Дискретная математика.

А. В. Тискин

Содержание

1 Булевые функции

Определение 1. $\mathbb{B} := \{0; 1\}$. *Булевая функция* — $f : \mathbb{B}^n \to \mathbb{B}$.
Множество булевых функций — P_2.
Множество булевых функция — $P_2^{(n)}$.
Количество всех булевых функция — $\left|P_2^{(n)}\right| = 2^{2^n}$.

Определение 2. Базовые функции:

- 0, 1 — функции-константы.
- $\neg x := 1 - x$
- $\wedge$ и $\vee$ — стандартные AND и OR.

Определение 3. Булевая функция $f(x_1, \ldots, x_i, \ldots, x_n)$ *существенно зависит* от x_i, если существуют $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$, что $f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n)$.

Определение 4. Пусть F — множество булевых функций. Тогда *сигнатурой* F или *множеством формул над* F называется множество итеративно заданных формул по принципу:

- формальный символ x;
- $f(A_1, \ldots, A_n)$, где $f \in F$, а $A_1, \ldots, A_n$ — уже определённые функции.

Формула реализует некоторую функцию (не обязательно из F). Формулы реализующие одну и ту же функцию называются *эквивалентными*.

Определение 5. Функция f *выразима* через F, если существует формула над F, реализующая f.

Определение 6. Замыкание F — множество $[F]$ функций, выразимых через F.

Утверждение 1.

- $F \subseteq [F]$

- $F_1 \subseteq F_2 \Rightarrow [F_1] \subseteq [F_2]$
- $[[F]] = [F]$

Определение 7. Множество F булевых функций называется *замкнутым*, если $F = [F]$.

Определение 8. Пусть R замкнуто, а $Q \subseteq R$.

- *Q полно для R*, если $[Q] = R$.
- *R конечно порождаемо*, если существует конечное полное для R множество Q, подмножество R. Минимальное по включение Q — *базис R*.

Определение 9. Функция f называется монотонной, если

$$\forall x_1 \leqslant x_1', \ldots, x_n \leqslant x_n' : f(x_1, \ldots, x_n) \leqslant f(x_1', \ldots, x_n').$$

Утверждение 2. *Множество монотонных функций замкнуто.*

Определение 10.
Литерал — это x или $\neg x$, где x — формальный символ (переменная).
Элементарная конъюнкция — $Y_1 \wedge \cdots \wedge Y_k$, где $Y_1, \ldots, Y_k$ — литералы (с попарно различными элементами).
Элементарная дизъюнкция — $Y_1 \vee \cdots \vee Y_k$, где $Y_1, \ldots, Y_k$ — литералы (с попарно различными элементами).
Дизъюнктивная нормальная форма (ДНФ) — $Z_1 \vee \cdots \vee Z_m$, где $Z_1, \ldots, Z_m$ — (различные) элементарные конъюнкции.
Конъюнктивная нормальная форма (КНФ) — $Z_1 \wedge \cdots \wedge Z_m$, где $Z_1, \ldots, Z_m$ — (различные) элементарные дизъюнкции.
Совершенная ДНФ (СДНФ) функции f от n переменных —

$$f(x_1, \ldots, x_n) = \bigvee_{f(\sigma_1, \ldots, \sigma_n) = 1} x_1^{\sigma_1} \wedge \cdots \wedge x_n^{\sigma_n},$$

где $x^0 = \neg x$, а $x^1 = x$.
Совершенная КНФ (СКНФ) функции f от n переменных —

$$f(x_1, \ldots, x_n) = \bigwedge_{f(\sigma_1, \ldots, \sigma_n) = 0} x_1^{1-\sigma_1} \vee \cdots \vee x_n^{1-\sigma_n},$$

где $x^0 = \neg x$, а $x^1 = x$.

Утверждение 3. *Система $\{\neg, \wedge, \vee\}$ полна (в P_2).*

Следствие 3.1. *Системы $\{\neg . \wedge\}$, $\{\neg, \vee\}$, $\{1, \wedge, \oplus\}$, $\{\uparrow\}$ и $\{\downarrow\}$ полны.*

Определение 11. Аналогично определяется *(совершенная) конъюктивная нормальная форма (КНФ)*.

Определение 12. *Двойственная функция* к f — $f^* := \neg f(\neg x_1, \ldots, \neg x_n)$.

Свойства:

- $f^{**} = f$

Утверждение 4 (принцип двойственности)**.** *Если f реализуема формулой Φ, то f^* реализуема формулой Φ^*, где все функции заменяются на двойственные.*

Определение 13 (полином Жегалкина (над $\mathbb{F}_2$))**.** Выражение функции в базисе $\{1, \wedge, \oplus\}$.

$$f(x_1, \ldots, x_n) = \sum_{\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, n\}} a_{i_1, \ldots, i_n} x_{i_1} \ldots x_{i_s}$$

Теорема 5 (Жегалкин)**.** *Любая функция реализуется полиномом Жегалкина единственным образом (с точностью до пропуска членов тождественно равных 0 и перестановок слагаемых и сомножителей).*

Доказательство. Всего коэффициентов $a_{i_1, \ldots, i_s}$ — 2^n. Тогда многочленов Жегалкина ровно 2^{2^n}; сколько и булевых функций. Покажем, что для каждой функций найдётся полином Жегалкина, и тогда докажем теорему.

Построение полинома аналогично рассуждению в формуле включений-исключений. Сначала рассмотрим значение f в точке $(0, \ldots, 0)$: оно определяет свободный член полинома. Далее рассмотрим значение f и имеющегося полинома (пока что состоящего только из, может быть, свободного члена) в точках вида $(0, \ldots, 0, 1, 0, \ldots, 0)$: по ним определяются коэффициенты при мономах первой степени (по аналогии с формулой включений-исключений). Так далее определяются все коэффициенты. □

Определение 14. Функция f *самодвойствена*, если $f = f^*$.

Пример 1.

- e_i и $\neg e_i$ для любого n и i самодвойственны;
- $\vee$, $\wedge$, $\oplus$, $\rightarrow$, $\leftarrow$, $\uparrow$ и $\downarrow$ не самодвойствены.

Утверждение 6. *Класс S самодвойственных функций замкнут.*

Определение 15. f *линейна*, если $f(x_1, \ldots, x_n) = a_0 \oplus (a_1 \wedge x_1) \oplus \cdots \oplus (a_n \wedge x_n)$ для некоторых $a_1, \ldots, a_n$.

Они же представляются как полиномы Жегалкина степени не выше первой.

Утверждение 7. *Класс L линейных функций замкнут.*

Теорема 8 (теорема Поста)**.** *Система функций полна (в P_2) тогда и только тогда, когда она не содержится целиком ни в одном из T_0, T_1, S, L и M.*

Доказательство. Пусть даны $f_0 \notin T_0$, $f_1 \notin T_1$, $f_S \notin S$, $f_L \notin L$, $f_M \notin M$.

Заметим, что $f_0(x, \ldots, x) \in \{1.\neg\}$, а $f_1(x, \ldots, x) \in \{0, \neg\}$. Тогда либо $0, 1 \in [\{f_0, f_1\}]$, либо $\neg \in [\{f_0, f_1\}]$.

Заметим, что для некоторых $\sigma_1, \ldots, \sigma_n$ имеем $f_S(\sigma_1, \ldots, \sigma_n) = f_S(\neg\sigma_1, \ldots, \neg\sigma_n)$. Поэтому $f_S(x_1^\sigma, \ldots, x_n^\sigma)$ — константная функция, а тогда она и $\neg f_S(x_1^\sigma, \ldots, x_n^\sigma)$ вместе дают 0 и 1, поэтому $0, 1 \in [\{\neg, f_S\}]$.

Заметим, что $\neg \in [\{0, 1, f_M\}]$.

Заметим, что $\wedge \in [\{f_L\}]$ или $\uparrow \in [\{f_L\}]$. Для заметим, что в полиноме Жегалкина f_L есть член хотя бы второй степени. □

2 Комбинаторика

Утверждение 9 (правило произведения)**.** *Если объект A можно выбрать m способами, а B — n, то пару $(A; B)$ можно выбрать mn способами.*

Утверждение 10 (правило суммы)**.** *Если объект A иожно выбрать m способами, а B — n способами, то объект "A или B" — $m+n$ способами.*

Утверждение 11 (принцип Дирихле)**.** *Пусть имеется $n+1$ шаров, разложенных по n урнам, то найдётся урна с хотя бы 2 шарами.*

Утверждение 12 (обобщённый принцип Дирихле)**.** *Пусть имеется n шаров, разложенных по k урнам, то найдётся урна с хотя бы $\lceil \frac{n}{k} \rceil$ шарами.*

Определение 16. *Упорядоченная расстановка* n элементов в ряд есть упорядоченная последовательность этих n элементов без повторений. Количество упорядоченных расстановок на n элементах равно $n! := \prod_{k=1}^{n} k$.

Упорядоченная расстановка k элементов из n в ряд есть упорядоченная последовательность каких-то k элементов из n без повторений. Количество упорядоченных расстановок k элементов из n равно $P(n,k) = A_n^k = \frac{n!}{(n-k)!}$.

k-элементная *выборка* среди n элементов есть подмножество множества данных n элементов. Таких выборок $\binom{n}{k} = C_n^k = \frac{n!}{k!(n-k)!}$.

Утверждение 13. *Свойства:*

1. $\binom{n}{k} = \binom{n}{n-k}$.

2. *(тождество Паскаля)* $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

3. *(биномиальная теорема)*
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

4. $$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

5. $$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{k} = 2^{n-1}$$

6. *(тождество Вандермонда)*
$$\binom{m+n}{k} = \sum_{r=0}^{k} \binom{m}{r} \binom{n}{k-r}$$

Определение 17. *Треугольником Паскаля* называется диаграмма следующего вида.

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Здесь каждое число равно сумме своих верхних соседей, а порождающими являются единичные левая и правая "стороны" диграммы.

3 Теория графов

To be read...