Лекция 8. Условная выразимость функций. Леммы об условной выразимости. Лемма о функции, не сохраняющий единицу, и о функции, сохраняющей ноль. Лемма о несамодополнительной функции. Лемма о самодополнительной функции.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Условная выразимость

Функция $h(x_1, \dots, x_n, y_1, \dots, y_m) \in P_2$ **условно выражает** функцию $g(x_1, \dots, x_n) \in P_2$ с **вспомогательными переменными** $y_1, \dots, y_m$, $m \geqslant 0$, если для любого набора $\alpha \in E_2^n$ выполняется следующее:

1) если $g(\alpha) = 1$, то **найдется** такой набор $\beta \in E_2^m$, что $h(\alpha, \beta) = 1$;

2) если $g(\alpha) = 0$, то **для любого** набора $\beta \in E_2^m$ верно $h(\alpha, \beta) = 0$.

Условная выразимость

Например, функция $h(x_1, x_2, y_1) = x_1 \oplus x_2 \cdot y_1$ условно выражает функцию $g(x_1, x_2) = x_1 \vee x_2$ с вспомогательной переменной y_1.

Если $\alpha = (0, 0) \in E_2^2$, то $g(0, 0) = 0$ и $h(0, 0, y_1) = 0$.

Если $\alpha \in E_2^2$ и $\alpha \neq (0, 0)$, то $g(\alpha) = 1$. В этом случае при $\alpha = (1, 0)$ или $\alpha = (1, 1)$ подходит $y_1 = 0$, при $\alpha = (0, 1)$ подходит $y_1 = 1$.

Условная выразимость

Утверждение 1. *Функция* $h(x_1, \ldots, x_n, y_1, \ldots, y_m) \in P_2$ *условно выражает функцию* $g(x_1, \ldots, x_n) \in P_2$ *с вспомогательными переменными* $y_1, \ldots, y_m$, $m \geqslant 0$, *тогда и только тогда, когда выполняется равенство:*

$$g(x_1, \ldots, x_n) = \bigvee_{\beta \in E_2^m} h(x_1, \ldots, x_n, \beta).$$

Условная выразимость

Например, функция $h(x_1, x_2, y_1) = x_1 \oplus x_2 \cdot y_1$ условно выражает функцию $g(x_1, x_2) = x_1 \vee x_2$ с вспомогательной переменной y_1:

$$h(x_1, x_2, 0) \vee h(x_1, x_2, 1) = x_1 \vee (x_1 \oplus x_2) = x_1 \vee x_2 = g(x_1, x_2).$$

Условная выразимость

Утверждение 2. *Функция* $h(x_1, \dots, x_n, y_1, \dots, y_m) \in P_2$ *условно выражает функцию* $g(x_1, \dots, x_n) \in P_2$ *с вспомогательными переменными* $y_1, \dots, y_m$, $m \geqslant 0$, *тогда и только тогда, когда выполняется равенство:*

$$g(x_1, \dots, x_n) = \exists y_1 \dots \exists y_m h(x_1, \dots, x_n, y_1, \dots, y_m).$$

Лемма о транзитивности условной выразимости

Лемма 1 (о транзитивности условной выразимости). *Если* $h_1(x_1, \ldots, x_n, y_1, \ldots, y_m) \in P_2$ *условно выражает* $g(x_1, \ldots, x_n) \in P_2$ *с вспомогательными переменными* $y_1, \ldots, y_m$, $m \geqslant 0$, *и* $h_2(x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_k) \in P_2$ *условно выражает* $h_1(x_1, \ldots, x_n, y_1, \ldots, y_m)$ *с вспомогательными переменными* $z_1, \ldots, z_k$, $k \geqslant 0$, *то* $h_2(x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_k)$ *условно выражает* $g(x_1, \ldots, x_n)$ *с вспомогательными переменными* $y_1, \ldots, y_m, z_1, \ldots, z_k$.

Лемма о транзитивности условной выразимости

Доказательство. Рассмотрим произвольный набор $\alpha \in E_2^n$.

1. Если $g(\alpha) = 1$, то, т. к. h_1 условно выражает g, найдется такой набор $\beta \in E_2^m$, что $h_1(\alpha, \beta) = 1$.

Т. к. h_2 условно выражает h_1, найдется такой набор $\gamma \in E_2^k$, что $h_2(\alpha, \beta, \gamma) = 1$.

Значит, найдется такой набор $(\beta, \gamma) \in E_2^{m+k}$, что $h_2(\alpha, \beta, \gamma) = 1$.

Лемма о транзитивности условной выразимости

Рассмотрим произвольный набор $\alpha \in E_2^n$.

2. Если $g(\alpha) = 0$, то, т. к. h_1 условно выражает g, для любого набора $\beta \in E_2^m$ верно $h_1(\alpha, \beta) = 0$.

Т. к. h_2 условно выражает h_1, для любого набора $\gamma \in E_2^k$ верно $h_2(\alpha, \beta, \gamma) = 0$.

Значит, для любого набора $(\beta, \gamma) \in E_2^{m+k}$ верно $h_2(\alpha, \beta, \gamma) = 0$.

Следовательно, h_2 условно выражает g.

$\square$

Лемма о замене множителя

Лемма 2 (о замене множителя). *Пусть* $g, g_1, g_2 \in P_2$,

$$g(x_1, \dots, x_n) = g_1(x_1, \dots, x_{n_1}) \cdot g_2(x_1, \dots, x_n),$$

где $n_1 \leqslant n$. *Если* $h_1(x_1, \dots, x_{n_1}, y_1, \dots, y_m) \in P_2$ *условно выражает* $g_1(x_1, \dots, x_{n_1})$ *с вспомогательными переменными* $y_1, \dots, y_m$, $m \geqslant 0$, *причем никакая переменная* y_j *не совпадает ни с какой переменной* x_i, $i = n_1 + 1, \dots, n$, $j = 1, \dots, m$, *то* $h(x_1, \dots, x_n, y_1, \dots, y_m) \in P_2$,

$$h(x_1, \dots, x_n, y_1, \dots, y_m) = h_1(x_1, \dots, x_{n_1}, y_1, \dots, y_m) \cdot g_2(x_1, \dots, x_n),$$

условно выражает $g(x_1, \dots, x_n)$ *с вспомогательными переменными* $y_1, \dots, y_m$.

Лемма о замене множителя

Доказательство. Рассмотрим произвольный набор $\alpha = (\alpha_1, \alpha_2) \in E_2^n$, где $\alpha_1 \in E_2^{n_1}$.

1. Если $g(\alpha) = 1$, то $g_1(\alpha_1) = 1$ и $g_2(\alpha) = 1$.

Т. к. h_1 условно выражает g_1, найдется такой набор $\beta \in E_2^m$, что $h_1(\alpha_1, \beta) = 1$.

Т. к. множества переменных $\{x_{n_1+1}, \ldots, x_n\}$ и $\{y_1, \ldots, y_m\}$ не пересекаются, для этого набора $\beta \in E_2^m$ верно $h(\alpha, \beta) = 1$.

Лемма о замене множителя

Рассмотрим произвольный набор $\alpha = (\alpha_1, \alpha_2) \in E_2^n$, где $\alpha_1 \in E_2^{n_1}$.

2. Если $g(\alpha) = 0$, то либо $g_1(\alpha_1) = 0$, либо $g_2(\alpha) = 0$.

2а) Если $g_1(\alpha_1) = 0$, то, т. к. h_1 условно выражает g_1, для любого набора $\beta \in E_2^m$ верно $h_1(\alpha_1, \beta) = 0$.

Значит, для любого набора $\beta \in E_2^m$ верно $h(\alpha, \beta) = 0$.

2б) Если же $g_2(\alpha) = 0$, то для любого набора $\beta \in E_2^m$ верно $h(\alpha, \beta) = 0$.

Следовательно, h условно выражает g.

$\square$

Условная выразимость над множеством

Пусть $S \subseteq P_2$.

Функция $g \in P_2$ **условно выразима** над S, если найдется некоторая S-КНФ, представляющая такую функцию $h \in P_2$, что h условно выражает g с какими-то вспомогательными переменными.

Лемма о подстановке константы

Лемма 3 (о подстановке константы). *Функция*

$$g_\sigma(x_2, \ldots, x_n) = g(\sigma, x_2, \ldots, x_n) \in P_2,$$

где $g(x_1, x_2, \ldots, x_n) \in P_2$, $\sigma \in E_2$, *условно выразима над множеством* $S = \{g, x^\sigma\} \subseteq P_2$.

Лемма о подстановке константы

Доказательство. Положим

$$h(x_2, \dots, x_n, y) = y^\sigma \cdot g(y, x_2, \dots, x_n).$$

Покажем, что $h(x_2, \dots, x_n, y)$ условно выражает $g_\sigma(x_2, \dots, x_n)$ с вспомогательной переменной y.

Рассмотрим произвольный набор $\alpha \in E_2^{n-1}$.

Лемма о подстановке константы

Итак,

$$h(x_2, \dots, x_n, y) = y^\sigma \cdot g(y, x_2, \dots, x_n)$$

и $\alpha \in E_2^{n-1}$ — произвольный набор.

1. Если $g_\sigma(\alpha) = 1$, то при $y = \sigma$ получаем

$$h(\alpha, \sigma) = \sigma^\sigma \cdot g(\sigma, \alpha) = g_\sigma(\alpha) = 1.$$

Лемма о подстановке константы

Итак,

$$h(x_2, \ldots, x_n, y) = y^\sigma \cdot g(y, x_2, \ldots, x_n)$$

и $\alpha \in E_2^{n-1}$ — произвольный набор.

2. Пусть $g_\sigma(\alpha) = 0$.

2а) При $y = \sigma$ получаем:

$$h(\alpha, \sigma) = \sigma^\sigma \cdot g(\sigma, \alpha) = g_\sigma(\alpha) = 0.$$

2б) При $y = \bar{\sigma}$ получаем:

$$h(\alpha, \bar{\sigma}) = \bar{\sigma}^\sigma \cdot g(\bar{\sigma}, \alpha) = 0.$$

Следовательно, h условно выражает g_σ.

$\square$

Выразимость подфункций

Следствие. *Пусть* $S \subseteq P_2$ *и* $x \in S$, $\bar{x} \in S$. *Если* $g(x_1, \ldots, x_n) \in S$, *то для любого набора* $\sigma \in E_2^k$, $0 \leqslant k \leqslant n$, *подфункция* $g_\sigma(x_{k+1}, \ldots, x_n)$,

$$g_\sigma(x_{k+1}, \ldots, x_n) = g(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n),$$

условно выразима над S.

Лемма о навешивании отрицания

Лемма 4 (о навешивании отрицания). *Функция*

$$g'(x_1, x_2, \ldots, x_n) = g(\bar{x}_1, x_2, \ldots, x_n) \in P_2,$$

где $g(x_1, x_2, \ldots, x_n) \in P_2$, *условно выразима над множеством* $S = \{g, x_1 \oplus x_2\} \subseteq P_2$.

Лемма о навешивании отрицания

Доказательство. Положим

$$h(x_1, \ldots, x_n, y) = (x_1 \oplus y) \cdot g(y, x_2, \ldots, x_n).$$

Покажем, что $h(x_1, \ldots, x_n, y)$ условно выражает $g'(x_1, x_2, \ldots, x_n)$ с вспомогательной переменной y.

Рассмотрим произвольный набор $\alpha = (a, \alpha_1) \in E_2^n$, где $a \in E_2$, $\alpha_1 \in E_2^{n-1}$.

Лемма о навешивании отрицания

Итак,

$$h(x_1, \ldots, x_n, y) = (x_1 \oplus y) \cdot g(y, x_2, \ldots, x_n)$$

и $\alpha = (a, \alpha_1) \in E_2^n$ — произвольный набор, где $a \in E_2$, $\alpha_1 \in E_2^{n-1}$.

1. Если $g'(\alpha) = 1$, то при $y = \bar{a}$ получаем

$$h(\alpha, \bar{a}) = (a \oplus \bar{a}) \cdot g(\bar{a}, \alpha_1) = g'(\alpha) = 1.$$

Лемма о навешивании отрицания

Итак,

$$h(x_1, \dots, x_n, y) = (x_1 \oplus y) \cdot g(y, x_2, \dots, x_n)$$

и $\alpha = (a, \alpha_1) \in E_2^n$ — произвольный набор, где $a \in E_2$, $\alpha_1 \in E_2^{n-1}$.

2. Пусть $g'(\alpha) = 0$.

2а) При $y = a$ получаем:

$$h(\alpha, a) = (a \oplus a) \cdot g(a, \alpha_1) = 0.$$

2б) При $y = \bar{a}$ получаем:

$$h(\alpha, \bar{a}) = (a \oplus \bar{a}) \cdot g(\bar{a}, \alpha_1) = g'(\alpha) = 0.$$

Следовательно, h условно выражает g'.

$\square$

Лемма о функции не из T_1 и о функции из T_0

Лемма 5 (о функции, не сохраняющей единицу, и о функции, сохраняющей ноль). *Если* $S = \{g_1, g_0\} \subseteq P_2$, *где* $g_1 \notin T_1$, $g_1 \neq 0$, $g_0 \in T_0$, $g_0 \neq 0$, *то либо* x *и* $\bar{x}$ *условно выразимы над множеством* S, *либо* $x_1 \oplus x_2$ *условно выразима над множеством* S.

Лемма о функции не из T_1 и о функции из T_0

Доказательство. Итак, $g_1(1,\ldots,1) = 0$. Т. к. $g_1 \neq 0$, найдется такой набор $\alpha \in E_2^n$, что $g_1(\alpha) = 1$. Не ограничивая общности рассуждений, пусть $\alpha = (\underbrace{0,\ldots,0}_{k},\underbrace{1,\ldots,1}_{n-k})$.

Если $k = n$, то положим $\varphi_1(x) = g_1(x,\ldots,x)$:

x	φ_1
0	1
1	0

Т. е. $\varphi_1(x) = \bar{x}$.

Лемма о функции не из T_1 и о функции из T_0

Пусть теперь $g_1(0,\ldots,0) = 0$ и $1 \leqslant k \leqslant n-1$. Положим
$\varphi_1(x_1, x_2) = g_1(\underbrace{x_1,\ldots,x_1}_{k}, \underbrace{x_2,\ldots,x_2}_{n-k})$:

x_1	x_2	φ_1
0	0	0
0	1	1
1	0	a
1	1	0

где $a \in E_2$.

Рассмотрим возможные случаи.

Лемма о функции не из T_1 и о функции из T_0

Пусть $a = 0$:

x_1	x_2	φ_1
0	0	0
0	1	1
1	0	0
1	1	0

Значит, $\varphi_1(x_1, x_2) = \bar{x}_1 x_2$.

Теперь $\varphi_1(y, x) = \bar{y} \cdot x$ условно выражает x с вспомогательной переменной y.

Далее $\varphi_1(x, y) = \bar{x} \cdot y$ условно выражает $\bar{x}$ с вспомогательной переменной y.

Лемма о функции не из T_1 и о функции из T_0

Пусть $a = 1$:

x_1	x_2	φ_1
0	0	0
0	1	1
1	0	1
1	1	0

Значит, $\varphi_1(x_1, x_2) = x_1 \oplus x_2$.

Лемма о функции не из T_1 и о функции из T_0

Если получена только $\bar{x}$, то проведем аналогичные рассуждения для g_0 и получим либо x, либо $x_1 \oplus x_2$.

$\square$

Самодополнительная функция

Функция $f(x_1, \ldots, x_n)$ называется **самодополнительной**, если

$$f(\bar{x}_1, \ldots, \bar{x}_n) = f(x_1, \ldots, x_n).$$

Например, функция $x_1 \oplus x_2$ является самодополнительной, т. к.

$$\bar{x}_1 \oplus \bar{x}_2 = (x_1 \oplus 1) \oplus (x_2 \oplus 1) = x_1 \oplus x_2.$$

Отметим, что не существует самодополнительных функций, **существенно** зависящих от одной переменной.

Лемма о несамодополнительной функции

Лемма 6 (о несамодополнительной функции). *Если $S = \{g, x_1 \oplus x_2\} \subseteq P_2$, где g — несамодополнительная функция, то x и $\bar{x}$ условно выразимы над множеством S.*

Лемма о несамодополнительной функции

Доказательство. Итак, g — несамодополнительная функция. Значит, найдется такой набор $\alpha \in E_2^n$, что $g(\alpha) = 1$ и $g(\bar{\alpha}) = 0$. Не ограничивая общности рассуждений, пусть $\alpha = (\underbrace{0, \ldots, 0}_{k}, \underbrace{1, \ldots, 1}_{n-k})$.

Если $k = n$, то положим $\varphi_1(x) = g(x, \ldots, x)$:

x	φ_1
0	1
1	0

Т. е. $\varphi_1(x) = \bar{x}$.
По лемме о навешивании отрицания $(x \oplus y) \cdot \varphi_1(y) = (x \oplus y) \cdot \bar{y}$ условно выражает x с вспомогательной переменной y.

Лемма о несамодополнительной функции

Пусть теперь $g(0,\ldots,0) = g(1,\ldots,1)$ и $1 \leqslant k \leqslant n-1$.
Положим $\varphi_1(x_1,x_2) = g(\underbrace{x_1,\ldots,x_1}_{k},\underbrace{x_2,\ldots,x_2}_{n-k})$:

x_1	x_2	φ_1
0	0	a
0	1	1
1	0	0
1	1	a

где $a \in E_2$.

Рассмотрим возможные случаи.

Лемма о несамодополнительной функции

Пусть $a = 0$:

x_1	x_2	φ_1
0	0	0
0	1	1
1	0	0
1	1	0

Значит, $\varphi_1(x_1, x_2) = \bar{x}_1 x_2$.

Теперь $\varphi_1(y, x) = \bar{y} \cdot x$ условно выражает x с вспомогательной переменной y.

Далее $\varphi_1(x, y) = \bar{x} \cdot y$ условно выражает $\bar{x}$ с вспомогательной переменной y.

Лемма о несамодополнительной функции

Пусть $a = 1$. Тогда рассмотрим $\varphi_2(x_1, x_2) = \varphi_1(x_1, x_2) \cdot (x_1 \oplus x_2)$:

x_1	x_2	φ_1	$x_1 \oplus x_2$	φ_2
0	0	1	0	0
0	1	1	1	1
1	0	0	1	0
1	1	1	0	0

Значит, $\varphi_2(x_1, x_2) = \bar{x}_1 x_2$.

Теперь $\varphi_2(y, x) = \bar{y} \cdot x$ условно выражает x с вспомогательной переменной y.

Далее $\varphi_2(x, y) = \bar{x} \cdot y$ условно выражает $\bar{x}$ с вспомогательной переменной y.

$\square$

Лемма о самодополнительной функции

Лемма 7 (о самодополнительной функции). *Если $S = \{g\} \subseteq P_2$, где g — самодополнительная функция, $g \in T_0$, $g \neq 0$, то $x_1 \oplus x_2$ условно выразима над множеством S.*

Лемма о самодополнительной функции

Доказательство. Итак, g — самодополнительная функция, $g \in T_0$, $g \neq 0$.

Из $g \in T_0$ следует $g(0, \dots, 0) = 0$.

Из того, что g — самодополнительная функция, следует $g(1, \dots, 1) = 0$.

Т. к. $g \neq 0$, найдется такой набор $\alpha \in E_2^n$, что $g(\alpha) = 1$. Не ограничивая общности рассуждений, пусть $\alpha = (\underbrace{0, \dots, 0}_{k}, \underbrace{1, \dots, 1}_{n-k})$.

Из того, что g — самодополнительная функция, следует $g(\bar{\alpha}) = 1$.

Лемма о самодополнительной функции

Положим $\varphi(x_1, x_2) = g(\underbrace{x_1, \ldots, x_1}_{k}, \underbrace{x_2, \ldots, x_2}_{n-k})$:

x_1	x_2	φ
0	0	0
0	1	1
1	0	1
1	1	0

Значит, $\varphi(x_1, x_2) = x_1 \oplus x_2$.

$\square$

Конец лекции