Math-Net.Ru

Общероссийский математический портал

В. В. Баяев, Усовершенствованный алгоритм поиска аннигиляторов низкой степени для многочлена Жегалкина, *Дискрет. матем.*, 2007, том 19, выпуск 4, 132–138

DOI: <https://doi.org/10.4213/dm982>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.234.156.22

26 апреля 2023 г., 15:40:00

Усовершенствованный алгоритм поиска аннигиляторов низкой степени для многочлена Жегалкина

© 2007 г. В. В. Баев

Булева функция g называется аннигилятором булевой функции f , если $fg = 0$. В некоторых задачах анализа конечных автоматов требуется найти для функции f ненулевые аннигиляторы низкой алгебраической степени.

В статье представлен алгоритм М2, вычисляющий для многочлена Жегалкина функции f базис пространства ее аннигиляторов степени, не превосходящей d . Алгоритм М2 является усовершенствованием разработанного ранее алгоритма и позволяет в ряде случаев сократить вычисления. При этом общая оценка сложности алгоритма М2 та же, что и для прежнего алгоритма.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 07-01-00154.

1. Введение

Булева функция g называется аннигилятором булевой функции f , если $fg = 0$. В [7] описан ряд базовых свойств аннигиляторов. Задачи поиска аннигиляторов низкой степени возникают при анализе фильтрующих генераторов, основанных на двоичном регистре сдвига с линейной обратной связью [1, 5].

В последнее время разработан ряд алгоритмов для различных представлений булевой функции f , исследуемой на наличие аннигиляторов. В [6] и [7] функция f задается вектором значений, в [4] функция f задается многочленом Жегалкина, в [3] — трейс-представлением, а в [2] — дизъюнктивной нормальной формой и формулой в операциях $\&$, $\vee$, $\neg$.

В данной работе описан алгоритм М2, который по многочлену Жегалкина функции f вычисляет базис пространства ее аннигиляторов степени, не превосходящей d . Алгоритм М2 является усовершенствованием алгоритма 1 из [4] на основе идей, использованных в алгоритме 2 из [6].

2. Обозначения

Пусть F_2 — поле из двух элементов, $\mathcal{F}_n$ — множество всех булевых функций $F_2^n \rightarrow F_2$, $\deg f$ — степень многочлена Жегалкина булевой функции f . Для булевой функции $f \in \mathcal{F}_n$ и числа d введем линейное пространство

$$A_d^n(f) = \{g \in \mathcal{F}_n \mid fg = 0, \deg g \leq d\}.$$

Для векторов $x = (x_1, \dots, x_n) \in F_2^n$ и $u = (u_1, \dots, u_n) \in F_2^n$ введем обозначение для монома Жегалкина

$$x^u = \prod_{i: u_i=1} x_i$$

и для покомпонентной дизъюнкции

$$x \vee u = (x_1 \vee u_1, \dots, x_n \vee u_n),$$

и пусть $\text{wt}(x)$ — вес вектора $x \in F_2^n$, то есть число единичных координат, пусть также

$$S_n^d = \sum_{k=0}^d \binom{n}{k}$$

и M_f — число мономов в многочлене Жегалкина функции f .

3. Описание алгоритма M2

В этом разделе мы опишем алгоритм M2, вычисляющий базис пространства $A_d^n(f)$. На входе алгоритма функция f задается множеством $M_f \subset F_2^n$ степеней мономов многочлена Жегалкина, а именно,

$$f(x) = \sum_{u \in M_f} x^u. \quad (1)$$

Верхняя оценка сложности алгоритма M2 есть $O(M_f(S_n^d)^3)$. Она совпадает с оценкой для алгоритма 1 из [4]. Оба эти алгоритма решают одну и ту же систему однородных линейных уравнений методом Гаусса. Новый алгоритм отличается от старого тем, что явно указывает удобный порядок уравнений и переменных, и тем, что в процессе решения отбрасывает некоторые линейно зависимые уравнения.

На векторах из F_2^n мы будем использовать стандартное отношение частичного порядка $\leq$, а также специальное отношение $\leq$ линейного порядка. Если рассматривать векторы $(x_1, \dots, x_n)$ из F_2^n как двоичные записи натуральных чисел $\sum_{i=1}^n x_i 2^{i-1}$ из отрезка $[0, 1, \dots, 2^n - 1]$, то отношение $\leq$ соответствует порядку чисел на этом отрезке:

$$(x_1, \dots, x_n) \leq (y_1, \dots, y_n) \iff \sum_{i=1}^n x_i 2^{i-1} \leq \sum_{i=1}^n y_i 2^{i-1}. \quad (2)$$

Аналогично определяется отношение $<$.

Представим $g \in A_d^n(f)$ в виде многочлена Жегалкина

$$g(x) = \sum_{v \in F_2^n: \text{wt}(v) \leq d} b_v x^v, \quad (3)$$

где $b_v \in F_2$ — неопределенные коэффициенты. Для вектора $u \in F_2^n$ и множества $\mathcal{M}_f \subset F_2^n$ положим

$$C_d(u) = \{x \in F_2^n \mid u \preceq x, \text{wt}(x \oplus u) \leq d\},$$

$$C_d(\mathcal{M}_f) = \bigcup_{u \in \mathcal{M}_f} C_d(u).$$

Запишем элементы множества $C_d(\mathcal{M}_f)$ в порядке возрастания: $C_d(\mathcal{M}_f) = \{w_1, \dots, w_N\}$, $w_t < w_{t+1}$, $t = 1, \dots, N-1$.

Составим систему уравнений относительно коэффициентов $b_v \in F_2$ многочлена (3). Эта система уже выводилась в [4], но здесь она понадобится в другом виде:

$$0 = f(x)g(x) = \sum_{u \in \mathcal{M}_f} x^u \sum_{v \in F_2^n: \text{wt}(v) \leq d} b_v x^v$$

$$= \sum_{u \in \mathcal{M}_f} \sum_{v \in F_2^n: \text{wt}(v) \leq d} b_v x^{u \vee v}.$$

Разбивая каждую сумму по v на группы по равным значениям вектора $u \vee v$, получим равенство

$$0 = \sum_{u \in \mathcal{M}_f} \sum_{w \in C_d(u)} \sum_{v \in F_2^n: \text{wt}(v) \leq d, u \vee v = w} b_v x^w.$$

Теперь, группируя все слагаемые по моному x^w , то есть меняя порядок суммирования по u и w , приходим к равенству

$$0 = \sum_{w \in C_d(\mathcal{M}_f)} \sum_{u \in \mathcal{M}_f: w \in C_d(u)} \sum_{v \in F_2^n: \text{wt}(v) \leq d, w \oplus u \preceq v \preceq w} b_v x^w. \quad (4)$$

Здесь

$$\bar{b} = (b_v \mid v \in F_2^n: \text{wt}(v) \leq d)$$

— набор неопределенных коэффициентов многочлена (3). Будем рассматривать $\bar{b}$ как вектор переменных. Равенство нулю многочлена в правой части (4) равносильно тому, что коэффициент при каждом мономе x^w равен нулю:

$$\sum_{u \in \mathcal{M}_f: u \preceq w, \text{wt}(w \oplus u) \leq d} \sum_{v \in F_2^n: \text{wt}(v) \leq d, w \oplus u \preceq v \preceq w} b_v = 0, \quad w \in C_d(\mathcal{M}_f). \quad (5)$$

Линейную комбинацию коэффициентов $\bar{b}$, стоящую в левой части w -го уравнения системы (5), мы обозначим $\Lambda_w(\bar{b})$.

Лемма 1. Если для $w \in C_d(\mathcal{M}_f)$ коэффициент при переменной b_v в линейной комбинации $\Lambda_w(\bar{b})$ равен единице, то $v \leq w$.

Доказательство. В системе (5) одно из ограничений в сумме по v как раз имеет вид $v \leq w$.

Лемма 2. Для отношений $\leq, \leq$ и векторов $v, w \in F_2^n$ выполняются следующие очевидные импликации: $v \leq w \implies v \leq w$, $v > w \implies \neg(v \leq w)$.

Следствие 1. Для каждого v , $v > w$, переменная b_v не входит в w -е уравнение системы (5).

Далее будем считать, что функция $f \in \mathcal{F}_n$ и число d фиксированы. Для каждого $w \in F_2^n$ будем рассматривать пару пространств функций из $\mathcal{F}_n$

$$\begin{aligned} A_{<w} &= \left\{ g(X) = \sum_{v \in f_2^n : \text{wt}(v) \leq d, v \leq w} b_v X^v \mid \Lambda_z(\bar{b}) = 0 \ \forall x \in C_d(\mathcal{M}_f) : z < w \right\}, \\ A_{\leq w} &= \left\{ g(X) = \sum_{v \in f_2^n : \text{wt}(v) \leq d, v \leq w} b_v X^v \mid \Lambda_z(\bar{b}) = 0 \ \forall x \in C_d(\mathcal{M}_f) : z \leq w \right\}, \end{aligned} \quad (6)$$

где запись $g(X) = \sum_v b_v X^v$ означает, что функция $g \in \mathcal{F}_n$ представима в виде линейной комбинации указанных мономов X^v с какими-то коэффициентами $b_v \in F_2$. Следствие 1 гарантирует, что в ограничениях не встретятся переменные b_v для $v > w$. Наша цель — найти пространство $A_{\leq(1, \dots, 1)} = A_d^n(f)$.

Алгоритм М2 последовательно выполняет итерации для t от 1 до $N - 1$. На каждой итерации выделим два основных шага:

- по базису пространства $A_{<w}$ вычисляем базис $A_{\leq w}$,
- по базису пространства $A_{\leq w}$ вычисляем базис пространства $A_{<w_{t+1}}$.

Каждая базисная функция представляется вектором коэффициентов $\bar{b}$. Пространство $A_{<0}$ состоит из двух функций, констант 0 и 1. Имея $A_{<0}$, можно начать итерационный процесс.

Шаг 1. При переходе $A_{<w_t} \rightarrow A_{\leq w_t}$ добавляется еще одно уравнение $\Lambda_{w_t}(\bar{b}) = 0$ на коэффициенты $\bar{b}$. Надо провести исключение базисной функции (ниже будет описана процедура этого исключения).

Шаг 2. При переходе $A_{\leq w_t} \rightarrow A_{<w_{t+1}}$ все ограничивающие уравнения те же самые, но расширяется представление функций, возникают новые мономы X^v для v таких, что $\text{wt}(v) \leq d$, $w_t < v \leq w_{t+1}$. Поскольку в определении пространств $A_{\leq w_t}$ и $A_{<w_{t+1}}$ для всех ограничивающих уравнений $\Lambda_z(\bar{b})$ выполнено неравенство $z \leq w_t$, для всех новых мономов X^v имеет место неравенство $z < v$. Тогда в силу следствия 1 в уравнения $\Lambda_z(\bar{b}) = 0$ из определения пространства $A_{<w_{t+1}}$ не входят новые коэффициенты b_v . Значит, к базису пространства $A_{\leq w_t}$ достаточно добавить новые мономы X^v , и мы получим базис пространства $A_{<w_{t+1}}$.

Описанный итерационный процесс по своей сути есть метод Гаусса, использованный для решения той же системы (5) в [4]. Далее мы опишем прием, который позволяет сократить вычисления, выбрасывая некоторые уравнения из системы (5).

Пусть на очередной итерации получено равенство $A_{\leq w_t} = 0$. Будем отождествлять F_2^n с множеством натуральных чисел от 0 до $2^n - 1$. Запишем векторы v такие, что $\text{wt}(v) \leq d$ в порядке возрастания: $v_1 < \dots < v_D$. Запишем функцию из $A_{\leq w_t}$ в виде

$$g(X) = \sum_{v \in F_2^n: \text{wt}(v) \leq d, v \leq w_t} b_v X^v = \sum_{k=1}^{j-1} b_{v_k} X^{v_k},$$

то есть v_j — наименьшее число веса, не превосходящего d , большее w_t . Выпишем определения пространств $A_{\leq w_t}$ и $A_{\leq v_j-1}$:

$$A_{\leq w_t} = \left\{ g(X) = \sum_{k=1}^{j-1} b_{v_k} X^{v_k} \mid \Lambda_z(\bar{b}) = 0 \ \forall z \in C_d(\mathcal{M}_f): z \leq w_t \right\},$$

$$A_{\leq v_j-1} = \left\{ g(X) = \sum_{k=1}^{j-1} b_{v_k} X^{v_k} \mid \Lambda_z(\bar{b}) = 0 \ \forall z \in C_d(\mathcal{M}_f): z \leq v_j - 1 \right\}.$$

Поскольку $w_t \leq v_j - 1$, множество ограничивающих уравнений для $A_{\leq v_j-1}$ содержит все уравнения для $A_{\leq w_t}$. Значит, $A_{\leq v_j-1} \subset A_{\leq w_t} = 0$. Теперь рассмотрим

$$A_{< v_j} = \left\{ g(X) = \sum_{k=1}^j b_{v_k} X^{v_k} \mid \Lambda_z(\bar{b}) = 0 \ \forall z \in C_d(\mathcal{M}_f): z < v_j \right\}.$$

По сравнению с $A_{\leq v_j-1}$ появляется новый моном X^{v_j} , а ограничивающие уравнения те же, и в них не входит b_{v_j} . Значит,

$$A_{< v_j} = \{g(X) = b_{v_j} X^{v_j}\} = \langle X^{v_j} \rangle.$$

Тогда

$$A_{\leq v_j} = \{g(X) = b_{v_j} \mid \Lambda_{v_j}(\bar{b}) = 0\}. \quad (7)$$

Возможны два случая.

В первом случае переменная b_{v_j} не входит в линейную комбинацию $\Lambda_{v_j}(\bar{b})$ (в частности, если $v_j \notin C_d(\mathcal{M}_f)$). Тогда ограничивающее уравнение имеет вид $0 = 0$, а значит $A_{\leq v_j} = \langle X^{v_j} \rangle$. Теперь можно перейти к шагу 2 итерационного процесса с текущим вектором v_j вместо w_t . Таким образом, пропустив все элементы $w \in C_d(\mathcal{M}_f)$ такие, что $w_t < w < v_j$, мы игнорируем соответствующие им уравнения системы (5).

Во втором случае переменная b_{v_j} входит в линейную комбинацию $\Lambda_{v_j}(\bar{b})$. Тогда ограничивающее уравнение имеет вид $b_{v_j} = 0$, и мы попадаем в начальную ситуацию $A_{\leq v_j} = \langle X \rangle$. Опять нужно будет рассмотреть представление (7) и выяснить, какой из двух случаев имеет место, то есть нужно увеличивать j на единицу, пока переменная b_{v_j} входит в линейную комбинацию $\Lambda_{v_j}(\bar{b})$. Если при этом j дошло до $D + 1$, то это означает, что $A_d^n(f) = A_{\leq (1, \dots, 1)} = 0$.

Распишем полученный алгоритм по шагам. В конце некоторых шагов в скобках указываются значения переменных. Дополним цепочку векторов $w_1 < \dots < w_N$ последним элементом $w_{N+1} = 2^n$.

Алгоритм М2. На входе числа n, d и список элементов множества $\mathcal{M}_f$. На выходе базис пространства $A_d^n(f)$.

1. Для функции (1) составляем систему (5) линейных уравнений относительно неизвестных коэффициентов функции (3) (подробно этот шаг описан в [4]).
2. Инициализируем текущий список базисных функций константной функцией 1, при этом $B = \{X^0\}$. Каждый элемент списка B представляется вектором коэффициентов $\bar{b}$. Обнуляем переменный вектор $W = 0$, инициализируем целочисленные переменные $j = 1, t = 1$.

$$((B) = A_{<w}, \quad j = \arg \max_{i: v_i \leq w} v_i, \quad t = \arg \min_{r: w \leq w_r} w_r)$$

3. Переход $A_{<w} \rightarrow A_{\leq w}$. Если $w \neq w_t$ (в системе (5) нет уравнения для w), то переходим к следующему знаку. Находим ближайший к концу элемент $\bar{b}$ списка B , для которого $\Lambda_{w_t}(\bar{b}) = 1$. Прибавляем вектор $\bar{b}_t$ к остальным векторам $\bar{b}$ списка B , для которых $\Lambda_{w_t}(\bar{b}) = 1$, а затем исключаем $\bar{b}_t$ из списка B и полагаем $t := t + 1$. Если $t = N + 1$, то выдаем на выход алгоритма список B .

$$((B) = A_{<w}, \quad j = \arg \max_{i: v_i \leq w} v_i, \quad t = \arg \min_{r: w \leq w_r} w_r)$$

4. Проверка равенства $A_{\leq w} = 0$. Если список B не пуст ($A_{\leq w} \neq 0$), то переходим к следующему шагу. Увеличиваем j на единицу, пока

$$(j \leq D) \ \& \ (v_j \in C_d(\mathcal{M}_f) \ \& \ (\text{переменная } b_{v_j} \text{ входит в линейную комбинацию } \Lambda_{v_j}(\bar{b}))).$$

По завершении цикла, в случае, если $j = D + 1$, выдаем на выход алгоритма пустой список B , в противном случае полагаем $B = \{X^{v_j}\}$ и $w = v_j$. Пока $(t \leq N) \ \& \ (w_t \leq w)$, увеличиваем t на 1.

$$((B) = A_{\leq w}, \quad j = \arg \max_{i: v_i \leq w} v_i, \quad t = \arg \min_{r: w < w_r} w_r)$$

5. Переход $A_{\leq w} \rightarrow A_{<w_t}$. Пока $(j < D) \ \& \ (v_{j+1} \leq w_t)$, увеличиваем j на единицу и добавляем функцию X^{v_j} в список B . По завершении цикла полагаем $w = w_t$. Если $t \leq N$, то переходим к шагу 3, в противном случае выдаем на выход алгоритма список B .

$$((B) = A_{<w}, \quad j = \arg \max_{i: v_i \leq w} v_i, \quad t = \arg \min_{r: w \leq w_r} w_r)$$

4. Заключение

В статье предложен алгоритм М2, вычисляющий базис пространства $A_d^n(f)$ аннигиляторов низкой степени для булевой функции f , заданной в виде многочлена Жегалкина. Этот алгоритм является модификацией алгоритма 1 из [4]. Оба эти алгоритма решают одну и ту же систему линейных однородных уравнений методом Гаусса. Алгоритм М2 отличается от исходного тем, что указывает удобный порядок уравнений и переменных, что позволяет в процессе решения отбрасывать некоторые линейно зависимые уравнения. Для алгоритма М2, как и для его предшественника, справедлива верхняя оценка сложности $O(M_f(S_n^d)^3)$.

Список литературы

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В., *Основы криптографии*. Гелиос, Москва, 2001.
2. Баев В. В., О сложности поиска аннигиляторов низкой степени для булевых функций. В сб.: *Материалы Международной научной конференции по проблемам безопасности и противодействию терроризму*. МЦНМО, Москва, 2006, с. 198–204.
3. Баев В. В., Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими трейс-формами. В сб.: *Труды VII Международной конференции «Дискретные модели в теории управляющих систем»*. МАКС, Москва, 2006, с. 25–29.
4. Баев В. В., О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций. *Дискретная математика* (2006) **18**, №3, 138–151.
5. Courtois N., Meier W., Algebraic attacks on stream ciphers with linear feedback. *Lecture Notes Computer Sci.* (2003) **2656**, 345–359.
6. Didier F., Tillich J. P., Computing the algebraic immunity efficiently. *Lecture Notes Computer Sci.* (2006) **4047**, 359–374.
7. Meier W., Pasalic E., Carlet C., Algebraic attacks and decomposition of Boolean functions. *Lecture Notes Computer Sci.* (2004) **3027**, 474–491.

Статья поступила 18.05.2007.