Дискретная математика.

А. В. Тискин
alextiskin@gmail.com

Содерждание:

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 — $P_2^{(n)}$.
Количестов 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 $f(x_1, \dots, x_i, \dots, x_n)$ *существенно зависит* от x_i, если существуют $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$, что $f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)$.

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;
- $f(A_1, \dots, A_n)$, где $f \in F$, а $A_1, \dots, A_n$ — 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, реализующаая 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 сущесвтует конечное полное для R множество Q, подмножество R. Минимальное по включение Q — *базис R*.

Определение 9. Функция f называется монотонной, если

$$\forall x_1 \leqslant x'_1, \dots, x_n \leqslant x'_n : f(x_1, \dots, x_n) \leqslant f(x'_1, \dots, x'_n).$$

Утверждение 2. *Если F — множество монотонных функций, то $[F]$ — множество монотонных функций.*

Определение 10.
Литерал — это x или $\neg x$, где x — формальный символ (переменная).
Элементарная конъюкция — $Y_1 \wedge \dots \wedge Y_k$, где $Y_1, \dots, Y_k$ — литералы (с попарно различными элементами).
Дизъюнктивная нормальная форма (ДНФ) — $Z_1 \vee \dots \vee Z_m$, где $Z_1, \dots, Z_m$ — (различные) элементарные конъюнкции.
Совершенная ДНФ — для любой функции f от n переменных

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

где $x^0 = x$, а $x^1 = \neg x$.

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

Следствие 0.1. *Системы $\{\neg . \wedge\}$, $\{\neg, \vee\}$, $\{1, \wedge, \oplus\}$, $\{\uparrow\}$ и $\{\downarrow\}$ полны.*

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

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

Свойтсва:

- $f^{**} = f$

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 $\{1, \wedge, \oplus\}$.

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

Теорема 1 (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 2^{2^n}; столько 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;
- $\vee$, $\wedge$, $\oplus$, $\to$, $\leftarrow$, $\uparrow$ и $\downarrow$ не самодвойствены.