Дискретная математика. Модуль 3. Лекция 1

Клуб альтруистичных и настойчивых

11 января 2016

Схемы. Булевы схемы

Важное примечание: В данной лекции все рассмотренные функции являются *всюду определенными.*

Схема — это функция, заданная последовательность присваиваний.

Также в профессиональной среде схемы принято называть SLP (*straight line programmes*).

Рассмотрим такую функцию f, определенную для булевых значений (*булеву функцию*): $f : \{0, 1\}^n \to \{0, 1\}$.

Базисом В булевой функции будем называть некий набор $B : \{f_1, f_2, \ldots, f_n\}$, где $f_1 \ldots f_n$ - булевы функции.

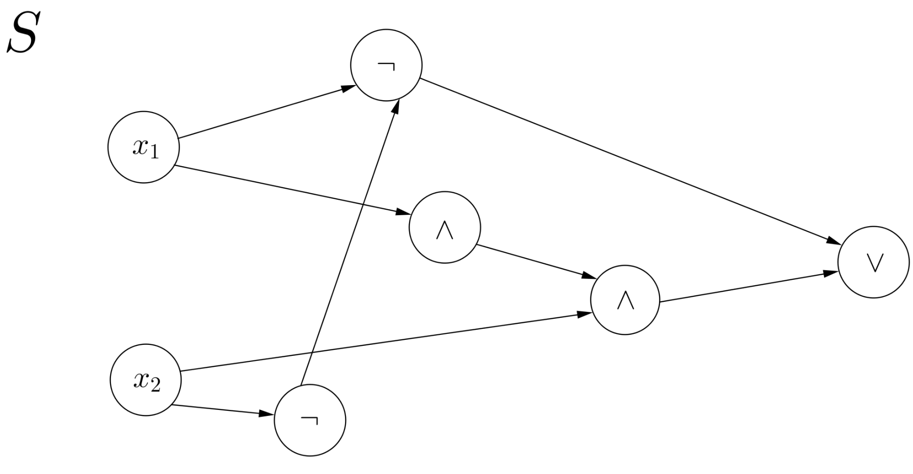
Булева схема в базисе B — последовательность функций $x_1, x_2, x_3 ... x_n, x_{n+1} := S_1, x_i := S_{L-n}$, которая вычисляет $x_L(x_1, \ldots, x_n)$.

$$S_j = g(S_{i_1}, ..., s_{i_r}), g \in B, i_< j$$

Стандартный базис есть базис, состоящий из операций отрицания, конъюнкции и дизъюнкции: $\{\neg, \vee, \wedge\}$

Пример 1

Стандартный базис. $x_1, \ldots x_n, s_1 := \neg x_1, s_2 = \neg x_2, s_3 := x_1 \wedge s_2, s_4 = x_2 \wedge s_1; s_5 = s_3 \vee s_4$



Если $x_2 = 0$, то $s_5 = x_1$

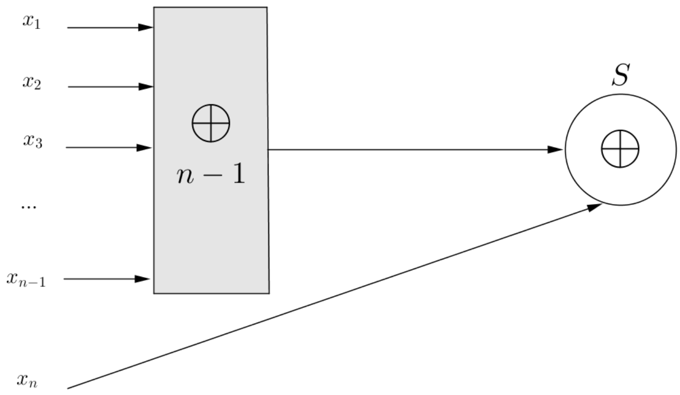
Если $x_2 = 1$, то $s_5 = \neg x_1$

Результатом является сложение по модулю 2 (1, если значения x_1 и x_2 разные) - $\oplus$.

Пример 2

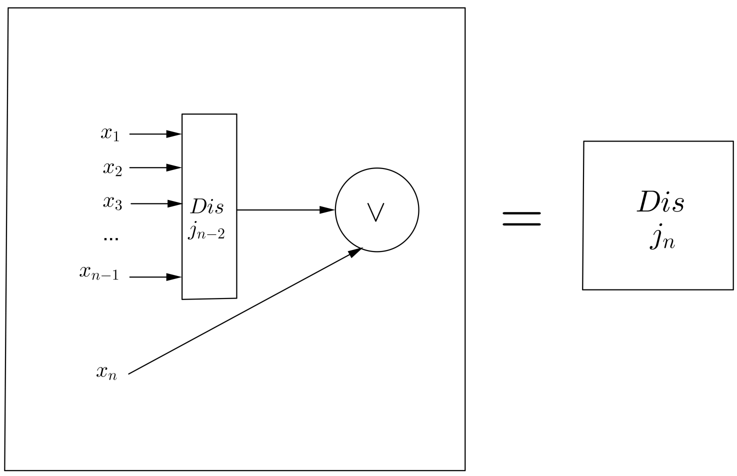
Составим схему которая является xor нескольких переменных. Индуктивное доказательство существования такой функции:

$x_1 \oplus x_2 \oplus \ldots \oplus x_{n-1} \oplus x_n = (x_1 \oplus x_2 \oplus \ldots \oplus x_{n-1}) \oplus x_n$



Пример 3

Дизъюнкция n переменных — аналогично, по индукции. Такие рассуждения можно построить и для конъюнкции.



Анализ схем

Анализ базисов: все ли функции можно выразить через схему в данном базисе?

Полный базис: Базис B - *полный*, если любую булеву функцию можно вычислить схемой в базисе B.

Теорема о стандартном базисе. *Стандартный базис — полный.*

Доказательство. Вспомним, что ДНФ - это дизъюнкция конъюнктов литералов. Построим схему ДНФ.

$x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n, c_1, \ldots, c_n, D$, где c_j — конъюнкция литералов, D — дизъюнкция. Данный порядок действий соответствует определению ДНФ, следовательно ДНФ представима в виде схемы и любая функция представима в виде ДНФ. что доказано ранее. (Note: $0 = x \wedge \neg x, 1 = x \vee \neg x$) **Q.E.D.**

Лемма. *Пусть базис B_1 — полный.*

$\forall f \in B_1$ *вычисляется схемой в базисе B_2.*

Тогда B_2 — полный.

Доказательство. Вычислим схему в базисе B_1.

$(B_1) x_1, \ldots x_n, s_j :=$вычисление $f, F(..)$

Теперь вычислим схему в базисе B_2.
(B_2)вычисление $f, F(..)$

Q.E.D.

Примечание: Заметим, что если стандартный базис выразим через некоторые функции, то данные функции будут составлять полный базис.

Следствие 1. *Полнота базиса Жегалкина* $\{1, x_1 \wedge x_2, x_1 \oplus x_2\}$.

Доказательство. $\neg x_1 = 1 \oplus x_1$ $x_1 \vee x_2 = x_1 \oplus x_2 \oplus (x_1 \wedge x_2)$ или $x_1 \vee x_2 = \neg(\neg x_1 \wedge \neg x_2)$ **Q.E.D.**

Немного о схемах.
Любая формула является схемой. При этом формула — частный случай схемы. Не любая схема — формула.
Пример: $x_1 \oplus x_2 = x_1 \wedge \neg x_2 \vee \neg x_1 \wedge x_2 = F(x_1 \oplus x_2) \oplus x_3 = (F) \wedge \neg x_3 \vee \neg F \wedge x_3$

Следствие 2. *Полнота базиса* $\neg, \wedge$.

Доказательство. $x \vee y = \neg(\neg x \wedge \neg y)$ **Q.E.D.**

Функция $f : \{0,1\}^n \to \{0,1\}$ называется *монотонной*, если $\forall i : x_i \leqslant y_i \Rightarrow f(x_1 \ldots x_n) \leqslant f(y_1 \ldots y_n)$
Монотонный базис — это базис $\vee, \wedge$

Теорема о монотонном базисе. *Монотонный базис* $\{\vee, \wedge\}$ *— неполный*

Доказательство. Воспользоваться монотонностью функций $x_1 \vee x_2$ и $x_1 \wedge x_2$ и немонотонностью функции $\neg x_1$ **Q.E.D.**

Утверждение 1. *Схема в монотонном базисе вычисляет монотонную функцию.*

Доказательство. Доказываем индукцией по размеру схем

$$x_1, \ldots, x_n, S_1 \ldots S_L, S_{L+1}$$

$$s_{L+1} := f(s_{i_1} ... s_{i_r})$$
$$S_{i\alpha}(x) \leqslant S_{i\alpha}(y)$$

Так как f — монотонная

$$S_{L+1}(x) \leqslant S_{L+1}(y)$$

Q.E.D.

Заметим также неполноту следующих базисов:

1. $\{\wedge, \oplus\}$
2. $\{1, \wedge\}$
3. $\{1, \oplus\}$

Утверждение 2. *Пусть f вычисляется схемой в базисе $\{1, \oplus\}$. Тогда* $f = a_0 \oplus \oplus_{i=1}(a_i \wedge x_i)$

Доказательство.

$$a_0 + \sum a_i x_i + b_0 + \sum b_i x_i = (a_0 + b_0) + \sum (a_i + b_i) x_i$$

Q.E.D.

Не все булевы функции — линейные
Линейных функций — 2^{n+1}
Булевых функций — 2^{2^n}
Получается, линейных функций меньше.