УДК 519.7
DOI: 10.24160/1993-6982-2017-6-161-165

О связи функциональных систем полиномов и арифметических полиномов, представляющих системы булевых функций

А.И. Мамонтов

Одной из основных областей математической кибернетики является теория функциональных систем. Функциональная система представляет собой пару (P, O), в которой P — носитель системы, а O — совокупность операций, заданных на P, т. е. функциональная система — это алгебра, элементами которой являются функции, а операции в этой алгебре соответствуют правилам построения функций друг из друга.

Традиционными модельными объектами теории считаются функциональные системы с операцией суперпозиции (переименование и отождествление переменных, подстановка функций на места переменных другой функции).

Исследована функциональная система полиномов с целыми коэффициентами. Рассмотрена связь функциональной системы полиномов с целыми коэффициентами с введенными В.Д. Малюгиным для выполнения параллельных логических вычислений арифметическими полиномами.

Проанализированы линейные полиномы с целыми коэффициентами. Множество всех таких функций обозначено $L(\mathbf{Z})$ и рассмотрено как подмножество в более обширном множестве $P(\mathbf{Z})$ функций, представленных полиномами произвольной степени с целыми коэффициентами. На $L(\mathbf{Z})$ и $P(\mathbf{Z})$ заданы операции суперпозиции. Приведены арифметические полиномы, представляющие некоторые системы булевых функций.

Установлено, что множество арифметических полиномов, представляющих некоторые системы булевых функций, не совпадают с $P(\mathbf{Z})$, однако замыкание относительно операции суперпозиции множества арифметических полиномов, представляющих некоторые системы булевых функций, с $P(\mathbf{Z})$ совпадает.

Показано, что множество линейных арифметических полиномов, представляющих некоторые системы булевых функций, не совпадают с $L(\mathbf{Z})$, однако замыкание относительно операции суперпозиции множества линейных арифметических полиномов, представляющих некоторые системы булевых функций, совпадает с $L(\mathbf{Z})$.

Ключевые слова: функциональная система полиномов, арифметический полином, параллельные логические вычисления.

Для цитирования: Мамонтов А.И. О связи функциональных систем полиномов и арифметических полиномов, представляющих системы булевых функций // Вестник МЭИ. 2017. № 6. С. 161—165. DOI: 10.24160/1993-6982-2017-6-161-165.

On the Connection between the Functional Systems of Polynomials and Arithmetic Polynomials Representing Systems of Boolean Functions

A.I. Mamontov

The theory of functional systems is one of the basic fields of mathematical cybernetics. A functional system is a pair (P, O), in which P is the system carrier and O is the totality of operations specified in P. That is, a functional system is an algebra the elements of which are functions, and operations in this algebra correspond to the rules according to which the functions are constructed from each other.

Functional systems involving a superposition operation (renaming and identifying the variables, and substituting functions for the variables of another function) are considered to be the conventional model objects of the theory.

A functional system of polynomials with integer coefficients is investigated. The connection between a functional system of polynomials with integer coefficients and the arithmetic polynomials introduced by V.D. Malyugin to perform parallel logic computations is considered.

Linear polynomials with integer coefficients are analyzed. The set of all such functions is denoted as $L(\mathbf{Z})$ and is considered as a subset in the broader set $P(\mathbf{Z})$ of functions represented by arbitrary-power polynomials with integer coefficients. Superposition (composition) operations are defined in L($\mathbf{Z}$) and P($\mathbf{Z}$). Arithmetic polynomials representing some systems of Boolean functions are given.

It has been found that the set of arithmetic polynomials representing certain systems of Boolean functions do not coincide with $P(\mathbf{Z})$. However, the closure with respect to the superposition operation of the set of arithmetic polynomials representing certain systems of Boolean functions coincides with $P(\mathbf{Z})$.

It is shown that the set of linear arithmetic polynomials representing some systems of Boolean functions does not coincide with $L(\mathbf{Z})$. However, the closure with respect to the superposition operation of the set of linear arithmetic polynomials representing certain systems of Boolean functions coincides with $L(\mathbf{Z})$.

Key words: functional system of polynomials, arithmetic polynomial, parallel logic computations.

For citation: Mamontov A.I. On the Connection between the Functional Systems of Polynomials and Arithmetic Polynomials Representing Systems of Boolean Functions. MPEI Vestnik. 2017; 6:161—165. (in Russian). DOI: 10.24160/1993-6982-2017-6-161-165.

Введение

Одной из основных областей математической кибернетики является теория функциональных систем. Функциональная система представляет собой пару (P, O), в которой P — носитель системы, а O — совокупность операций, заданных на P. Таким образом, функциональная система — это алгебра, элементами которой являются функции, а операции соответствуют правилам построения функций друг из друга [1].

Традиционные модельные объекты теории — функциональные системы с операцией суперпозиции (переименованием и отождествлением переменных, подстановкой функций на места переменных другой функции). Следует отметить, что функциональные системы полиномов начал и продолжает исследовать Н.Ф. Алексиадис [2, 3].

В работе изучена функциональная система полиномов с целыми коэффициентами, проанализирована ее связь с коэффициентами, введенными В.Д. Малюгиным для выполнения параллельных логических вычислений арифметическими полиномами [4 — 6].

О функциональной системе полиномов с целыми коэффициентами

Пусть $\mathbf{Z}$ — множество всех целых чисел. Для любого $z \in \mathbf{Z}$ через $\mathbf{Z}^n$ обозначим n-ю декартову степень множества $\mathbf{Z}$, т. е. множество $\mathbf{Z} \times \ldots \times \mathbf{Z}$ (n раз). Основные объекты, представленные в работе, — это функции, отображающие $\mathbf{Z}^n$ в $\mathbf{Z}$.

Определение 1. Переменная x_i называется существенной для функции $f(x_1, \ldots, x_i, \ldots, x_n)$, если найдутся такие $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n, b, c$, что

$$f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n) = \\ = f(a_1, \ldots, a_{i-1}, c, a_{i+1}, \ldots, a_n).$$

Определение 2. Переменная, которая не является существенной для функции f, называется фиктивной переменной для f.

Замечание. Следуя сложившейся в отечественной литературе традиции, назовем функции f, g равными, $f = g$, если одна из функций f, g получается из другой путем переименования переменных, а также введения и изъятия фиктивных переменных.

Операции суперпозиции функций заключаются в перестановке, переименовании, отождествлении переменных; введении и удалении фиктивной переменной; подстановке функций на места переменных другой функции.

Определение 3. Замыканием (относительно операции суперпозиции) множества A называется множество всех суперпозиций над A. Замыкание множества A обозначают через $[A]$. Множество A считают замкнутым классом, если $A = [A]$.

Определение 4. Множество A функций называется полной системой в замкнутом классе B, если $[A] = B$.

Определение 5. Полная система называется базисом, если любая ее собственная подсистема не является полной.

Рассмотрим функции вида

$$f(x_1, x_2, \ldots, x_n) = a_0 + a_1 x_1 + a_2 x_2 + \ldots + a_n x_n, \qquad (1)$$

отображающие $\mathbf{Z}^n$ в $\mathbf{Z}$ (при этом $a_1, a_2, \ldots, a_n \in \mathbf{Z}$). Каждый такой полином полностью определяется вектором коэффициентов (a_0, a_1, …, a_n) и представляет ровно одну функцию $f: \mathbf{Z}^n \to \mathbf{Z}$. Различным векторам коэффициентов соответствуют различные функции, поэтому отождествим (1) и представленную ей функцию, чтобы избежать довольно длинного определения формулы. Множество всех таких функций обозначим $L(\mathbf{Z})$ и рассмотрим как подмножество в более обширном множестве функций, представимых полиномами

$$f(x_1, \ldots, x_n) = \sum_{j_1, \ldots j_n \geq 0} a(j_1, \ldots j_n) x_1^{j_1} \ldots x_n^{j_n}.$$

Здесь $a(j_1, \ldots, j_n) \in \mathbf{Z}$ (множество таких функций обозначим как $P(\mathbf{Z})$).

Очевидно, что системы $\{1, x–y, xy\}$, $\{1, –x, x+y, xy\}$ являются базисами в $P(\mathbf{Z})$, а $\{1, x–y\}$, $\{1, –x, x+y\}$ — в $L(\mathbf{Z})$.

Об арифметических полиномах

Одним из способов описания систем булевых функций являются арифметические полиномы [4]. Приведем необходимые определения из [4].

Рассмотрим систему булевых функций $\{y_j, j = 1, \ldots, m\}$ от аргументов $\{x_i, i = 1, \ldots, n\}$

$$y_j = f_j(x_1, \ldots, x_n), x_i, y_i \in \{0,1\}, \qquad (2)$$

отображающую $\varphi_0: \{0, 1\}^n \to \{0, 1\}^m$.

Интерпретируем значения функций как двоичные числа

$$\sum_{j=1}^{m} y_j 2^{j-1} = Y.$$

Положим, что функции системы (2) пространственно упорядочены в кортеж в соответствии с записью

$$f_m(x_1, \ldots, x_n) * f_{m-1}(x_1, \ldots, x_n) * \ldots * f_j(x_1, \ldots, x_n),$$

где * — разделительный знак.

Рассмотрим полином

$$P(x_1, \ldots, x_n) = \sum_{(i_1, i_2, \ldots, i_k) \in \{0,1\}^n} z_{i_1 i_2 \ldots i_k} x_1^{i_1} \ldots x_n^{i_n},$$

где $z_{i_1, i_2, \ldots, i_k} \in \mathbf{Z}$.

Арифметический полином $P(x_1, \ldots, x_n)$ представляет некоторую систему функций вида (2), если $P(x_1, \ldots, x_n)$: $\{0, 1\}^n \to \{0, 1, \ldots, 2^{m-1}\}$.

О связи полиномов произвольной степени

Через P', L' обозначим множества арифметических и линейных арифметических полиномов, представляющих некоторые системы булевых функций. Опишем связь $P(\mathbf{Z})$ и P'.

В работе [4] доказана следующая теорема

Теорема 1. *Произвольный кортеж булевых функций может быть представлен арифметическим полиномом и притом единственным образом.*

Замечание. Из определения P' видно, что $P' \subseteq P(\mathbf{Z})$. Поскольку функция $-x \in P(\mathbf{Z}) \setminus P'$, то имеет место неравенство $P' \neq P(\mathbf{Z})$.

Однако справедливо следующее.

Утверждение 1. Верно равенство $[P'] = P(\mathbf{Z})$.

Доказательство. Поскольку функции 1, xy, $g(x, y) = 1 + x - y$ и $h(x) = 1 + x$ представляют кортежи булевых функций 1, xy, $x\bar{y} * x \oplus y$, $x*\bar{x}$, то 1, xy, $g(x, y)$, $h(x) \in P'$. А так как $g(y, h(x)) = y - x$, то $[P']$ содержит полную в $P(\mathbf{Z})$ систему $\{1, x - y, xy\}$. Утверждение доказано.

Рассмотрим множество $OL(\mathbf{Z})$ линейных одночленов с целыми коэффициентами, т. е. функции вида Ax или A.

Вопрос о представлении компьютерного варианта коэффициентов таких многочленов можно считать решенным, поскольку целочисленный тип данных реализован во всех современных языках программирования, а для представления больших целых чисел разработаны специальные библиотеки. Поэтому при организации параллельных логических вычислений удобны представления арифметических полиномов с помощью суперпозиций над полными в $P(\mathbf{Z})$ системами, содержащими множество $OL(\mathbf{Z})$.

Пример 1. При $x, y \in \{0, 1\}$ имеет место равенство $x \vee y = x + y - xy$. Поскольку $xy \in [\{x + y - xy, -x, 0\}]$ и $x - y \in [\{x + y, -x\}]$, то замыкание системы $B = OL(\mathbf{Z}) \cup \{x + y - xy, x + y\}$ содержит полную в $P(\mathbf{Z})$ систему $\{1, x - y, xy\}$, т. е. система B полна в $P(\mathbf{Z})$. Заменив в некотором арифметическом полиноме операции умножения по правилу $xy = x + y - x \vee y$, получим так называемую вторую арифметическую форму из [7]. Эта форма более выгодна по сравнению с арифметическим полиномом для представления некоторых систем булевых функций.

Обобщим пример следующим образом.

Пример 2. Пусть $x \circ y = a + bx + by + cxy$. Рассмотрим систему $G = OL(\mathbf{Z}) \cup \{x + y, x \circ y\}$. При $|c| > 1$ или $c = 0$, функция $xy \notin G$ и эта система не является полной в $P(\mathbf{Z})$.

Пусть $|c| = 1$, тогда с помощью функции $x + y$ и одночленов $-bx$ и $-a$ образуем функции $x - a$ и $x - by$. Используя их из $x \circ y$, образуем функцию cxy. При $c = 1$ имеет место равенство $cxy = xy$, а при $c = -1$ функция xy строится из функции cxy и одночлена $-x$. Таким образом, $\{1, -x, x + y, xy\} \in [G]$, т. е. система G является полной в $P(\mathbf{Z})$.

Отметим, что операция «$\circ$» коммутативная и исследуем ее ассоциативность:

$$(x \circ y) \circ z = a + (b + ac)z + ab + bbx + bby + bcxy + bcxz + bcyz + ccxyz.$$

Таким образом, операция «$\circ$» ассоциативна тогда и только тогда, когда $b + ac = bb$, т. е. при $c = 1$ операция «$\circ$» ассоциативна тогда и только тогда, когда $a = bb - b$, а при $c = -1$, когда $a = b - bb$.

При выполнении условий полноты и ассоциативности операции «$\circ$»:

- систему G можно использовать для представления любого арифметического полинома в памяти компьютера;
- ее можно пропускать так же, как пропускают операцию умножения при привычной записи полиномов (при выводе полинома на экран).

При применении операции «$\circ$» для хранения некоторых полиномов требуется меньше памяти, чем при использовании привычного способа представления полиномов. Так, полином

$$1 + 2x_3 + 3x_2 + 4x_2x_3 + 5x_1 + 6x_1x_3 + 7x_1x_2 + 8x_1x_2x_3$$

при переходе к полной системе $OL(\mathbf{Z}) \cup \{x \circ y, x + y\}$, где $x \circ y = x + y + xy$, преобразуется к виду

$$1 - 4(x_2 \circ x_3) - 2(x_1 \circ x_3) - 1(x_1 \circ x_2) + 8(x_1 \circ x_2 \circ x_3).$$

Отметим также, что при таком способе хранения не теряются некоторые функциональные свойства полинома, которые теряются при привычном сжатии коэффициентов полинома методом Хафмана или другими похожими методами.

Перечислим варианты выбора параметров a, b, c:

$$c = -1,\ b = 1,\ x \circ y = x + y - xy;$$
$$c = 1,\ b = 1,\ x \circ y = x + y + xy;$$
$$c = 1,\ b = -1,\ x \circ y = 2 - x - y + xy;$$
$$c = -1,\ b = 2,\ x \circ y = -2 + 2x + 2y - xy.$$

Пример 3. Пусть $(a, b) = 1$, тогда линейное диофантово уравнение $ax + by = 1$ разрешимо в целых числах, следовательно, с помощью функций $x + ay$, $x + by$, $-x$ можно получить функцию $x + y$, т. е. система $OL(\mathbf{Z}) \cup \{x + ay, x + by, xy\}$ является полной в $P(\mathbf{Z})$. Данную систему можно применять при сжатии некоторых полиномов.

О связи линейных полиномов

Исследуем связь $L(\mathbf{Z})$ и L'. Отметим, что в [4] установлено следующее.

Теорема 2. *Всякий кортеж булевых функций может быть реализован композицией линейных полиномов глубины не более 3.*

В связи с этим рассмотрим связь $L(\mathbf{Z})$ и L'.

Замечание. Из определения L' видно, что $L' \subseteq L(\mathbf{Z})$. Поскольку функция $-x \in L(\mathbf{Z}) \setminus L'$, то имеет место неравенство $L' \neq L(\mathbf{Z})$.

Аналогично утверждению 1 доказывается следующее.

Утверждение 2. Верно равенство $[L'] = L(\mathbf{Z})$.

Рассмотрим множество $OL(\mathbf{Z})$ линейных одночленов с целыми коэффициентами. Понять, образует ли произвольная конечная система функций из $L(\mathbf{Z})$ вместе с множеством $OL(\mathbf{Z})$ полную в $L(\mathbf{Z})$ систему, можно с помощью алгоритма, изложенного в [8].

Приведем пример базиса в $L(\mathbf{Z})$.

Одним из препятствий практического использования арифметической логики в логическом проектировании и управлении является невозможность применения существующих методов для решения задач большой размерности, поскольку описание арифметических полиномов и манипуляция с ними требуют весовых коэффициентов астрономических величин даже для схем малой размерности [9]. Эта проблема поднимается в [10, 11].

Для представления линейных полиномов с такими коэффициентами можно взять специальные полные системы. Например, если большая часть коэффициентов линейного арифметического полинома — числа, кратные 4 (функции f_1, f_2 из системы (2) равны нулю), то выгодно применять систему $OL(\mathbf{Z})\cup\{x + y, x + 4y\}$, используя для представления коэффициентов числа a_i, b_i, такие, что коэффициент линейного полинома

$$z_i = \begin{cases} 4a_i, \text{ если } b_i = 1; \\ a_i, \text{ иначе.} \end{cases}$$

При этом для хранения каждого из коэффициентов, не кратных 4, требуется на 1 бит больше (бит для хранения $OL(\mathbf{Z})$), чем при использовании традиционной схемы, напротив, для хранения каждого из коэффициентов, кратных 4 требуется на 1 бит меньше, поэтому если N — количество коэффициентов полинома; M — количество коэффициентов полинома, не кратных 4; $M << N$, то при хранении полинома можно экономить $N - 2M$ бит.

Заключение

Показан способ использования некоторых результатов о базисах функциональных систем полиномов для улучшения моделирования логических вычислений посредством арифметических полиномов. Установлены связи между функциональными системами полиномов и арифметическими полиномами, представляющими системы булевых функций. Это может помочь в дальшем их обогащении и даст возможность использовать достижения этих разделов друг в друге.

Работа выполнена при поддержке РФФИ (проект № 17-01-00485).

Литература

1. **Кудрявцев В.Б.** Функциональные системы. М.: Изд-во МГУ, 1982.

2. **Алексиадис Н.Ф.** Функциональная система полиномов с натуральными коэффициентами // Вестник МЭИ. 2013. № 6. С. 125—140.

3. **Алексиадис Н.Ф.** Алгоритмическая неразрешимость проблемы полноты для полиномов с целыми коэффициентами // Вестник МЭИ. 2015. № 3. С. 110—117.

4. **Малюгин В.Д.** Параллельные логические вычисления посредством арифметических полиномов. М.: Физматлит, 1997.

5. **Finko O., Samoylenko D., Dichenko S., Eliseev N.** Parallel Generator of Q-valued Pseudorandom Sequences Based on Arithmetic Polynomials // Przeglad Elektrotechniczny. 2015. V. 91. No. 3. Pp. 24—27.

6. **Сизоненко А.Б.** Параллельная реализация криптографических блоков подстановок и перестановок арифметическими полиномами // Доклады Томского гос. ун-та систем управления и радиоэлектроники. 2012. № 1—2 (26). С. 140—144.

7. **Власов А.А., Мамаев Е.И.** Расширенные арифметико-логические формы для реализации булевых функций // Труды науч. конф. по итогам науч.-исслед. работ Марийского гос. техн. ун-та. Йошкар-Ола, 2000. С. 100—107.

8. **Мамонтов А.И., Мещанинов Д.Г.** Алгоритм распознавания полноты в функциональной системе $L(\mathbf{Z})$ // Дискретная математика. 2014. Т. 26. № 1. С. 85—95.

9. **Шмерко В.П.** Теоремы Малюгина: новое понимание в логическом управлении, проектировании СБИС и структурах данных для новых технологий // Автоматика и телемеханика. 2004. № 6. С. 61—83.

10. **Дзюжаньски П., Малюгин В., Шмерко В., Янушкевич С.** Линейные модели схем на многозначных элементах // Автоматика и телемеханика. 2002. № 6. С. 99—119.

11. **Финько О.А.** Реализация систем булевых функций большой размерности методами модулярной арифметики // Автоматика и телемеханика. 2004. № 6. С. 37—60.

References

1. **Kudpyavtsev V.B.** Funktsional'nye Sistemy. M.: Izd-vo MGU, 1982. (in Russian).

2. **Aleksiadis N.F.** Funktsional'naya Sistema Polinomov s Natural'nymi Koeffitsientami. Vestnik MPEI. 2013;6:125—140. (in Russian).

3. **Aleksiadis N.F.** Algoritmicheskaya Nerazreshimost' Problemy Polnoty dlya Polinomov s Tselymi Koeffitsientami. Vestnik MPEI. 2015;3:110—117. (in Russian).

4. **Malyugin V.D.** Parallel'nye Logicheskie Vychisleniya Pocredstvom Arifmeticheskih Polinomov. M.: Fizmatlit, 1997. (in Russian).

5. **Finko O., Samoylenko D., Dichenko S., Eliseev N.** Parallel Generator of Q-valued Pseudorandom

Sequences Based on Arithmetic Polynomials. Przeglad Elektrotechniczny. 2015;91;3:24—27.

6. **Sizonenko A.B.** Parallel'naya Realizatsiya Kriptograficheskih Blokov Podstanovok i Perestanovok Arifmeticheskimi Polinomami. Doklady Tomskogo Gos. Un-ya Sistem Upravleniya i Radioelektroniki. 2012;1—2 (26):140—144.(in Russian).

7. **Vlasov A.A., Mamaev E.I.** Rasshirennye Arifmetiko-Logicheskie Formy dlya Realizatsii Bulevyh Funktsiy. Trudy Nauch. Konf. po Itogam Nauch.-issled. Rabot Mariyskogo Gos. Tekhn. Un-ya, Yoshkar-Ola, 2000:100—107. (in Russian).

8. **Mamontov A.I., Meshchaninov D.G.** Algoritm Raspoznavaniya Polnoty v Funktsional'noy Sisteme *L*(**Z**). Diskretnaya Matematika. 2014;26;1:85—95. (in Russian).

9. **Shmerko V.P.** Teoremy Malyugina: Novoe Ponimanie v Logicheskom Upravlenii, Proektirovanii SBIS i Strukturah Dannyh dlya Novyh Tekhnologiy. Avtomatika i telemekhanika. 2004;6:61—83.(in Russian).

10. **Dzyuzhan'ski P., Malyugin V., Shmerko V., Yanushkevich S.** Lineynye Modeli Skhem na Mnogoznachnyh Elementah. Avtomatika i Telemekhanika. 2002;6:99—119. (in Russian).

11. **Fin'ko O.A.** Realizatsiya Sistem Bulevyh Funktsiy Bol'shoy Razmernosti Metodami Modulyarnoy Arifmetiki. Avtomatika i Telemekhanika. 2004;6:37—60. (in Russian).

Сведения об авторе

Мамонтов Андрей Игоревич — кандидат технических наук, доцент кафедры математического моделирования НИУ «МЭИ», e-mail: MamontovAI@yandex.ru

Information about author

Mamontov Andrey I. — Ph.D. (Phys.-Math.), Assistant Professor of Mathematical Modeling Dept., NRU MPEI, e-mail: MamontovAI@yandex.ru

Статья поступила в редакцию 24.04.2017