А. В. Архангельская

О РЕШЕНИИ НЕКОТОРЫХ ЗАДАЧ, СВЯЗАННЫХ С ЗАМКНУТЫМИ КЛАССАМИ БУЛЕВЫХ ФУНКЦИЙ

В курсе «Математическая логика и теория алгоритмов», входящем в федеральный компонент специальности 090105 (075500) «Комплексное обеспечение информационной безопасности автоматизированных систем», присутствует раздел, посвященный замкнутым классам булевых функций (б.ф.). Проведение в течение семи лет занятий по данной дисциплине для студентов 3 курса факультета кибернетики и информационной безопасности Национального исследовательского ядерного университет «МИФИ» позволяет утверждать, что у многих слушателей возникают проблемы при решении задач, связанных с замкнутыми классами б.ф. Как правило, это касается задач, в которых требуется определить мощности систем б.ф., привести пример б.ф., принадлежащей к какому-либо классу, и некоторых других. Опыт автора показывает, что большинство ошибок допускается студентами из-за неумения построить четкий алгоритм решения задачи, последовательно изложить необходимые шаги и обосновать связь между ними, т. е. обосновать, почему одно утверждение следует из другого.

Таким образом, целесообразно описать некоторые типовые задачи, связанные с некоторыми замкнутыми классами б.ф., и привести указания по их решению. Отметим, что приведенные методы решения задач могут быть не единственными, а описание всех возможных способов решения задач не является целью настоящей статьи.

Введем необходимые обозначения и приведем определения основных замкнутых классов б.ф., задачи о которых будет рассмотрены далее.

Обозначения:

E_2 — множество, состоящее из двух элементов $\{0,1\}$;

P_2 — класс всех б.ф.;

$P_2(n)$ — класс б.ф., зависящих от n переменных;

T_0 — класс б.ф., сохраняющих константу 0;

$T_0(n)$ — класс б.ф., сохраняющих константу 0 и зависящих от n переменных;

T — класс б.ф., сохраняющих константу 1;

$T_1(n)$ — класс б.ф., сохраняющих константу 1 и зависящих от n переменных;

L — класс линейных б.ф.;

$L(n)$ — класс линейных б.ф., зависящих от n переменных;

A — класс аффинных б.ф.;

$A(n)$ — класс аффинных б.ф., зависящих от n переменных;

S — класс самодвойственных б.ф.;

$S(n)$ — класс самодвойственных б.ф., зависящих от n переменных;

M — класс монотонных б.ф.;

$M(n)$ — класс монотонных б.ф., зависящих от n переменных;

$i = \overline{1,n}$ — число i пробегает натуральные значения от 1 до n;

$\oplus$ — сложение по модулю 2;

$\overline{x}$ — отрицание $x, x \in E_2$;

$x_1 \vee x_2$ — дизъюнкция x_1 и x_2; $x_1, x_2 \in E_2$;

$\alpha_{i_1 \ldots i_k}$ — коэффициент многочлена Жегалкина при элементарной конъюнкции $x_{i_q} x_{i_2} \ldots x_{i_k}$.

Определение 1. Класс б.ф., сохраняющих константу $k, k \in E_2$:

$T_k = \{f \in P_2 : f(k,\ldots k) = k\}$.

Определение 2. Класс линейных б.ф.:

$L = \{f \in P_2 : f = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \ldots \oplus \alpha_n x_n; n = 1,2,\ldots; \alpha_i \in E_2, i = \overline{1,n}\}$.

Определение 3. Класс аффинных б.ф.:

$A = \{f \in P_2 : f = \alpha_0 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \ldots \oplus \alpha_n x_n; n = 1,2,\ldots; \alpha_i \in E_2, i = \overline{1,n}\}$.

Определение 4. Класс самодвойственных б.ф.:

$S = \{f \in P_2 : f(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}; n = 1,2,\ldots\}$.

Определение 5. Класс монотонных б.ф.:

$M = \{f \in P_2 : \forall (a_1, a_2, \ldots, a_n) \le (b_1, b_2, \ldots, b_n) \Rightarrow f(a_1, a_2, \ldots, a_n) \le f(b_1, b_2, \ldots, b_n);$

$n = 1,2,\ldots; a_i, b_i \in E_2, i = \overline{1,n}\}$, где отношение сравнения $\le$ на векторах применяется поэлементно.

Далее рассмотрим типовые задачи и приведем указания по их решению.

Задача 1. Выяснить, является ли аффинной б.ф. $f \in P_2(n)$, заданная вектором-столбцом значений.

Указание. Поскольку вектор-столбец значений б.ф. определяет ее табличное задание, знаем значения б.ф. f на любом векторе из ее области определения. Тогда определим коэффициенты многочлена Жегалкина б.ф. f $\alpha_0, \alpha_1, \ldots, \alpha_n$ по значениям б.ф. f на векторах $(0,0,\ldots,0), (1,0,\ldots,0), \ldots (0,\ldots,0,1)$.

Далее методом неопределенных коэффициентов начинаем находить значения других коэффициентов многочлена Жегалкина, рассматривая значения б.ф. f на наборах веса 2, 3 и т. д. Как только находим коэффициент, отличный от нуля, можно прекратить дальнейший поиск, и тогда $f \notin A$, в противном случае $f \in A$.

Задача 2. Выяснить, является ли аффинной б.ф. $f \in P_2(n)$, заданная в виде формулы.

Указание. Используя следующие формулы: $\overline{x} = x \oplus 1, x_1 \vee x_2 = x_1 \oplus x_2 \oplus x_1 x_2$, получить многочлен Жегалкина б.ф. f, определить степень его нелинейности и, если она не превосходит 1, сделать вывод об аффинности б.ф. f.

Если в исходной формуле для б.ф. f встречаются элементарные б.ф., отличные от конъюнкции, дизъюнкции, отрицания и сложения по модулю 2, можно построить табличное задание б.ф. f и из него получить многочлен Жегалкина, что в общем случае можно сделать методом неопределенных коэффициентов, и по его степени нелинейности определить принадлежность б.ф. f к классу аффинных б.ф. A.

Задача 3. Б.ф. $f \in A(n)$, а вектор-столбец ее значений задан лишь частично, т. е. известны значения б.ф. f на некотором числе наборов. Требуется определить значения б.ф. f на остальных наборах.

Указание. Можно методом неопределенных коэффициентов найти коэффициенты многочлена Жегалкина б.ф. f. Поскольку $f \in A(n)$, в ее многочлене Жегалкина отсутствуют одночлены степени 2 и более, т. е. все коэффициенты $\alpha_{i_1 \ldots i_k} = 0, \mathrm{k} \geq 2$. Лучше рассматривать вектора, на которых известны значения б.ф. f, в порядке по возрастанию их весов.

В некоторых подобных задачах может потребоваться решение системы линейных уравнений в множестве E_2.

Задача 4. Выяснить, принадлежит ли б.ф. f, заданная формулой или вектором-столбцом, множеству $T_1 \setminus T_0$.

Указание. Класс $T_1 \setminus T_0$ содержит б.ф., принадлежащие классу T_1, но не принадлежащие классу T_0, следовательно, необходимо рассмотреть значения б.ф. f на наборах $(0,0,...,0)$ и $(1,1,...,1)$.

Если $f(1,1,...,1) = 0$, то $f \notin T_1 \setminus T_0$. Если $f(1,1,...,1) = 1$ и $f(0,0,...,0) = 1$, то $f \in T_1 \setminus T_0$. Во всех остальных случаях $f \notin T_1 \setminus T_0$.

Задача 5. Найти все значения n, при которых б.ф. $f \in P_2(n)$, заданная в виде формулы, принадлежит классу $T_0 \setminus T_1$.

Указание. Учитывая указание к задаче 5, необходимо решить относительно n следующую систему уравнений:

$$\begin{cases} f(0,0,...0) = 0, \\ f(1,1,...,1) = 0. \end{cases}$$

Задача 6. Найти количество б.ф., зависящих от переменных $x_1, x_2, ..., x_n$ и принадлежащих множеству $K_1 \bigcap K_2$, где $K_1, K_2 \in \{T_0, T_1, A, L, S\}$ и $K_1 \neq K_2$.

Указание. В зависимости от того, какие классы K_1 и K_2 заданы, есть два способа решения задачи. Рассмотрим или табличное задание б.ф., или ее многочлен Жегалкина. Необходимо для выбранного способа задания б.ф. определить, какие ограничения на ее значения или на значения коэффициентов ее многочлена Жегалкина накладывает принадлежность б.ф. множеству $K_1 \bigcap K_2$. Далее необходимо посчитать количество таких б.ф. исходя из указанных ограничений.

Как правило, табличное задание целесообразно рассматривать в том случае, когда $K_1, K_2 \in \{T_0, T_1, S\}$, в противном случае удобнее использовать задание б.ф. в виде многочлена Жегалкина.

Задача 7. Найти количество б.ф., зависящих от переменных $x_1, x_2, ..., x_n$ и принадлежащих множеству $K_1 \bigcup K_2$, где $K_1, K_2 \in \{T_0, T_1, A, L, S\}$ и $K_1 \neq K_2$.

Указание. Используем формулу для определения мощности объединения множеств $|K_1 \cup K_2| = |K_1| + |K_2| - |K_1 \cap K_2|$ и указание к задаче 6.

Задача 8. По вектору значений б.ф. $f \in P_2(n)$ определить, является ли она монотонной.

Указание. Пусть $(\beta_0, \beta_1, \ldots, \beta_{2^n-1})$ — вектор значений б.ф. f, рассмотрим два его непересекающихся подвектора $\beta_0^1 = (\beta_0, \beta_1, \ldots, \beta_{2^{n-1}-1})$ и $\beta_0^2 = (\beta_{2^{n-1}}, \beta_{2^{n-1}+1}, \beta_1, \ldots, \beta_{2^n-1})$. Если отношение $\beta_0^1 \leq \beta_0^2$ не выполнено, то б.ф. f не является монотонной. В противном случае аналогичную операцию выполняем для векторов β_0^1 и β_0^2, т. е. проверяем, выполняется ли отношение $\beta_{\sigma,0}^{1,2} \leq \beta_{\sigma,1}^{1,2}, \sigma \in E_2$ для их подвекторов равной длины. Если хотя бы одно из указанных отношений не выполнено, то б.ф. f не является монотонной. В противном случае продолжаем рассматривать равные подвекторы и проверять выполнение отношения $\leq$ между ними, для монотонной б.ф. f оно должно выполняться для подвекторов произвольной длины.

Задача 9. Определить, является ли монотонной б.ф. $f \in P_2(n)$, заданная в виде формулы.

Указание. Б.ф. f является монотонной, если при помощи эквивалентных преобразований ее можно представить в виде формулы над множеством $\{x_1 x_2, x_1 \vee x_2\}$ или других монотонных

б.ф. Б.ф. f является немонотонной, если из нее можно получить немонотонную б.ф. одной переменной путем замены остальных переменных константами.

Задача 10. Определить, является ли самодвойственной б.ф. $f \in P_2(n)$, заданная в виде формулы.

Указание. В общем случае можно получить задание б.ф. $\overline{f(\overline{x_1}, \overline{x_2}, ..., \overline{x_n})}$ в виде формулы и проверить, равна ли она $f(x_1, x_2, ..., x_n)$. Иногда это проще сделать, найдя вначале многочлен Жегалкина б.ф. $f(x_1, x_2, ..., x_n)$, а затем $\overline{f(\overline{x_1}, \overline{x_2}, ..., \overline{x_n})}$, учитывая, что $\overline{x} = x \oplus 1$.

В некоторых случаях можно использовать следующее свойство: самодвойственная б.ф. равновероятна. Здесь часто встречается ошибка, когда студенты считают равновероятную б.ф. всегда самодвойственной, что очевидно является неверным.

Задача 11. Определить, является ли самодвойственной б.ф. $f \in P_2(n)$, заданная в виде вектора-столбца.

Указание. Табличное задание самодвойственной б.ф. обладает следующим свойством: значения б.ф. на векторах, имеющих одинаковые порядковые номера, если считать сверху и снизу таблицы, должны быть различны. Это следует из того, что указанные вектора равны $(a_1, a_2, ..., a_n)$ и $(\overline{a_1}, \overline{a_2}, ..., \overline{a_n})$ соответственно и для самодвойственной б.ф. f выполняется равенство $f(\overline{a_1}, \overline{a_2}, ..., \overline{a_n}) = \overline{f(a_1, a_2, ..., a_n)}$. Также в некоторых случаях можно воспользоваться тем, что самодвойственная б.ф. равновероятна.

Задача 12. Б.ф. $f \in S(n)$, а вектор-столбец ее значений задан лишь частично, т. е. известны значения б.ф. f на некотором числе наборов. Требуется определить значения б.ф. f на остальных наборах.

Указание. Использовать указание к задаче 11, т. е. если известно значение б.ф. $f(a_1, a_2, ..., a_n)$, то значение $f(\overline{a_1}, \overline{a_2}, ..., \overline{a_n}) = \overline{f(a_1, a_2, ..., a_n)}$.

Можно рассматривать и другие задачи, связанные с замкнутыми классами б.ф., однако приведенные в настоящей статье примеры позволяют выработать методику решения подобных задач и успешно их разрешать.