А.В. Бухман

О РАСПОЗНАВАНИИ ФУНКЦИЙ, ИНВАРИАНТНЫХ ОТНОСИТЕЛЬНО ПРЕОБРАЗОВАНИЯ МЁБИУСА, И ЧЕТНЫХ ФУНКЦИЙ, ЗАДАННЫХ В ФОРМЕ ПОЛИНОМОВ.*

Введение.

Статья относится к исследованиям, решающим следующую задачу: требуется построить эффективный алгоритм, который для булевой функции, поданной ему на вход в виде полинома, определяет, обладает ли эта функция некоторым заданным свойством. При такой постановке проверка непосредственно по определению большинства свойств, используемых на практике, имеет экспоненциальную временную алгоритмическую сложность относительно размера входных данных, то есть размера символьной записи полинома. Поэтому интересным является вопрос о построении полиномиальных алгоритмов. С.Н. Селезневой [1], С.П. Горшковым [2] доказана полиномиальная решаемость задач распознавания ряда свойств для булевых функций.

В данной работе предложены полиномиальные алгоритмы проверки свойств булевых функций, представленных в форме полиномов. В статье рассмотрены два свойства: инвариантность булевой функции относительно преобразования Мёбиуса и чётность булевой функции.

Стоит отметить, что выбранные для рассмотрения свойства имеют практическое значение. Так, свойство функции быть инвариантной относительно преобразования Мёбиуса имеет приложения в криптографии [4]. Свойство чётности функции напрямую связано с самодвойственностью. А последнее свойство важно при исследования на полноту [1].

Статья организована следующим образом. В леммах 1 и 2 установлены некоторые особенности полиномов функций, обладающих рассматриваемыми свойствами. Далее эти леммы применяются для построения полиномиальных алгоритмов, которые для произвольной булевой функции, заданной полиномом Жегалкина, определяют, обладает ли функция интересующими нас свойствами (теоремы 1 и 2). Полученные алгоритмы оказываются очень похожими. Это даёт основание говорить о некоторой схожести функций, обладающих свойством инвариантности относительно преобразования Мёбиуса, и чётных функций. Эта

* Работа выполнена при поддержке РФИИ, грант 12-01-00706а.

особенность отражена в теореме 3, которая устанавливает взаимно однозначное соответствие между двумя классами функций.

Основные определения.

Пусть $E_2 = \{0,1\}$. Будем обозначать E_2^n множество всех упорядоченных наборов длины n из E_2. На множестве E_2^n введём частичный порядок так, что $\alpha \leq \beta$, если каждая компонента набора α меньше либо равна соответствующей компоненты набора β. *Весом* $|\alpha|$ *набора* α называется число единиц в нём. Противоположным к набору α из E_2^n будем называть набор $\bar{\alpha}$ из E_2^n, который отличается от α во всех компонентах.

Булевой функцией, зависящей от n переменных, будем называть любое отображение вида $E_2^n \to E_2$. Множество всех булевых функций, зависящих от n переменных будем обозначать P_2^n.

Будем задавать булевы функций в виде полиномов.

Мономом над переменными $x_1, \dots, x_n$ называется любое выражение вида $x_{i_1} \dots x_{i_l}$, где $1 \leq l \leq n, 1 \leq i_1, \dots, i_l \leq n$, и все переменные различны; либо просто 1.

Рангом $rk(K)$ монома K назовём количество переменных в нём.

Равенство мономов рассматривается с точностью до перестановки сомножителей.

Введём обозначение K_α для монома, соответствующего набору α и равного $x_{i_1} \dots x_{i_l}$, при этом переменная x_{i_j} входит в этот моном тогда и только тогда, когда $\alpha_{i_j} = 1$ (α_{i_j} – компонента вектора α с номером i_j).

Полиномом Жегалкина называется сумма по модулю 2 конечного числа различных мономов или 0 (который можно понимать как сумму нулевого числа мономов).

Индексом $ind(K)$ монома $K = x_{i_1} \dots x_{i_l}$ будем называть множество $\{x_{i_1}, \dots, x_{i_l}\}$.

Введём естественное упорядочение на множестве мономов от переменных $x_1, \dots, x_n$: $K_\alpha \leq K_\beta$, если $\alpha \leq \beta$. Будем писать $K_\alpha < K_\beta$, если $K_\alpha \leq K_\beta$ и $K_\alpha \neq K_\beta$.

Для монома K и полинома П будем писать $K \in$ П, если K является слагаемым полинома П.

Длиной полинома называется число его слагаемых. Длину нулевого полинома будем считать равной 0.

Равенство полиномов рассматривается с точностью до перестановки слагаемых.

Каждая булева функция может быть задана единственным полиномом Жегалкина[3]. Полином Жегалкина функции f будем обозначать $П_f$.

Преобразованием Мёбиуса будем называть отображение $\mu: P_2^n \to P_2^n$, которое функцию $f \in P_2^n$ переводит в функцию $g \in P_2^n$ такую, что $g(\alpha) = \bigoplus_{\beta \le \alpha} f(\beta)$. Будем обозначать $\mu(f) = g$.

Будем говорить, что булева функция f инвариантна относительно преобразования Мёбиуса, если $\mu(f) = f$. Данное свойство исследовалось в работе [4].

В качестве алгоритмической модели будем рассматривать RAM[5].

Если в полиноме l слагаемых и n переменных, то положим, что длина его записи равна $N = ln$.

Функции, инвариантные относительно преобразования Мёбиуса.

Лемма 1. *Пусть функция $f \in P_2^n$ инвариантна относительно преобразования Мёбиуса. Пусть $K \in \Pi_f$ и набор α удовлетворяет условиям, что $f(\alpha) = 0$, $K_\alpha > K$ и не существует $\widetilde{K} \in \Pi_f$ такого, что $K_\alpha > \widetilde{K} > K$. Тогда найдётся слагаемое $K' \in \Pi_f$ такое, что $K'K = K_\alpha$.*

Доказательство.

Для каждого слагаемого $K \in \Pi_f$ функции f проведём индукцию по рангу набора.

Базис. Пусть $|\alpha| = rk(K) + 1$, тогда $Kf(\alpha) = f(\alpha) = 0$. Но при этом $K \in \Pi_{Kf}$. Следовательно, найдётся слагаемое $K' \in \Pi_f$ (возможно не одно, но их должно быть нечётное число) такое, что $K'K = K_\alpha$.

Шаг индукции. Пусть утверждение леммы верно для всех мономов, удовлетворяющих условиям леммы, ранга $s > rk(K)$. Покажем его справедливость для мономов ранга $s + 1$. Возьмём набор α такой, что $|\alpha| = s + 1$. По предположению индукции каждому набору $\beta < \alpha$, такому, что $K_\beta > K$ соответствует нечётное число мономов K'' таких, что $K''K = K_\beta$.

Далее, для разных β соответствующие им мономы K'' различны. Теперь предположим, что нет монома K' такого, что $K'K = K_\alpha$. Тогда, по предположению индукции полином функции Kf содержит слагаемое K_β для всех наборов β таких, что $K_\beta \ge K, rk(K_\beta) \le s$. Следовательно, $K(\alpha)f(\alpha) = 1$ (так как в полиноме Π_{Kf} нечётное число слагаемых K_β, таких, что $K \le K_\beta \le K_\alpha$), но $f(\alpha) = 0$. Приходим к противоречию с тем, что отсутствует слагаемое K' такое, что $K'K = K_\alpha$.

Лемма доказана.

Следствие 1. *Пусть функция $f \in P_2^n$ инвариантна относительно преобразования Мёбиуса. Для любого $K \in \Pi_f$ число наборов α, которые удовлетворяют условиям, что $f(\alpha) = 0$, $K_\alpha > K$ и не существует $\widetilde{K} \in \Pi_f$ такого, что $K_\alpha > \widetilde{K} > K$, не превосходит длины полинома.*

Теорема 1. *Свойство булевой функции быть инвариантной относительно преобразования Мёбиуса можно распознать по её полиному со сложность $O(N^3)$, где N — длина записи полинома.*

Доказательство.

Пусть задана булева функция f.

Все наборы значений её аргументов можно разбить на три группы:

1. Наборы, которым соответствуют мономы, не сравнимые ни с одним слагаемым полинома Π_f или меньшие некоторого минимального из них.

Эти наборы проверять не надо – там функция равна 0, как и требуется в случае, если функция инвариантна относительно преобразования Мёбиуса.

2. Наборы, которым соответствуют мономы, строго большие хотя бы одного слагаемого полинома Π_f и не совпадающие ни с каким другим из них.

На таких наборах функция должна быть равна 0. Проверим, что это выполнено, перебрав все такие наборы. Для каждого монома K, который является слагаемым полинома Π_f проверяем что $f(\alpha) = 0$, для всевозможных наборов α таких, что $K_\alpha > K$ и не существует монома $\widetilde{K} \in \Pi_f$ такого, что $K_\alpha \geq \widetilde{K} > K$. Чтобы функция была инвариантна относительно преобразования Мёбиуса, число проверяемых наборов α, по следствию 1, должно быть не более, чем l (l — длина полинома). Проверка, что $f(\alpha) = 0$, выполняется со сложностью $O(ln)$. Получаем $O(N^2)$ шагов. Всего слагаемых l. Поэтому общая сложность $O(N^3)$.

3. Наборы, соответствующие слагаемым полинома. Чтобы функция была инвариантна относительно преобразования Мёбиуса нужно, чтобы на каждом таком наборе функция равнялась 1. Каждый набор проверяются за линейное время. Всего наборов l, поэтому сложность шага $O(N^2)$.

Теорема доказана.

О сложности распознавания чётности функции по её полиному.

Функция $f \in P_2^n$ называется *чётной*, если для всех наборов $\alpha \in E_2^n$ выполнено $f(\alpha) = f(\bar{\alpha})$.

Полиномиальный алгоритм, который по полиному функции проверяет является ли она чётной, был описан ранее С.Н. Селезневой в работе [1], его сложность была равна $O(N^4)$. Предложенный здесь алгоритм имеет лучшую оценку сложности работы в худшем случае. Приведённый здесь алгоритм имеет сложность $O(N^3)$, чем более ранний.

Лемма 2. Пусть функция $f \in P_2^n$ чётная. Пусть $K \in \Pi_f$ и набор α удовлетворяет условиям, что не существует $\widetilde{K} \in \Pi_f$ такого, что $K > \widetilde{K} \geq K_\alpha$. Тогда найдётся слагаемое $K' \in \Pi_f$ такое, что $ind(K') \cap ind(K) = K_\alpha$.

Доказательство.

Доказательство проведём индукцией по $\rho = |ind(K)| - |ind(K_\alpha)|$.

Базис $\rho = 1$. Рассмотрим полином функции $f(\overline{x_1}, \dots, \overline{x_n})$. Так как функция f – чётная, то слагаемое K_α не принадлежит полиному функции $f(\overline{x_1}, \dots, \overline{x_n})$.

При этом $K(\bar{x}_1,\dots,\bar{x}_n) = K + K_\alpha + \dots$. Следовательно, в полиноме Π_f обязательно найдётся чётное число слагаемых K' таких, что $K'(\overline{x_1}, \dots, \bar{x}_n) = K' + K_\alpha + \cdots$. Последнее равносильно тому, что найдется чётное количество K' таких, что $ind(K') \supseteq ind(K_\alpha)$. При этом, в силу чётности исходной функции, множество $\{K' : ind(K') \supseteq ind(K)\}$ имеет нечётное число элементов. Учитывая, что $\rho = 1$, из теоретико-множественных соображений получаем равенство

$$|\{K' : ind(K') \cap ind(K) \supseteq ind(K_\alpha)\}| = |\{K' : ind(K') \cap ind(K) = ind(K)\}| + |\{K' : ind(K') \cap ind(K) = ind(K_\alpha)\}|.$$

Далее учитывая, что

$$\{K' : ind(K') \cap ind(K) \supseteq ind(K)\} = \{K : ind(K') \supseteq ind(K)\},$$

где $|\{K : ind(K') \supseteq ind(K)\}|$ - нечётное число, и

$$\{K' : ind(K') \cap ind(K) \supseteq ind(K_\alpha)\} = \{K' : ind(K') \supseteq ind(K_\alpha)\},$$

где $|\{K' : ind(K') \supseteq ind(K_\alpha)\}|$ – чётное число, получаем $|\{K' : ind(K') \cap ind(K) = K_\alpha\}|$ – нечётное число.

Шаг индукции. Пусть для всех α, удовлетворяющим условиям леммы и таких, что $\rho = |ind(K)| - |ind(K_\alpha)| < s$, утверждение леммы верно. Покажем его справедливость для $\rho = s$. Рассмотрим $f(\bar{x}_1, \dots, \bar{x}_n)$. Заметим, что слагаемое K_α не входит в полином функции $f(\bar{x}_1, \dots, \bar{x}_n)$. Следовательно, в Π_f будет чётное число слагаемых $\widehat{K}$ таких, что $ind(K_\alpha) \subseteq ind(\widehat{K})$.

Учитывая то, что всего наборов $\beta : K_\alpha < K_\beta \leq K$ нечётное число, и для каждого из них $|\{K' : ind(K_\beta) = ind(K) \cap ind(K')\}|$ – нечётное число (по предположению индукции). Получаем, что

$$|\{K' : ind(K_\alpha) = ind(K) \cap ind(K')\}| = |\{K' : ind(K_\alpha) \subseteq K'\}| - \sum_{K_\alpha < K_\beta \leq K} |\{K' : ind(K_\beta) = ind(K) \cap ind(K')\}|$$

– нечётное число.

Лемма доказана.

Следствие 2. Пусть функция $f \in P_2^n$ чётная. Пусть $K \in \Pi_f$, количество наборов α, удовлетворяющих условию, что не существует $\widetilde{K} \in \Pi_f$ такого, что $K > \widetilde{K} \geq K_\alpha$, будет не больше l.

Теорема 2. *Проверить, является ли функция чётной по её полиному можно со сложностью $O(N^3)$, где N – длина записи полинома.*

Доказательство.

Пусть задана функция $f \in P_2^n$. Надо проверить равенство полиномов двух функций $f(x_1, \dots, x_n)$ и $f(\bar{x}_1, \dots, \bar{x}_n)$.

Все мономы от переменных $x_1, \dots, x_n$ разобьём на три группы:

1. Мономы не сравнимые ни с каким слагаемым полинома функции f или большие некоторого максимального из них.

Эти мономы проверять не надо, так как полином $\Pi_{f(\bar{x}_1,\dots,\bar{x}_n)}$ не будет содержать такие слагаемые, как и $\Pi_{f(x_1,\dots,x_n)}$.

2. Мономы, строго меньшие хотя бы одного слагаемого полинома Π_f и не совпадающие ни с каким другим. Такие мономы отсутствуют в полиноме функции $f(x_1, \dots, x_n)$ и должны отсутствовать в полиноме $f(\bar{x}_1, \dots, \bar{x}_n)$. Просто посчитаем коэффициент при соответствующем мономе в полиноме функции $f(\bar{x}_1, \dots, \bar{x}_n)$. Если хотя бы у одного из них он равен 1, то функция не является чётной. Алгоритм выдаёт – НЕТ.

В силу следствия 2 можно утверждать, что мономов, удовлетворяющих условиям этого шага, не более чем l, для каждого из l слагаемых полинома Π_f. Если их окажется больше, то функция не является чётной, алгоритм останавливается и выдаёт – НЕТ.

Сложность шага $O(lN^2) = O(N^3)$.

3. Мономы, равные слагаемым полинома Π_f. Каждый проверяются за линейное время. Сложность этого шага $O(N^2)$.

Если окажется, что полиномы совпадают, то функция чётная, иначе – нет.

Теорема доказана.

О связи между чётными функциями и функциями инвариантными относительно преобразования Мёбиуса.

Нетрудно заметить, что леммы 1 и 2, а также теоремы 1 и 2 похожи по своим формулировкам и способам доказательств.

Это даёт основание утверждать то, что эти два класса функций связаны между собой. Следующая теорема показывает их связь.

Введём преобразование ν, которое преобразует один полином в другой.

Пусть $П = K_1 + \cdots + K_l$ – полином, который зависит от переменных $x_1,\ldots,x_n$, положим $\nu(П) = K_1' + \cdots + K_l'$, где K_i' это такие мономы, что $ind(K_i') = \{x_1, \ldots, x_n\} \backslash ind(K_i)$.

Теорема 3. *Полином* П *является полиномом чётной булевой функции тогда и только тогда, когда* $\nu(П)$ *является полиномом функции, инвариантной относительно преобразования Мёбиуса.*

Доказательство.

Заметим, что:

1. функция чётная в том и только в том случае, когда для любого набора $\alpha \in E_2^n$ верно, что $|\{K: K > K_\alpha\}|$ – чётное число;

2. функция инвариантна относительно преобразования Мёбиуса в том и только в том случае, когда для любого набора $\alpha \in E_2^n$ верно, что $|\{K: K > K_\alpha\}|$ – чётное число.

Далее из определения ν видно, что если для какого-то полинома П выполнено условие 1, то для $\nu(П)$ будет верно условие 2. И наоборот.

Теорема доказана.

Данную теорему можно применять для того, чтобы доказывать свойства одного класса функций (инвариантных относительно преобразования Мёбиуса или чётных), основываясь на свойствах функций другого класса. Например, в работе [1] было показано, что если полином чётной функции имеет длину l и в нём содержится слагаемое ранга r, то будет верно соотношение $l^2 \geq 2^r$. Тогда для функций инвариантных относительно преобразования Мёбиуса можно сформулировать следующее утверждение.

Утверждение 1. *Пусть* П *– полином функции инвариантной относительно преобразования Мёбиуса. Пусть его длина* l*, и в нём содержится слагаемое ранга* r*, тогда будет верно соотношение* $l^2 \geq 2^{n-r}$.

Доказательство.

Заметим, что преобразование ν обладает следующими свойствами:

1. оно не изменяет длину полинома;

2. слагаемому ранга r оно ставит в соответствие слагаемое ранга $n - r$.

Пусть полином П содержит слагаемое ранга r. Тогда в полиноме $\nu(П)$ будет присутствовать слагаемое ранга $n - r$. Длина $\nu(П)$ равна l. Учитывая, что $\nu(П)$ – полином чётной функции, то для чисел r и l верно $l^2 \geq 2^{n-r}$.

Утверждение доказано.

Список литературы.

1. Селезнева С. Н. О сложности распознавания полноты множества булевых функций, реализованных полиномами Жегалкина// Дискретная математика. 1997. Т. 4, вып. 9. С. 34-41.
2. Горшков С. Н. О сложности распознавания мультиаффинности, биюнктивности, слабой положительности и слабой отрицательности булевой функции. Обозрение прикл. и промышленной матем. Сер. Дискр.матем. 1997. 4, вып. 2. С. 216-237.
3. Яблонский С.В. Введение в дискретную математику. М.:Наука: 1986.
4. Pieprzyk J., Zhang X.-M. Computing mobius transforms of boolean functions and characterising coincident boolean functions// Boolean Functions: Cryptography and Applications. France, Rouen: Publications des Universites de Rouen et du Havre, 2007. P. 135-151.
5. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.:Мир: 1979.