1^1x_2^0 + 1 \cdot x_1^1x_2^1, \quad p_{01} = p_0 \otimes p_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix},$$

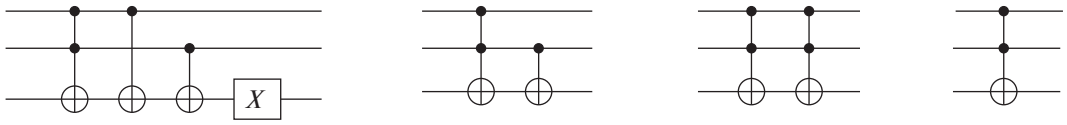
$$e_{10} = e_1 \otimes e_0 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = x_1(1 + x_2) = 0 \cdot x_1^0x_2^0 + 0 \cdot x_1^0x_2^1 + 1 \cdot x_1^1x_2^0 + 1 \cdot x_1^1x_2^1, \quad p_{10} = p_1 \otimes p_0 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix},$$

$$e_{11} = e_1 \otimes e_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = x_1x_2 = 0 \cdot x_1^0x_2^0 + 0 \cdot x_1^0x_2^1 + 0 \cdot x_1^1x_2^0 + 1 \cdot x_1^1x_2^1, \quad p_{11} = p_1 \otimes p_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Мы видим, что векторы-столбцы p_{00}, p_{01}, p_{10} и p_{11} в точности задают коэффициенты полиномов Жегалкина, которые отвечают базисным двухбитовым функциям e_{00}, e_{01}, e_{10} и e_{11} соответственно. При этом, столбец p_{00} задает полином e_{00}, столбец p_{01} определяет полином e_{01} и т.д. Все рассматриваемые функции представлены графически на рис. 3.

Всего существует 16 двухбитовых булевых функций (табл. 2). Мы описали 4 функции, которые являются базисными. Все остальные 12 функций могут быть представлены как суперпозиции четырех базисных, например:

$$e_{00} + e_{01} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 1 + x_2 + x_1 + x_1x_2 + x_2 + x_1x_2 = 1 + x_1 = 1 \cdot x_1^0x_2^0 + 0 \cdot x_1^0x_2^1 + 1 \cdot x_1^1x_2^0 + 0 \cdot x_1^1x_2^1.$$



$e_{00} = x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ $e_{01} = x_1x_2 \oplus x_2$ $e_{10} = x_1x_2 \oplus x_1$ $e_{11} = x_1x_2$

Рис. 3. Квантовые схемы для двухбитовых базисных булевых функций.

Проводя то же самое вычисление на языке p-векторов, сразу получаем правильный результат для столбца коэффициентов полинома Жегалкина:

$$p_{00} + p_{01} = \begin{pmatrix}1\\1\\1\\1\end{pmatrix} + \begin{pmatrix}0\\1\\0\\1\end{pmatrix} = \begin{pmatrix}1\\0\\1\\0\end{pmatrix}.$$

Заметим, что гейт, соответствующий полиному $e_{00} + e_{01} = 1 + x_1$, сводится к действию двухкубитового оператора CNOT (первый кубит управляет третьим) и действию однокубитового гейта X (NOT), который действует на нижний кубит.

Полученные в настоящем разделе результаты можно сформулировать в виде следующих двух утверждений.

Утверждение 2 (алгоритм построения булевой функции в виде полинома Жегалкина)

Произвольная булева функция является суперпозицией базисных функций $e_{j_1j_2\ldots j_n} = e_{j_1} \otimes e_{j_2} \otimes \ldots \otimes e_{j_n}$. Индексу j_k отвечает множитель $(x_k + 1)$ при $j_k = 0$ и множитель x_k при $j_k = 1$. Столбец коэффициентов полинома Жегалкина задается при этом суммой тензорных произведений p-столбцов базисных функций $p_{j_1j_2\ldots j_n} = p_{j_1} \otimes p_{j_2} \otimes \ldots \otimes p_{j_n}$. Индексу j_k отвечает столбец p_0 при $j_k = 0$ и столбец p_1 при $j_k = 1$.

Утверждение 3 (о преобразовании полиномов Жегалкина в квантовые схемы)

Каждому полиному Жегалкина соответствует некоторая квантовая схема. Слагаемому 1 соответствует оператор X, действующий на кубит результатов y; слагаемому x_{j_k} отвечает оператор CNOT с соответствующим управляющим кубитом; произведению из m булевых аргументов $x_{j_1}x_{j_2}\ldots x_{j_m}$ отвечает соответствующий оператор $C^{(m)}NOT$, где $m = 1,\ldots,n$, n – число битов в области определения.

Из Утверждения 3 следует, что каждому слагаемому в полиноме Жегалкина сопоставляется некоторый гейт (вентиль). Перечислим все возможные вентили такого рода. Имеется $C_n^0 = 1$ гейт X, действующий непосредственно на кубит результатов, имеется $C_n^1 = n$ различных гейтов $CNOT$, C_n^2 гейтов $C^{(2)}NOT$ и т.д. Таким образом, полный набор базовых вентилей содержит $\sum_{k=0}^{n} C_n^k = 2^n$ элементов. Каждый из элементов-вентилей может

Таблица 2. Таблица истинности для 16 возможных двухбитовых булевых функций

x_1	x_2	e_{00}	e_{01}	e_{10}	e_{11}	$e_{00} + e_{01}$	$e_{00} + e_{10}$	$e_{00} + e_{11}$	$e_{01} + e_{10}$
0	0	1	0	0	0	1	1	1	0
0	1	0	1	0	0	1	0	0	1
1	0	0	0	1	0	0	1	0	1
1	1	0	0	0	1	0	0	1	0
x_1	x_2	$e_{01} + e_{11}$	$e_{10} + e_{11}$	$e_{00} + 1$	$e_{01} + 1$	$e_{10} + 1$	$e_{11} + 1$	1	0
0	0	1	0	0	1	1	1	1	0
0	1	0	0	1	0	1	1	1	0
1	0	0	1	1	1	0	1	1	0
1	1	1	1	1	1	1	0	1	0

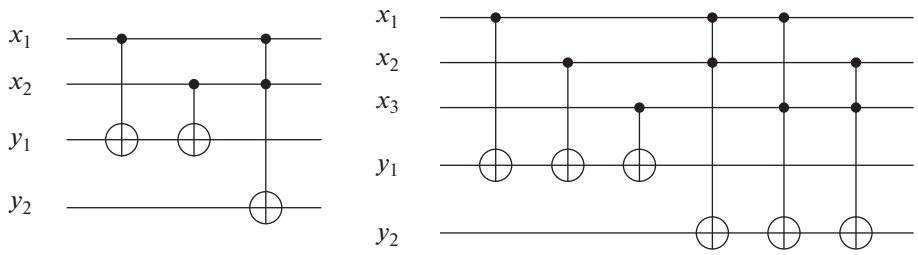


Рис. 4. Квантовые схемы полусумматора (слева) и сумматора (справа).

либо входить, либо не входить в квантовую схему, следовательно всего имеется 2^{2^n} различных булевых квантовых схем в полном соответствии с числом возможных булевых функций.

4. БУЛЕВЫ ФУНКЦИИ С МНОГОБИТОВЫМ МНОЖЕСТВОМ ЗНАЧЕНИЙ

До сих пор мы предполагали, что регистр множества значений y содержит только один кубит. Рассмотрение можно легко обобщить на произвольный случай, когда регистр множества значений y содержит произвольное число m кубитов.

В качестве примеров таких более сложных логических элементов (гейтов) рассмотрим полусумматор (half-adder) и сумматор (adder). Рассматриваемые элементы используются для реализации устройств, производящих операцию сложения. Оба гейта имеют двухкубитовый регистр множества значений ($m = 2$); при этом область определения полусумматора имеет два кубита ($n = 2$), а область определения сумматора содержит три кубита ($n = 3$).

Состояние кубитов y_1 и y_2 множества значений полусумматора в зависимости от состояния кубитов x_1 и x_2 области определения задается следующими соотношениями:

$$y_1 = x_1 + x_2, \quad y_2 = x_1x_2.$$

Для сумматора аналогичные соотношения имеют вид:

$$y_1 = x_1 + x_2 + x_3, \quad y_2 = x_1x_2 + x_1x_3 + x_2x_3.$$

На рис. 4 представлены квантовые схемы полусумматора и сумматора.

Таблица 3. Таблица истинности для полусумматора

x_1	x_2	$y_1 = x_1 + x_2$	$y_2 = x_1x_2$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Таблица 4. Таблица истинности для сумматора

x_1	x_2	x_3	$y_1 = x_1 + x_2 + x_3$	$y_2 = x_1x_2 + x_1x_3 + x_2x_3$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Утверждение 1 о блочно-диагональном характере булевых преобразований может быть обобщено на случай многобитового множества значений. Как было показано выше, в случае однобитового множества значений в качестве блочных матриц выступают следующие две матрицы размерности 2×2: $u_0 = I$, $u_1 = X$. В общем случае m-битового множества значений, в качестве блочных матриц будут выступать уже матрицы размерности $2^m \times 2^m$. Например, в случае двухбитового множества значений в качестве блочных матриц выступают следующие четыре матрицы размерности 4×4:

$$u_{00} = u_0 \otimes u_0 = I \otimes I,\ u_{01} = u_0 \otimes u_1 = I \otimes X,\ u_{10} = u_1 \otimes u_0 = X \otimes I,\ u_{11} = u_1 \otimes u_1 = X \otimes X.$$

Здесь нижние индексы матриц идентифицируют значения битов множества значений булевой функции. Сказанное делает очевидным построение блочных матриц и в более сложных случаях.

Представленные выше рассуждения совместно со знанием таблиц истинности (табл. 3, 4) позволяют легко построить унитарные матрицы преобразований для произвольных булевых функций

с n-битовой областью определения и m-битовым множеством значений.

В общем случае булевой функции с n-битовой областью определения и m-битовым множеством значений унитарная матрица преобразования U_f действует на состояния регистра из $n+m$ кубит и имеет размерность соответственно $2^{n+m} \times 2^{n+m}$.

Представленное выше Утверждение 1 можно обобщить следующим образом.

Утверждение 1А (о блочно-диагональном характере булевых преобразований с n-битовой областью определения и m-битовым множеством значений)

Унитарная матрица, отвечающая булевой функции, имеет блочно-диагональный вид, причем значениям функции $f(x) = j_1 \ldots j_m$ соответствует матрица $u_{j_1 \ldots j_m} = u_{j_1} \otimes \ldots \otimes u_{j_m}$, где $u_0 = I$, $u_1 = X$. Предполагается, как и раньше, что значения аргумента x для n-битовой области определения упорядочены в порядке возрастания от 0 до $2^n - 1$.

Заметим также, что в случае, когда регистр множества значений y содержит произвольное число m кубитов, в таблице истинности возникает m булевых столбцов значений функции. К каждому такому столбцу непосредственно применимы Утверждения 2 и 3. Это свойство уже фактически было использовано нами в изображениях квантовых схем для полусумматора и сумматора.

Для Утверждения 1А можно получить аналог формулы (3). Если булева функция имеет m-битовую область значений $(y_1, y_2, \ldots, y_m)$, то легко видеть, что итоговое квантовое преобразование U_f основано на преобразованиях, полученных из составляющих исходной функции $U_{y_1}, U_{y_2}, \ldots, U_{y_m}$. Первые элементы тензорных произведений на главной диагонали матрицы U_f представляют собой диагональ матрицы U_{y_1}, вторые элементы в тензорном произведении – диагональ матрицы U_{y_2} и т.д. Данный факт может быть описан математически следующим образом:

$$U_f = U_{y_1} * U_{y_2} * \ldots * U_{y_m}, \tag{4}$$

где $A * B = (A_{ij} \otimes B_{ij})_{ij}$ – операция умножения Хатри-Рао [17], которая по сути является поэлементным тензорным умножение для блочных матриц. То есть формула (4) является произведением (в смысле Хатри-Рао) формул (3) для каждой из функций $y_1, y_2, \ldots, y_m$. Следовательно, формула (4) может быть переписана в следующем виде:

$$U_f = \operatorname{diag}\left((y_1 \cdot X + \overline{y}_1 \cdot I) * (y_2 \cdot X + \overline{y}_2 \cdot I) * \ldots * (y_m \cdot X + \overline{y}_m \cdot I)\right).$$

Проведя несложные вычисления, получим итоговую формулу:

$$U_f = \operatorname{diag}\left(\sum_{i_1, i_2, \ldots, i_m = 0}^{1} (i_1 \cdot y_1 + \overline{i}_1 \cdot \overline{y}_1)(i_2 \cdot y_2 + \overline{i}_2 \cdot \overline{y}_2) \ldots (i_m \cdot y_m + \overline{i}_m \cdot \overline{y}_m) X^{i_1} \otimes X^{i_2} \otimes \ldots \otimes X^{i_m}\right).$$

Или в более сокращенном виде:

$$U_f = \operatorname{diag}\left(\sum_{i_1, i_2, \ldots, i_m = 0}^{1} \prod_{j=1}^{m} (i_j \cdot y_j + \overline{i}_j \cdot \overline{y}_j) \cdot \bigotimes_{j=1}^{m} X^{i_j}\right). \tag{5}$$

В случае если мы имеем дело с однобитовой функцией ($m = 1$), данная формула сводится к формуле (3).

5. ОБОБЩЕНИЕ НА СЛУЧАЙ МНОГОЗНАЧНОЙ ЛОГИКИ

Перед рассмотрением общего случая многозначной логики, подробно рассмотрим трехзначную логику. Вместо битов/кубитов используются триты/кутриты. Если мы рассматриваем функции с n-тритной областью определения, то всего можно составить 3^{3^n} различных функции.

В случае битовых функций мы имели дело с операцией инвертирования. Для функций многозначной логики вводятся операции сдвига. Для трехзначной логики – операции сдвига соответственно на 0, 1 и 2 представляются в виде матриц:

$$T_0 = I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad T_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Матрица T_1 обеспечивает сдвиг на 1

$$((|0\rangle \to |1\rangle, |1\rangle \to |2\rangle, |2\rangle \to |0\rangle).$$

В обозначениях Дирака эти переходы можно записать следующим образом:

$$T_1 = |1\rangle\langle 0| + |2\rangle\langle 1| + |0\rangle\langle 2|.$$

Аналогично, матрица T_2 обеспечивает сдвиг на 2

$$(|0\rangle \to |2\rangle, |1\rangle \to |0\rangle, |2\rangle \to |1\rangle).$$

В этом случае имеем:

$$T_2 = |2\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 2|.$$

Нетрудно проверить справедливость следующих тождеств:

$$T_1^2 = T_2, \quad T_1^3 = T_0 = I.$$

Можно заметить, что действие оператора T_1 оказывается аналогичным повороту плоскости на 120 градусов. Три таких поворота, осуществленные последовательно, приводят к тождественному преобразованию.

Оказывается, что такое наглядное качественное геометрическое представление можно строго формализовать. Введем для этого посредством матричной экспоненты следующее унитарное преобразование: $T = \exp(-iS\theta)$. Здесь θ – угол поворота, а S – эрмитов оператор, который нужно подобрать таким образом, чтобы при $\theta = \frac{2\pi}{3}$ (120 градусов) преобразование превращалось в T_1, поэтому:

$$\ln(T_1) = -i\frac{2\pi}{3}S.$$

Вычисление главного матричного логарифма от T_1 приводит к следующему результату для оператора S:

$$S = \frac{i}{\sqrt{3}}\begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}.$$

Замечательно, что полученная в результате матрица S есть эрмитов оператор, задающий проекцию спина 1 на некоторое выделенное направление. Путем явного вычисления матричной экспоненты $T = \exp(-iS\theta)$ можно показать, что для угла поворота в 120 градусов $\left(\theta = \frac{2\pi}{3}\right)$ действительно получаем оператор T_1 :

$$T_1 = \exp\left(-i\frac{2\pi}{3}S\right).$$

Аналогично, для угла поворота в 240 градусов получаем оператор T_2, а для углов в 0 и 360 градусов – тождественное преобразование.

Собственные значения оператора S есть $m = -1,0,1$. Эти числа соответствуют возможным значениям проекции спина и, таким образом, нумеруют возможные состояния, в которых может находиться частица со спином 1 (в нашем случае- это трехуровневый логический элемент). Традиционный номер логического состояния отличается от спиновой проекции на единицу: $x = m + 1 = 0,1,2$.

Заметим наконец, что представленная матричная экспонента имеет смысл для произвольного угла поворота θ. В этом общем случае, в результате преобразования, система оказывается в суперпозиции всех трех базисных состояний. Пусть, например, система первоначально находилась в состоянии $|0\rangle$. Рассмотрим преобразование, отвечающее углу $\theta = \frac{\pi}{3}$ (60 градусов). Это преобразование условно можно назвать “сдвигом на 1/2”, поскольку отвечает половине от угла, задающего сдвиг на 1. Можно показать, что в результате данного преобразования возникнет следующее состояние, которое является суперпозицией всех трех возможных состояний:

$$|\psi\rangle = \frac{2}{3}|0\rangle + \frac{2}{3}|1\rangle - \frac{1}{3}|2\rangle.$$

Полученные коэффициенты разложения задают амплитуды вероятности. Понятно, что рассматриваемый общий случай преобразования соответствует переходу от традиционной классической дискретной математики к квантовой информатике.

Зная таблицу истинности для заданной функции, можно легко построить ее унитарное представление, которое, как и в случае обычной двоичной логики, будет блочно-диагональным (только теперь элементарные блоки – это матрицы 3×3).

Утверждение 1Б (о блочно-диагональном характере булевых преобразований в приложении к троичной логике)

Унитарная матрица, отвечающая булевой функции, имеет блочно-диагональный вид, причем значениям функции $f(x) = 0$ соответствует матрица $T_0 = I$, значениям функции $f(x) = 1$ соответствует матрица T_1, а значениям функции $f(x) = 2$ соответствует матрица T_2. Предполагается, что значения аргумента x для функции от n аргументов упорядочены в порядке возрастания от 0 до $3^n - 1$.

Для данного утверждения легко построить формулу, аналогичную формуле (3) для Утверждения 1:

$$U_f = \mathrm{diag}\left(m_0(f)\cdot T_0 + m_1(f)\cdot T_1 + m_2(f)\cdot T_2\right), \tag{6}$$

где $m_x(f)$ – двоичный массив (маска) длины 3^n, где единица на i-ой позиции означает, что элемент f_i равен x, а ноль на i-ой позиции означает, что f_i не равен x.

Для формирования базисных функций следует рассмотреть степени вектора x от 0 до 2 (рассматриваем арифметические операции по модулю 3).

$$x = \begin{pmatrix}0\\1\\2\end{pmatrix},\quad x^0 = \begin{pmatrix}1\\1\\1\end{pmatrix},\quad x^1 = x = \begin{pmatrix}0\\1\\2\end{pmatrix},\quad x^2 = \begin{pmatrix}0\\1\\1\end{pmatrix}.$$

Векторы-столбцы x^0, x^1 и x^2 объединим в единую матрицу:

$$Q = \left[x^0\ \ x^1\ \ x^2\right] = \begin{pmatrix}1&0&0\\1&1&1\\1&2&1\end{pmatrix}.$$

Стандартные базисные функции можно представить в виде суперпозиции столбцов x^0, x^1 и x^2:

$$e_0 = \begin{pmatrix}1\\0\\0\end{pmatrix} = 1 + 2x^2 = 1\cdot x^0 + 0\cdot x^1 + 2x^2,\quad e_1 = \begin{pmatrix}0\\1\\0\end{pmatrix} = 2x + 2x^2 = 0\cdot x^0 + 2\cdot x^1 + 2x^2,$$

$$e_2 = \begin{pmatrix}0\\0\\1\end{pmatrix} = x + 2x^2 = 0\cdot x^0 + 1\cdot x^1 + 2x^2.$$

В полной аналогией с рассмотренной выше двузначной логикой, введем векторы-столбцы p_0, p_1 и p_2, содержащие коэффициенты полиномов Жегалкина для функций e_0, e_1 и e_2 соответственно.

$$p_0 = \begin{pmatrix}1\\0\\2\end{pmatrix},\quad p_1 = \begin{pmatrix}0\\2\\2\end{pmatrix},\quad p_2 = \begin{pmatrix}0\\1\\2\end{pmatrix}.$$

Объединим рассматриваемые столбцы в единую матрицу:

$$P = \left[p_0\ \ p_1\ \ p_2\right] = \begin{pmatrix}1&0&0\\0&2&1\\2&2&2\end{pmatrix}.$$

Рассматриваемая матрица P является обратной по отношению к матрице Q, т.е. $QP = PQ = I$ (результат матричного умножения рассматривается по модулю 3). Это условие справедливо и для двухзначной логики (в этом случае матрицы P и Q совпадают).

Теперь перейдем к общему случаю – рассмотрим k-значную логику. В этом случае, для формирования базисных функций следует рассмотреть степени вектор аx от 0 до $k-1$. Соответствующий набор будет полным в том и только том случае, когда $k = p$ – простое число [2]. В остальном, рассмотрение аналогично представленному выше случаю $k = 3$.

В k-значной логике рассматриваются функции от произвольного числа переменных (n) с количеством логических уровней k, где k – простое число. Пусть логическая функция f представляет собой столбец из k^n чисел, заданных в лексикографическом порядке. При этом каждое из k^n логических значений функции есть целое число от 0 до $k-1$.

Пусть столбец логических значений есть

$$x = \begin{pmatrix}0\\1\\\vdots\\k-1\end{pmatrix}.$$

На основе степеней x от 0 до $k-1$ строится матрица Q размерности $k\times k$: $Q = \left[x^0\ \ldots\ x^{k-1}\right]$. Для

матрицы Q строится обратная к ней матрица P. Таким образом, при вычислениях по модулю k, справедливо тождество: $QP = PQ = I$ (результат матричного умножения рассматривается по модулю k). При нахождении коэффициентов полинома Жегалкина ключевую роль играют столбцы матрицы P: $P = [p_0 \ \dots \ p_{k-1}]$. Заметим, что для того, чтобы матрица Q была неособенной и соответственно существовала обратная матрица, необходимо и достаточно, чтобы число k, определяющее размерность логики, было простым.

Утверждение 1 в общем случае (о блочно-диагональном характере булевых преобразований в приложении к k-уровневой логике)

Унитарная матрица, отвечающая булевой функции, имеет блочно-диагональный вид, причем значениям функции $f(x) = 0$ соответствует матрица $T_0 = I$, значениям функции $f(x) = 1$ соответствует матрица T_1, значениям функции $f(x) = 2$ соответствует матрица T_2 и т.д., где T_i – описанный выше оператор сдвига на i. Предполагается, что значения аргумента x для функции от n аргументов упорядочены в порядке возрастания от 0 до $k^n - 1$.

Математически данное утверждение выглядит следующим образом (по аналогии с (6)):

$$U_f = \mathrm{diag}\left(\sum_{i=0}^{k-1} m_i(f) \cdot T_i\right). \tag{7}$$

Утверждение 2 в общем случае (алгоритм построения булевой функции в виде полинома Жегалкина)

Столбец a размерности k^n, определяющий коэффициенты полинома Жегалкина, задается суммой тензорных произведений p-столбцов $p_{j_1 j_2 \dots j_n} = p_{j_1} \otimes p_{j_2} \otimes \dots \otimes p_{j_n}$ по всем строкам таблицы истинности с весами, равными значениям логической функции f в рассматриваемых строках. Логическому индексу j_m ($j_m = 0,1,..,k-1$) отвечает столбец p_{j_m}, т.е. получаем столбец p_0 при $j_m = 0$, p_1 при $j_m = 1$, ..., p_{k-1} при $j_m = k-1$.

Возникающий в результате столбец a, определяющий коэффициенты полинома Жегалкина, также оказывается представленным в лексикографическом порядке в отношении показателей степени переменных $x_1, \dots, x_n$.

Представленное Утверждение 2 задает алгоритм преобразования столбца логической функции f в столбец a коэффициентов полинома Жегалкина. При этом используются столбцы матрицы P, а в качестве весов фигурируют значения логической функции f.

Можно показать, что обратному преобразованию, которое осуществляет переход от столбца a коэффициентов полинома Жегалкина к значениям логической функции f, соответствует использование столбцов матрицы Q совместно с элементами столбца a в качестве весов. Последовательное применение рассматриваемых преобразований (прямого и обратного) приводит к тождественному преобразованию.

Таким образом, между функциями-столбцами f и a имеет место дуализм – своеобразное отношение двойственности, которое можно представить в следующем символьном виде:

$$f \underset{Q}{\overset{P}{\rightleftarrows}} a.$$

Либо:

$$a = P * f, \quad f = Q * a.$$

Будем говорить, что первое из представленных выражений задает P – преобразование, второе – Q-преобразование. P – преобразование позволяет найти столбец коэффициентов полинома Жегалкина a по известной булевой функции f. Q-преобразование, напротив, позволяет найти булеву функцию f по известному столбцу коэффициентов полинома Жегалкина a.

В случае обычной двухуровневой логики $P = Q$, поэтому

$$a = Q * f, \quad f = Q * a.$$

В этом случае в результате многократного применения Q-преобразования столбцы f и a поочередно переходят друг в друга. Таким образом, в случае двухуровневой логики столбец истинности f сам может рассматриваться как столбец коэффициентов полинома Жегалкина для функции a.

Представленные здесь методы и алгоритмы были апробированы нами для логик с размерностями, задаваемыми следующими простыми числами: $k = 2,3,5,7,11,13,17,19,23$ и 29. Соответствующие им матрицы P представлены в приложении. Программный код на языке Matlab для расчета этих матриц может быть найден на репозитории https://github.com/PQCLab/DiscreteMath.

6. ВЫВОДЫ

Представленные методы и алгоритмы наглядно демонстрируют глубокую связь между классической дискретной математикой и квантовой информатикой. Разработанные нами методы и алгоритмы позволяют рассмотреть унитарные квантовые представления для произвольных булевых функции с многобитовыми областями определения и многобитовыми множествами значений. Подробно описана связь полиномов Жегалкина и схем квантовой логики. Выполнено обобщение разработанной теории на случай многозначных (k-значных) логик, когда $k = p$-простое число

Разработанные методы и алгоритмы имеют существенное значение для перехода от классической машинной логики к квантовым компьютерам. Автоматизация построения квантовых схем является важной проблемой при реализации полноценных квантовых вычислительных устройств. Наш подход, позволяет существенно упростить эту процедуру для квантовых преобразований, основанных на использовании классических булевых функций.

СПИСОК ЛИТЕРАТУРЫ

1. *Панюкова Т.А.* Комбинаторика и теория графов. М.: Ленанд. 2014, 216 с.
2. *Яблонский С.В.* Введение в дискретную математику. М.: Высшая школа, 2003. 386 с.
3. *Зарипова Э.Р., Кокотчикова М.Г., Севастьянов Л.А.* Дискретная математика. Часть II. Математическая логика // М.: РУДН. 2013.
4. *Зуев Ю.А.* По океану дискретной математики. От перечислительной комбинаторики до современной криптографии. В 2 томах. Т. 2. Графы. Алгоритмы. Коды, блок-схемы, шифры. М.: Либроком. 2012, 370 с.
5. *Гордеев Э.Н., Леонтьев В.К., Медведев Н.В.* О свойствах булевых полиномов, актуальных для криптосистем // Вопросы кибербезопасности. 2017. № 3(21). С. 63–69.
6. *Токарева Н.Н.* Симметричная криптография. Краткий курс: учебное пособие. Новосибирск. Новосиб. гос. ун-т. 2012, 234 с.
7. Quantum Computing: Progress and Prospects. 2019 Edition. Washington DC, National Academies of Sciences, Engineering, and Medicine. The National Academies Press.
8. *Panjin Kim, Daewan Han, Kyung Chul Jeong* Time–space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2 // Quantum Information Processing. 2018. 17:339.
9. *Markus Grassl, Brandon Langenberg, Martin Roetteler, Rainer Steinwandt.* Applying Grover's Algorithm to AES: Quantum Resource Estimates // PQCrypto 2016: Post-Quantum Cryptography. 2016. P. 29–43.
10. *Денисенко Д.В., Никитенкова М.В.* Применение квантового алгоритма Гровера в задаче поиска ключа блочного шифра SDES // ЖЭТФ. 2019. Т. 155. № 1. С. 32.
11. *Денисенко Д.В., Маршалко Г.Б., Никитенкова М.В., Рудской В.И., Шишкин В.А.* Оценка сложности реализации алгоритма Гровера для перебора ключей алгоритмов блочного шифрования ГОСТ Р 34.12-2015 // ЖЭТФ. 2019. Т. 155. № 4. С. 645.
12. *Денисенко Д.В.* О реализации подстановок в виде квантовых схем без использования дополнительных кубитов // ЖЭТФ. 2019. Т. 155. № 6. С. 999.
13. *Жегалкин И.И.* О технике вычислений предложений в символической логике // Матем. сб. 1927. Т. 34. № 1. С. 9–28.
14. *Новиков Ф. А.* Дискретная математика для программистов // Издательство: Питер. 2008, 384 с.
15. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация // М.: Мир. 2006, 824 с.
16. *Валиев К. А., Кокин А.А.* Квантовые компьютеры: надежда и реальность // Ижевск: НИЦ "Регулярная и хаотическая динамика". 2001, 352 с.
17. *Liu S., Trenkler G.* Hadamard, Khatri-Rao, Kronecker and other matrix products // International Journal of Information and Systems Sciences. 2007. V. 4. № 1. P. 160–177.

ПРИЛОЖЕНИЕ

Здесь представлены матрицы P, состоящие из коэффициентов полиномов Жегалкина для различных уровней логик.

$k = 2$:

$$P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$k = 3$:

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 2 & 2 & 2 \end{pmatrix}$$

$k = 5$:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 1 & 1 & 4 \\ 0 & 4 & 3 & 2 & 1 \\ 4 & 4 & 4 & 4 & 4 \end{pmatrix}$$

$k = 7$:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 3 & 2 & 5 & 4 & 1 \\ 0 & 6 & 5 & 3 & 3 & 5 & 6 \\ 0 & 6 & 6 & 1 & 6 & 1 & 1 \\ 0 & 6 & 3 & 5 & 5 & 3 & 6 \\ 0 & 6 & 5 & 4 & 3 & 2 & 1 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 \end{pmatrix}$$

$k = 11$:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 10 & 5 & 7 & 8 & 2 & 9 & 3 & 4 & 6 & 1 \\ 0 & 10 & 8 & 6 & 2 & 7 & 7 & 2 & 6 & 8 & 10 \\ 0 & 10 & 4 & 2 & 6 & 8 & 3 & 5 & 9 & 7 & 1 \\ 0 & 10 & 2 & 8 & 7 & 6 & 6 & 7 & 8 & 2 & 10 \\ 0 & 10 & 1 & 10 & 10 & 10 & 1 & 1 & 1 & 10 & 1 \\ 0 & 10 & 6 & 7 & 8 & 2 & 2 & 8 & 7 & 6 & 10 \\ 0 & 10 & 3 & 6 & 2 & 7 & 4 & 9 & 5 & 8 & 1 \\ 0 & 10 & 7 & 2 & 6 & 8 & 8 & 6 & 2 & 7 & 10 \\ 0 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \end{pmatrix}$$

$k = 13$:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 12 & 6 & 4 & 3 & 5 & 2 & 11 & 8 & 10 & 9 & 7 & 1 \\ 0 & 12 & 3 & 10 & 4 & 1 & 9 & 9 & 1 & 4 & 10 & 3 & 12 \\ 0 & 12 & 8 & 12 & 1 & 8 & 8 & 5 & 5 & 12 & 1 & 5 & 1 \\ 0 & 12 & 4 & 4 & 10 & 12 & 10 & 10 & 12 & 10 & 4 & 4 & 12 \\ 0 & 12 & 2 & 10 & 9 & 5 & 6 & 7 & 8 & 4 & 3 & 11 & 1 \\ 0 & 12 & 1 & 12 & 12 & 1 & 1 & 1 & 1 & 12 & 12 & 1 & 12 \\ 0 & 12 & 7 & 4 & 3 & 8 & 11 & 2 & 5 & 10 & 9 & 6 & 1 \\ 0 & 12 & 10 & 10 & 4 & 12 & 4 & 4 & 12 & 4 & 10 & 10 & 12 \\ 0 & 12 & 5 & 12 & 1 & 5 & 5 & 8 & 8 & 12 & 1 & 8 & 1 \\ 0 & 12 & 9 & 4 & 10 & 1 & 3 & 3 & 1 & 10 & 4 & 9 & 12 \\ 0 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 \end{pmatrix}$$

$k = 17$:

$$P = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 16 & 8 & 11 & 4 & 10 & 14 & 12 & 2 & 15 & 5 & 3 & 7 & 13 & 6 & 9 & 1 \\
0 & 16 & 4 & 15 & 1 & 2 & 8 & 9 & 13 & 13 & 9 & 8 & 2 & 1 & 15 & 4 & 16 \\
0 & 16 & 2 & 5 & 13 & 14 & 7 & 11 & 8 & 9 & 6 & 10 & 3 & 4 & 12 & 15 & 1 \\
0 & 16 & 1 & 13 & 16 & 13 & 4 & 4 & 1 & 1 & 4 & 4 & 13 & 16 & 13 & 1 & 16 \\
0 & 16 & 9 & 10 & 4 & 6 & 12 & 3 & 15 & 2 & 14 & 5 & 11 & 13 & 7 & 8 & 1 \\
0 & 16 & 13 & 9 & 1 & 8 & 2 & 15 & 4 & 4 & 15 & 2 & 8 & 1 & 9 & 13 & 16 \\
0 & 16 & 15 & 3 & 13 & 5 & 6 & 7 & 9 & 8 & 10 & 11 & 12 & 4 & 14 & 2 & 1 \\
0 & 16 & 16 & 1 & 16 & 1 & 1 & 1 & 16 & 16 & 1 & 1 & 1 & 16 & 1 & 16 & 16 \\
0 & 16 & 8 & 6 & 4 & 7 & 3 & 5 & 2 & 15 & 12 & 14 & 10 & 13 & 11 & 9 & 1 \\
0 & 16 & 4 & 2 & 1 & 15 & 9 & 8 & 13 & 13 & 8 & 9 & 15 & 1 & 2 & 4 & 16 \\
0 & 16 & 2 & 12 & 13 & 3 & 10 & 6 & 8 & 9 & 11 & 7 & 14 & 4 & 5 & 15 & 1 \\
0 & 16 & 1 & 4 & 16 & 4 & 13 & 13 & 1 & 1 & 13 & 13 & 4 & 16 & 4 & 1 & 16 \\
0 & 16 & 9 & 7 & 4 & 11 & 5 & 14 & 15 & 2 & 3 & 12 & 6 & 13 & 10 & 8 & 1 \\
0 & 16 & 13 & 8 & 1 & 9 & 15 & 2 & 4 & 4 & 2 & 15 & 9 & 1 & 8 & 13 & 16 \\
0 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16
\end{pmatrix}$$

$k = 19$:

$$P = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 18 & 9 & 6 & 14 & 15 & 3 & 8 & 7 & 2 & 17 & 12 & 11 & 16 & 4 & 5 & 13 & 10 & 1 \\
0 & 18 & 14 & 2 & 13 & 3 & 10 & 12 & 8 & 15 & 15 & 8 & 12 & 10 & 3 & 13 & 2 & 14 & 18 \\
0 & 18 & 7 & 7 & 8 & 12 & 8 & 18 & 1 & 8 & 11 & 18 & 1 & 11 & 7 & 11 & 12 & 12 & 1 \\
0 & 18 & 13 & 15 & 2 & 10 & 14 & 8 & 12 & 3 & 3 & 12 & 8 & 14 & 10 & 2 & 15 & 13 & 18 \\
0 & 18 & 16 & 5 & 10 & 2 & 15 & 12 & 11 & 13 & 6 & 8 & 7 & 4 & 17 & 9 & 14 & 3 & 1 \\
0 & 18 & 8 & 8 & 12 & 8 & 12 & 18 & 18 & 12 & 12 & 18 & 18 & 12 & 8 & 12 & 8 & 8 & 18 \\
0 & 18 & 4 & 9 & 3 & 13 & 2 & 8 & 7 & 14 & 5 & 12 & 11 & 17 & 6 & 16 & 10 & 15 & 1 \\
0 & 18 & 2 & 3 & 15 & 14 & 13 & 12 & 8 & 10 & 10 & 8 & 12 & 13 & 14 & 15 & 3 & 2 & 18 \\
0 & 18 & 1 & 1 & 18 & 18 & 18 & 18 & 1 & 18 & 1 & 18 & 1 & 1 & 1 & 1 & 18 & 18 & 1 \\
0 & 18 & 10 & 13 & 14 & 15 & 3 & 8 & 12 & 2 & 2 & 12 & 8 & 3 & 15 & 14 & 13 & 10 & 18 \\
0 & 18 & 5 & 17 & 13 & 3 & 10 & 12 & 11 & 15 & 4 & 8 & 7 & 9 & 16 & 6 & 2 & 14 & 1 \\
0 & 18 & 12 & 12 & 8 & 12 & 8 & 18 & 18 & 8 & 8 & 18 & 18 & 8 & 12 & 8 & 12 & 12 & 18 \\
0 & 18 & 6 & 4 & 2 & 10 & 14 & 8 & 7 & 3 & 16 & 12 & 11 & 5 & 9 & 17 & 15 & 13 & 1 \\
0 & 18 & 3 & 14 & 10 & 2 & 15 & 12 & 8 & 13 & 13 & 8 & 12 & 15 & 2 & 10 & 14 & 3 & 18 \\
0 & 18 & 11 & 11 & 12 & 8 & 12 & 18 & 1 & 12 & 7 & 18 & 1 & 7 & 11 & 7 & 8 & 8 & 1 \\
0 & 18 & 15 & 10 & 3 & 13 & 2 & 8 & 12 & 14 & 14 & 12 & 8 & 2 & 13 & 3 & 10 & 15 & 18 \\
0 & 18 & 17 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18
\end{pmatrix}$$

$k = 23$:

$$P = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 22 & 11 & 15 & 17 & 9 & 19 & 13 & 20 & 5 & 16 & 2 & 21 & 7 & 18 & 3 & 10 & 4 & 14 & 6 & 8 & 12 & 1 \\
0 & 22 & 17 & 5 & 10 & 11 & 7 & 15 & 14 & 21 & 20 & 19 & 19 & 20 & 21 & 14 & 15 & 7 & 11 & 10 & 5 & 17 & 22 \\
0 & 22 & 20 & 17 & 14 & 16 & 5 & 12 & 19 & 10 & 2 & 8 & 15 & 21 & 13 & 4 & 11 & 18 & 7 & 9 & 6 & 3 & 1 \\
0 & 22 & 10 & 21 & 15 & 17 & 20 & 5 & 11 & 19 & 14 & 7 & 7 & 14 & 19 & 11 & 5 & 20 & 17 & 15 & 21 & 10 & 22 \\
0 & 22 & 5 & 7 & 21 & 8 & 11 & 4 & 10 & 20 & 6 & 9 & 14 & 17 & 3 & 13 & 19 & 12 & 15 & 2 & 16 & 18 & 1 \\
0 & 22 & 14 & 10 & 11 & 20 & 21 & 17 & 7 & 15 & 19 & 5 & 5 & 19 & 15 & 7 & 17 & 21 & 20 & 11 & 10 & 14 & 22 \\
0 & 22 & 7 & 11 & 20 & 4 & 15 & 9 & 21 & 17 & 18 & 13 & 10 & 5 & 6 & 2 & 14 & 8 & 19 & 3 & 12 & 16 & 1 \\
0 & 22 & 15 & 19 & 5 & 10 & 14 & 21 & 17 & 7 & 11 & 20 & 20 & 11 & 7 & 17 & 21 & 14 & 10 & 5 & 19 & 15 & 22 \\
0 & 22 & 19 & 14 & 7 & 2 & 10 & 3 & 5 & 11 & 8 & 6 & 17 & 15 & 12 & 18 & 20 & 13 & 21 & 16 & 9 & 4 & 1 \\
0 & 22 & 21 & 20 & 19 & 5 & 17 & 7 & 15 & 14 & 10 & 11 & 11 & 10 & 14 & 15 & 7 & 17 & 5 & 19 & 20 & 21 & 22 \\
0 & 22 & 22 & 22 & 22 & 1 & 22 & 1 & 22 & 22 & 1 & 1 & 22 & 22 & 1 & 1 & 22 & 1 & 22 & 1 & 1 & 1 & 1 \\
0 & 22 & 11 & 15 & 17 & 14 & 19 & 10 & 20 & 5 & 7 & 21 & 21 & 7 & 5 & 20 & 10 & 19 & 14 & 17 & 15 & 11 & 22 \\
0 & 22 & 17 & 5 & 10 & 12 & 7 & 8 & 14 & 21 & 3 & 4 & 19 & 20 & 2 & 9 & 15 & 16 & 11 & 13 & 18 & 6 & 1 \\
0 & 22 & 20 & 17 & 14 & 7 & 5 & 11 & 19 & 10 & 21 & 15 & 15 & 21 & 10 & 19 & 11 & 5 & 7 & 14 & 17 & 20 & 22 \\
0 & 22 & 10 & 21 & 15 & 6 & 20 & 18 & 11 & 19 & 9 & 16 & 7 & 14 & 4 & 12 & 5 & 3 & 17 & 8 & 2 & 13 & 1 \\
0 & 22 & 5 & 7 & 21 & 15 & 11 & 19 & 10 & 20 & 17 & 14 & 14 & 17 & 20 & 10 & 19 & 11 & 15 & 21 & 7 & 5 & 22 \\
0 & 22 & 14 & 10 & 11 & 3 & 21 & 6 & 7 & 15 & 4 & 18 & 5 & 19 & 8 & 16 & 17 & 2 & 20 & 12 & 13 & 9 & 1 \\
0 & 22 & 7 & 11 & 20 & 19 & 15 & 14 & 21 & 17 & 5 & 10 & 10 & 5 & 17 & 21 & 14 & 15 & 19 & 20 & 11 & 7 & 22 \\
0 & 22 & 15 & 19 & 5 & 13 & 14 & 2 & 17 & 7 & 12 & 3 & 20 & 11 & 16 & 6 & 21 & 9 & 10 & 18 & 4 & 8 & 1 \\
0 & 22 & 19 & 14 & 7 & 21 & 10 & 20 & 5 & 11 & 15 & 17 & 17 & 15 & 11 & 5 & 20 & 10 & 21 & 7 & 14 & 19 & 22 \\
0 & 22 & 21 & 20 & 19 & 18 & 17 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22
\end{pmatrix}$$

$k = 29$:

$$P = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 28 & 14 & 19 & 7 & 23 & 24 & 4 & 18 & 16 & 26 & 21 & 12 & 20 & 2 & 27 & 9 & 17 & 8 & 3 & 13 & 11 & 25 & 5 & 6 & 22 & 10 & 15 & 1 \\
0 & 28 & 7 & 16 & 9 & 22 & 4 & 13 & 24 & 5 & 20 & 23 & 1 & 6 & 25 & 25 & 6 & 1 & 23 & 20 & 5 & 24 & 13 & 4 & 22 & 9 & 16 & 7 & 28 \\
0 & 28 & 18 & 15 & 24 & 16 & 20 & 6 & 3 & 7 & 2 & 10 & 17 & 25 & 8 & 21 & 4 & 12 & 19 & 27 & 22 & 26 & 23 & 9 & 13 & 5 & 14 & 11 & 1 \\
0 & 28 & 9 & 5 & 6 & 9 & 13 & 5 & 4 & 4 & 6 & 22 & 28 & 22 & 13 & 13 & 22 & 28 & 22 & 6 & 4 & 4 & 5 & 13 & 9 & 6 & 5 & 9 & 28 \\
0 & 28 & 19 & 21 & 16 & 25 & 7 & 9 & 15 & 23 & 18 & 2 & 12 & 24 & 3 & 26 & 5 & 17 & 27 & 11 & 6 & 14 & 20 & 22 & 4 & 13 & 8 & 10 & 1 \\
0 & 28 & 24 & 7 & 4 & 5 & 6 & 22 & 20 & 9 & 25 & 16 & 1 & 13 & 23 & 23 & 13 & 1 & 16 & 25 & 9 & 20 & 22 & 6 & 5 & 4 & 7 & 24 & 28 \\
0 & 28 & 12 & 12 & 1 & 1 & 1 & 28 & 17 & 1 & 17 & 12 & 17 & 1 & 12 & 17 & 28 & 12 & 17 & 12 & 28 & 12 & 1 & 28 & 28 & 28 & 17 & 17 & 1 \\
0 & 28 & 6 & 4 & 22 & 6 & 5 & 4 & 13 & 13 & 22 & 9 & 28 & 9 & 5 & 5 & 9 & 28 & 9 & 22 & 13 & 13 & 4 & 5 & 6 & 22 & 4 & 6 & 28 \\
0 & 28 & 3 & 11 & 20 & 7 & 25 & 13 & 27 & 24 & 8 & 14 & 12 & 23 & 19 & 10 & 6 & 17 & 15 & 21 & 5 & 2 & 16 & 4 & 22 & 9 & 18 & 26 & 1 \\
0 & 28 & 16 & 23 & 5 & 13 & 9 & 6 & 7 & 22 & 21 & 25 & 1 & 4 & 20 & 20 & 4 & 1 & 25 & 24 & 22 & 7 & 6 & 9 & 13 & 5 & 23 & 16 & 28 \\
0 & 28 & 8 & 27 & 23 & 20 & 16 & 5 & 19 & 25 & 14 & 26 & 17 & 7 & 18 & 11 & 22 & 12 & 3 & 15 & 4 & 10 & 24 & 13 & 9 & 6 & 2 & 21 & 1 \\
0 & 28 & 4 & 9 & 13 & 4 & 22 & 9 & 6 & 6 & 13 & 5 & 28 & 5 & 22 & 22 & 5 & 28 & 5 & 13 & 6 & 6 & 9 & 22 & 4 & 13 & 9 & 4 & 28 \\
0 & 28 & 2 & 3 & 25 & 24 & 23 & 22 & 8 & 20 & 10 & 11 & 12 & 16 & 14 & 15 & 13 & 17 & 18 & 19 & 9 & 21 & 7 & 6 & 5 & 4 & 26 & 27 & 1 \\
0 & 28 & 1 & 1 & 28 & 28 & 28 & 28 & 1 & 28 & 1 & 1 & 1 & 28 & 1 & 1 & 28 & 1 & 1 & 1 & 28 & 1 & 28 & 28 & 28 & 28 & 1 & 1 & 28 \\
0 & 28 & 15 & 10 & 7 & 23 & 24 & 4 & 11 & 16 & 3 & 8 & 17 & 20 & 27 & 2 & 9 & 12 & 21 & 26 & 13 & 18 & 25 & 5 & 6 & 22 & 19 & 14 & 1 \\
0 & 28 & 22 & 13 & 9 & 22 & 4 & 13 & 5 & 5 & 9 & 6 & 28 & 6 & 4 & 4 & 6 & 28 & 6 & 9 & 5 & 5 & 13 & 4 & 22 & 9 & 13 & 22 & 28 \\
0 & 28 & 11 & 14 & 24 & 16 & 20 & 6 & 26 & 7 & 27 & 19 & 12 & 25 & 21 & 8 & 4 & 17 & 10 & 2 & 22 & 3 & 23 & 9 & 13 & 5 & 15 & 18 & 1 \\
0 & 28 & 20 & 24 & 6 & 9 & 13 & 5 & 25 & 4 & 23 & 7 & 1 & 22 & 16 & 16 & 22 & 1 & 7 & 23 & 4 & 25 & 5 & 13 & 9 & 6 & 24 & 20 & 28 \\
0 & 28 & 10 & 8 & 16 & 25 & 7 & 9 & 14 & 23 & 11 & 27 & 17 & 24 & 26 & 3 & 5 & 12 & 2 & 18 & 6 & 15 & 20 & 22 & 4 & 13 & 21 & 19 & 1 \\
0 & 28 & 5 & 22 & 4 & 5 & 6 & 22 & 9 & 9 & 4 & 13 & 28 & 13 & 6 & 6 & 13 & 28 & 13 & 4 & 9 & 9 & 22 & 6 & 5 & 4 & 22 & 5 & 28 \\
0 & 28 & 17 & 17 & 1 & 1 & 1 & 28 & 12 & 1 & 12 & 17 & 12 & 1 & 17 & 12 & 28 & 17 & 12 & 17 & 28 & 17 & 1 & 28 & 28 & 28 & 12 & 12 & 1 \\
0 & 28 & 23 & 25 & 22 & 6 & 5 & 4 & 16 & 13 & 7 & 20 & 1 & 9 & 24 & 24 & 9 & 1 & 20 & 7 & 13 & 16 & 4 & 5 & 6 & 22 & 25 & 23 & 28 \\
0 & 28 & 26 & 18 & 20 & 7 & 25 & 13 & 2 & 24 & 21 & 15 & 17 & 23 & 10 & 19 & 6 & 12 & 14 & 8 & 5 & 27 & 16 & 4 & 22 & 9 & 11 & 3 & 1 \\
0 & 28 & 13 & 6 & 5 & 13 & 9 & 6 & 22 & 22 & 5 & 4 & 28 & 4 & 9 & 9 & 4 & 28 & 4 & 5 & 22 & 22 & 6 & 9 & 13 & 5 & 6 & 13 & 28 \\
0 & 28 & 21 & 2 & 23 & 20 & 16 & 5 & 10 & 25 & 15 & 3 & 12 & 7 & 11 & 18 & 22 & 17 & 26 & 14 & 4 & 19 & 24 & 13 & 9 & 6 & 27 & 8 & 1 \\
0 & 28 & 25 & 20 & 13 & 4 & 22 & 9 & 23 & 6 & 16 & 24 & 1 & 5 & 7 & 7 & 5 & 1 & 24 & 16 & 6 & 23 & 9 & 22 & 4 & 13 & 20 & 25 & 28 \\
0 & 28 & 27 & 26 & 25 & 24 & 23 & 22 & 21 & 20 & 19 & 18 & 17 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28 & 28
\end{pmatrix}$$