

УДК 519.716

МОНОТОННЫЕ БУЛЕВЫ ПОЛИНОМЫ^{*)}

М. Н. Вялый, В. К. Леонтьев, М. В. Осетров

Булевы функции являются полиномами над полем из двух элементов (полиномы Жегалкина). Рассматриваются монотонные полиномы, соответствующие монотонным булевым функциям. Найдены все монотонные полиномы степеней 1, 2, 3. Доказано, что при фиксированной степени d число существенных переменных в монотонном полиноме степени d ограничено.

Постановка задачи и предварительные утверждения

Любая булева функция $f: \{0, 1\}^n \rightarrow \{0, 1\}$ является полиномом над полем из двух элементов и поэтому имеет однозначно определённое каноническое представление

$$f(\mathbf{x}) = \sum_{\mathbf{w} \in \{0, 1\}^n} c_{\mathbf{w}} \mathbf{x}^{\mathbf{w}}, \quad (1)$$

где $\mathbf{w} = (\alpha_1, \dots, \alpha_n)$, $\alpha_i \in \{0, 1\}$, $\mathbf{x}^{\mathbf{w}} = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, $x_i^{\alpha_i} = 1$ при $\alpha_i = 0$ и $x_i^{\alpha_i} = x_i$ при $\alpha_i = 1$, $c_{\mathbf{w}} \in \{0, 1\}$, а суммирование производится по модулю 2. Такое представление функции $f(\mathbf{x})$ называется полиномом Жегалкина.

Монотонным полиномом будем называть полином, задающий монотонную функцию. Ограничение монотонного полинома на подкуб также является монотонным полиномом. Кроме того, множество монотонных полиномов замкнуто относительно композиции. В [2] построен алгоритм распознавания монотонности полинома, полиномиальный по длине записи полинома в каноническом представлении.

В настоящей статье рассматриваются свойства монотонных полиномов. Если ограничиться функциями, в которых все переменные

^{*)} Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 02-01-00547, 02-01-00716, 00-15-96064).

существенны, то при каждом d существует лишь конечное число монотонных полиномов степени d (см. теорему ниже). Это позволяет перечислять монотонные функции не только по числу переменных, но и по степени представляющих полиномов. В дальнейшем при перечислении монотонных полиномов всегда будем опускать несущественные переменные и приводить ответы с точностью до перестановки переменных.

Выражение «полином f » всюду означает «полином, задающий функцию f ».

Очевидно, что константы 0 и 1 являются монотонными полиномами степени 0, а единственный монотонный полином степени 1 имеет вид x_1 . Ниже найдены все монотонные полиномы степеней 2 и 3.

В случае поля из двух элементов выражение коэффициентов полинома через его значения имеет простой вид.

Лемма 1. Для коэффициентов полинома f выполняются соотношения

$$c_w = \sum_{a \leq w} f(a),$$

где \leq — обычный порядок на булевом кубе (покомпонентное сравнение).

Доказательство. Учитывая однозначность канонического представления булевой функции в виде полинома Жегалкина, достаточно проверить, что

$$f(x) = \sum_{w \in \{0,1\}^n} \sum_{a \leq w} f(a) x^w.$$

При фиксированном x имеем

$$\begin{aligned} \sum_{w \in \{0,1\}^n} \sum_{a \leq w} f(a) x^w &= \sum_{w \leq x} \sum_{a \leq w} f(a) \\ &= \sum_a f(a) \sum_{a \leq w \leq x} 1 = \sum_{a \leq x} f(a) 2^{|x|-|a|} = f(x). \end{aligned}$$

Из леммы 1 вытекают такие следствия для монотонных полиномов.

Следствие 1. Монотонный полином, отличный от единицы, имеет свободный член 0.

Моном x^w назовем *минимальным мономом* полинома $f = \sum_v c_v x^v$, если $c_w = 1$ и $c_u = 0$ для всех $u < w$.

Следствие 2 ([2]). Пусть f — монотонный полином, $\sum_v c_v x^v$ — его каноническое представление. Если $f(w) = 0$, то $c_w = 0$. Если x^w — минимальный моном полинома f , то w — нижняя единица функции f . И наоборот, если w — нижняя единица функции f , то x^w — минимальный моном.

Следствие 3. Монотонный полином степени не более k содержит не более k линейных слагаемых.

Доказательство. Тожественно равный единице полином содержит 0 линейных слагаемых. Пусть полином f , не равный тождественно единице, имеет линейные слагаемые x_1, \dots, x_k . Обозначим через $\mathbf{e}_i = (0, 0, \dots, 0, 1, 0, \dots, 0)$, $1 \leq i \leq k$, такой набор, в котором единица находится в i -й позиции. По следствию 2 наборы $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_k$ — нижние единицы функции f . Поэтому

$$c_{\mathbf{s}_k} = \sum_{\mathbf{a} \leq \mathbf{s}_k} f(\mathbf{a}) = 2^k - 1 \equiv 1 \pmod{2}, \text{ где } \mathbf{s}_k = \sum_{j=1}^k \mathbf{e}_j.$$

Таким образом, $\deg f \geq k$.

Лемма 1 и следствие 2 показывают, что по нижним единицам функции f (минимальным мономам полинома f) остальные коэффициенты полинома восстанавливаются однозначно. Коэффициенты монотонных полиномов удовлетворяют также системе уравнений, получающейся применением следующей леммы.

Лемма 2. Полином $f(x_1, \dots, x_n)$ является монотонным тогда и только тогда, когда для любого k , $1 \leq k \leq n$, выполняется тождество

$$(1 + x_k)f(x_1, \dots, x_n) \frac{\partial f}{\partial x_k}(x_1, \dots, x_n) = 0. \quad (2)$$

Производная определяется естественным образом: для любого \mathbf{x}

$$f(\mathbf{x} + \mathbf{e}_k) = f(\mathbf{x}) + \frac{\partial f}{\partial x_k}(\mathbf{x}).$$

Доказательство. Функция монотонна тогда и только тогда, когда для любых наборов \mathbf{x}, \mathbf{y} таких, что \mathbf{y} покрывает \mathbf{x} , из $f(\mathbf{x}) = 1$ следует $f(\mathbf{y}) = 1$. Если \mathbf{y} покрывает \mathbf{x} , то при некотором k , $1 \leq k \leq n$, имеем $\mathbf{y} = \mathbf{x} + \mathbf{e}_k$, $x_k = 0$. Таким образом, уравнения (2) задают приведенное выше условие в виде полиномиального тождества.

Замечание. Если полином функции f задан каноническим представлением (списком мономов), то условия (2) проверяются за полиномиальное время. Следовательно, имеется полиномиальный алгоритм проверки монотонности полинома, отличающийся от приведенного в [2].

Разложения по минимальным мономам

Лемма 3. Пусть f — монотонный полином ненулевой степени и x_1 — линейное слагаемое функции f . Тогда

$$f(x_1, x_2, \dots, x_n) = x_1 + (1 + x_1)g(x_2, \dots, x_n), \quad \deg g = \deg f - 1.$$

ДОКАЗАТЕЛЬСТВО. Заметим, что \mathbf{e}_1 — нижняя единица функции f (следствие 2). Поэтому ограничение на подкуб $\{x \mid x_1 = 1\}$ функции f тождественно равно единице. Это означает, что для любого $\mathbf{w} = (0, \mathbf{w}')$, $\mathbf{w}' \neq \mathbf{0}$, выполнено равенство $c_{\mathbf{w}} + c_{\mathbf{w}+\mathbf{e}_1} = 0$, т. е. $c_{\mathbf{w}} = c_{\mathbf{w}+\mathbf{e}_1}$. Группируя слагаемые с учётом этого соотношения, получаем представление $f(x_1, x_2, \dots, x_n) = x_1 + (1 + x_1)g(x_2, \dots, x_n)$.

Лемма 3 допускает следующее обобщение. Пусть $x_1 x_2 \dots x_r$ — минимальный моном полинома f . Запишем разложение функции f по переменным x_1, \dots, x_r . Для наглядности обозначим остальные переменные через u_1, \dots, u_{n-r} . Получаем

$$f(\mathbf{x}, \mathbf{u}) = \sum_{\mathbf{w} \in \{0,1\}^r} C_{\mathbf{w}}(\mathbf{u}) \mathbf{x}^{\mathbf{w}}. \quad (3)$$

Здесь $C_{\mathbf{w}}(\mathbf{u})$ — полином от \mathbf{u} степени не выше $\deg f - |\mathbf{w}|$. Этот полином будем называть \mathbf{w} -м коэффициентом разложения по минимальному моному $x_1 x_2 \dots x_r$.

Лемма 4. В обозначениях, введенных выше, $\deg C_0(\mathbf{u}) < \deg f$.

ДОКАЗАТЕЛЬСТВО. Поскольку \mathbf{s}_r — нижняя единица функции f , ограничение на подкуб $\{x \mid x_1 = x_2 = \dots = x_r = 1\}$ полинома f тождественно равно единице. Степени полиномов $C_{\mathbf{w}}(\mathbf{u})$ при $\mathbf{w} \neq \mathbf{0}$ меньше $\deg f$. Поэтому и степень $C_0(\mathbf{u})$ должна быть меньше $\deg f$, так как $\sum_{\mathbf{w}} C_{\mathbf{w}}(\mathbf{u})$ тождественно равен единице.

Для каждого набора $\mathbf{v} \in \{0,1\}^r$ ограничения f на подкубы $\{x \mid x_i = v_i, 1 \leq i \leq r\}$

$$S_{\mathbf{v}}(\mathbf{u}) = \sum_{\mathbf{w} \leq \mathbf{v}} C_{\mathbf{w}}(\mathbf{u}) \quad (4)$$

являются монотонными полиномами, степень которых меньше степени f .

Отметим также, что $S_{\mathbf{s}_r}(\mathbf{u})$ тождественно равен единице, а если $\mathbf{w} \neq \mathbf{s}_r$, то $S_{\mathbf{w}}(\mathbf{u})$ не равен тождественно единице (поскольку $x_1 x_2 \dots x_r$ — минимальный моном). Поэтому, в частности, свободный член равен единице только для коэффициента разложения $C_{\mathbf{s}_r}$.

Разложение по минимальному моному позволяет оценить число существенных переменных в монотонном полиноме.

Теорема. Для каждого $d \geq 0$ существует такое число N_d , что число существенных переменных в любом монотонном полиноме степени d не превосходит N_d .

ДОКАЗАТЕЛЬСТВО. Прежде всего заметим (аналогично лемме 1), что формулы (4) допускают обращение

$$C_{\mathbf{w}}(\mathbf{u}) = \sum_{\mathbf{v} \leq \mathbf{w}} S_{\mathbf{v}}(\mathbf{u}). \quad (5)$$

Действительно,

$$\sum_{\mathbf{v} \leq \mathbf{w}} S_{\mathbf{v}}(\mathbf{u}) = \sum_{\mathbf{v} \leq \mathbf{w}} \sum_{\mathbf{t} \leq \mathbf{v}} C_{\mathbf{t}}(\mathbf{u}) = \sum_{\mathbf{t} \leq \mathbf{w}} 2^{|\mathbf{w}| - |\mathbf{t}|} C_{\mathbf{t}}(\mathbf{u}) = C_{\mathbf{w}}(\mathbf{u}).$$

Дальнейшее доказательство проведем по индукции. При $d = 1$ утверждение очевидно. Пусть утверждение теоремы справедливо для всех $d' < d$.

Пусть монотонный полином f степени d существенно зависит от n переменных. Рассмотрим его минимальный моном минимальной степени, скажем, $x_1 x_2 \dots x_r$ и разложение (3) для этого монома. По предположению индукции каждое ограничение $S_{\mathbf{v}}(\mathbf{u})$ существенно зависит не более чем от N_{d-1} переменных, а во все ограничения входит не более $2^r N_{d-1}$ существенных переменных. В силу (5) каждый коэффициент разложения $C_{\mathbf{v}}$ зависит от тех же самых переменных. Поэтому f зависит не более чем от $r + 2^r N_{d-1}$ переменных. Таким образом, $N_d \leq d + 2^d N_{d-1}$.

ЗАМЕЧАНИЕ. Из доказательства теоремы следует, что $N_d \leq d! 2^{d(d+1)/2}$. Эта оценка очень грубая. Определение порядка роста N_d представляется интересной задачей. Здесь мы ограничимся лишь простым примером, дающим гораздо более слабую нижнюю оценку. Рассмотрим следующую последовательность функций:

$$\begin{aligned} f_1(x_1, x_2, x_3) &= \text{MAJ}(x_1, x_2, x_3) = x_1 x_2 + x_2 x_3 + x_3 x_1, \\ f_{k+1}(x_{11}, \dots, x_{1N}, x_{21}, \dots, x_{2N}, \dots, x_{N1}, \dots, x_{NN}) \\ &= f_k(f_k(x_{11}, \dots, x_{1N}), f_k(x_{21}, \dots, x_{2N}), \dots, f_k(x_{N1}, \dots, x_{NN})). \end{aligned}$$

Монотонный полином функции f_k зависит от 3^{2^k} переменных и имеет степень 2^{2^k} . Это показывает, что на бесконечной подпоследовательности значений d рост N_d сверхлинейный: $N_d \geq d^{\log_2 3}$.

Помимо монотонности сумм $S_{\mathbf{v}}(\mathbf{u})$ (см. (4)) монотонность полинома функции f влечет импликацию

$$S_{\mathbf{v}}(\mathbf{u}) \rightarrow S_{\mathbf{w}}(\mathbf{u}) \text{ при } \mathbf{v} \leq \mathbf{w}. \quad (6)$$

Легко видеть, что этих импликаций и монотонности сумм $S_{\mathbf{v}}(\mathbf{u})$ достаточно для монотонности функции f .

Сумма из левой части (6) повторяется в правой, а условие $A \rightarrow A+B$ равносильно тождеству

$$A(1 + A + B) = AB = 0. \quad (7)$$

Тождество (7), разумеется, выполнено при $B = 0$.

Пару полиномов (f, g) назовём *монотонной* парой, если f, g — монотонные и $f \rightarrow g$, что равносильно $f(1 + g) = f(f + g) = 0$.

Монотонные полиномы степени 2

Минимальная степень минимального монома 1. По лемме 3 полином имеет вид $x_1 + (1 + x_1)g(x_2, \dots)$, $\deg g = 1$. Монотонный полином g степени 1 единственный. Соответствующий полином второй степени — дизъюнкция двух переменных:

$$x_1 + (1 + x_1)x_2 = x_1 + x_2 + x_1x_2 = x_1 \vee x_2. \quad (8^1)$$

Минимальная степень минимального монома 2. Пусть f — искомый полином. Если x_1x_2, x_1x_3 — его мономы, то x_2x_3 — также его моном. Действительно, ограничение f на подкуб $\{x \mid x_4 = \dots = x_n = 0\}$ — монотонный полином степени 2, не содержащий линейных слагаемых и содержащий мономы x_1x_2 и x_1x_3 . Поскольку полином $x_1x_2 + x_1x_3$ — не монотонный, ограничение имеет вид $x_1x_2 + x_1x_3 + x_2x_3$.

Отсюда получаем, что f — симметрический полином степени 2. Легко проверить, что если он зависит от двух или трех переменных, то он монотонный (конъюнкция двух переменных или функция голосования от трех переменных). Уже при четырех переменных полином $x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$ не является монотонным.

Таким образом, получаем ещё два решения:

$$x_1x_2, \quad (8^2)$$

$$\text{MAJ}(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3. \quad (8^3)$$

Монотонные полиномы степени 3

При поиске монотонных полиномов третьей степени нам потребуется таблица монотонных пар полиномов степени не выше 2. Построим такую таблицу прямым перебором.

Очевидно, что пары вида $(0, f), (f, 1), (f, f)$ будут монотонными. Если $(1, f)$ — монотонная пара, то $f = 1$. Аналогично, если $(f, 0)$ — монотонная пара, то $f = 0$.

Рассмотрим монотонную пару (x_1, f) , $f \neq 1$ и $f \neq x_1$. Очевидно, что $f \neq 0$, f зависит от x_1 и содержит моном x_1 . Поэтому $f = x_1 \vee x_2$.

Рассмотрим монотонную пару (f, x_1) , $f \neq 0$ и $f \neq x_1$. Очевидно, что $f \neq 1$ и f зависит от x_1 . Пусть $f = f_1x_1 + f_0$, где f_0 от x_1 не зависит. Тогда

$$f(1 + x_1) = (f_1x_1 + f_0)(1 + x_1) = f_0(1 + x_1) = 0$$

и $f_0 = 0$, а $f = x_1x_2$.

Осталось разобрать случаи полиномов степени 2. Перебирая все возможные варианты, получим ещё четыре монотонные пары. В результате получаем таблицу монотонных пар степени не выше 2:

$$\begin{array}{ll} (0, X) & X \text{ любой,} \\ (X, 1) & X \text{ любой,} \\ (X, X) & X \text{ любой,} \\ (x_1, x_1 \vee x_2), & \\ (x_1x_2, x_1), & (9) \\ (x_1x_2, x_1 \vee x_2), & \\ (x_1x_2, x_1 \vee x_3), & \\ (x_1x_2, \text{MAJ}(x_1, x_2, x_3)), & \\ (\text{MAJ}(x_1, x_2, x_3), x_1 \vee x_2), & \end{array}$$

Минимальная степень минимального монома 1. По лемме 3 полином имеет вид $x_1 + (1 + x_1)g(x_2, \dots)$, $\deg g = 2$. Полином g задается одной из формул (8^1-8^3). Получаем три решения:

$$x_1 + (1 + x_1)(x_2 + x_3 + x_2x_3) = x_1 \vee x_2 \vee x_3, \quad (10^1)$$

$$x_1 + (1 + x_1)x_2x_3 = x_1 \vee x_2x_3, \quad (10^2)$$

$$x_1 + (1 + x_1)(x_2x_3 + x_2x_4 + x_3x_4) = x_1 \vee \text{MAJ}(x_2, x_3, x_4). \quad (10^3)$$

Минимальная степень минимального монома 2. Пусть f — искомый полином и x_1x_2 — его минимальный моном. Рассмотрим разложение (3) по этому моному:

$$f = x_1x_2(1 + A(\mathbf{u})) + x_1B(\mathbf{u}) + x_2C(\mathbf{u}) + D(\mathbf{u}).$$

По лемме 4 имеем $\deg D(\mathbf{u}) \leq 2$. При $x_1 = x_2 = 1$ полином f тождественно равен единице, при других значениях x_1 и x_2 ограничения являются монотонными полиномами. Таким образом, $A + B + C + D = 0$, а $D, B + D$ и $C + D$ — монотонные полиномы. Более того, из условия монотонности функции f следует, что $(D, B + D)$ и $(D, C + D)$ — монотонные пары.

Рассмотрим возможные случаи.

Пусть $D = 0$. Тогда квадратичные части монотонных полиномов B, C совпадают: $B = C + A$, а полином A может зависеть не более чем от двух переменных ($\deg A \leq 1$).

При $A = 0$ имеем $B = C$, что даёт три решения:

$$x_1x_2 + (x_1 + x_2)u_1u_2, \quad (10^4)$$

$$x_1x_2 + (x_1 + x_2)(u_1u_2 + u_1 + u_2), \quad (10^5)$$

$$x_1x_2 + (x_1 + x_2)(u_1u_2 + u_1u_3 + u_2u_3). \quad (10^6)$$

При $A = u_1$ имеем $C = 0$ и ещё одно решение:

$$x_1x_2(1 + u_1) + x_1u_1 = x_1(x_2 \vee u_1). \quad (10^7)$$

При $A = u_1 + u_2$, учитывая монотонность B и C , получаем $C = u_1u_2$ или $C = u_2$. Таким образом,

$$f = x_1x_2(1 + u_1 + u_2) + x_1(u_1u_2 + u_1 + u_2) + x_2u_1u_2, \quad (10^8)$$

$$f = x_1x_2(1 + u_1 + u_2) + x_1u_1 + x_2u_2. \quad (10^9)$$

Все 6 найденных решений различны, что можно проверить, сравнивая количество мономов в этих решениях:

Решение	Мономы степени 2	Мономы степени 3
(10^4)	1	2
(10^5)	5	2
(10^6)	1	6
(10^7)	2	1
(10^8)	3	4
(10^9)	3	2

Убедимся, что других решений с минимальными мономами степени 2 нет.

Пусть $D = u_1$ или $D = u_1 \vee u_2$. Тогда есть минимальный моном степени 1.

Пусть $D = u_1u_2$. Если $A \neq 0$, то этот случай сводится к случаю $A = 0$ переходом к разложению по минимальному моному u_1u_2 . Пусть $A = 0$. Из таблицы монотонных пар (9) видно, что $\deg B \leq 1$ и $\deg C \leq 1$ при условии, что $B + C + u_1u_2 = 0$. Но тогда $\deg f \leq 2$.

$D = \text{MAJ}(u_1, u_2, u_3)$. Таблица монотонных пар (9) показывает, что невозможно добиться выполнения условия $A + B + C + D = 0$, так как $\deg A \leq 1$.

Минимальная степень минимального монома 3. Пусть f — искомый полином и $x_1x_2x_3$ — его минимальный моном. Рассмотрим разложение (3) по этому моному:

$$f = x_1x_2x_3 + x_1x_2A(\mathbf{u}) + x_2x_3B(\mathbf{u}) + x_3x_1C(\mathbf{u}) \\ + x_1D(\mathbf{u}) + x_2E(\mathbf{u}) + x_3F(\mathbf{u}) + G(\mathbf{u}).$$

По лемме 4 $\deg G(u) \leq 2$. При $x_1 = x_2 = x_3 = 1$ полином f тождественно равен единице, так что $A + B + C + D + E + F + G = 0$. При других значениях x_1, x_2, x_3 ограничения являются монотонными полиномами. Поскольку минимальная степень минимального монома равна трем, получаем, что среди полиномов A, B, C ненулевые имеют степень 1, ненулевые среди полиномов D, E, F — однородные степени 2, а $G = 0$. Отсюда следует, что $A + B + C = 0$ и $D + E + F = 0$.

Пусть хотя бы один из D, E, F ненулевой, скажем, D . Тождество $D + E + F = 0$ может (с точностью до перестановки переменных) выполняться только при $D = E, F = 0$. В этом случае $S_{110} = A$ и из таблицы монотонных пар (9) получаем, что $D = u_1 u_2, A = u_1$. С другой стороны, $S_{101} = C + D$ и $S_{011} = B + D$ образуют с D монотонные пары, поэтому равны либо $u_1 u_2$, либо $u_1 \vee u_2$, либо $u_1 \vee u_3$. В любом случае $A + B + C \neq 0$.

Пусть $D = E = F = 0$ и хотя бы один из A, B, C не равен 0. Тогда ровно два из них не равны 0. Получаем решение

$$f = x_1 x_2 x_3 + x_1 x_2 u_1 + x_1 x_3 u_1 = x_1 \text{MAJ}(x_2, u_1, u_2). \quad (10^{10})$$

Если $A = B = C = D = E = F = 0$, получаем конъюнкцию трех переменных:

$$f = x_1 x_2 x_3. \quad (10^{11})$$

Итак, с точностью до перестановки переменных есть 11 различных монотонных полиномов степени 3, задаваемых формулами (10^1-10^{11}) .

ЛИТЕРАТУРА

1. **Леонтьев В. К.** О некоторых задачах, связанных с булевыми полиномами // Журн. вычислительной математики и мат. физики. 1999. Т. 39, № 6. С. 1045–1054.
2. **Селезнева С. Н.** О свойствах полиномов над конечными полями и об алгоритмической сложности распознавания свойств функций многозначных логик, представленных полиномами: Дис. ... канд. физ.-мат. наук. М.: МГУ, 2000.

Адреса авторов:

М. Н. Вялый,
В. К. Леонтьев

ВЦ РАН, Вавилова, 40,
117967 Москва, Россия.

E-mail: vyalyi@mccme.ru,
lvk@ccas.ru

М. В. Осетров

МГУ, Воробьевы горы,
119992 Москва, Россия

Статья поступила

18 июня 2002 г.