§2. Подстановка и унификация в логике 1-го порядка

Давайте проанализируем доказательство какой-либо теоремы, например, теоремы о среднем арифметическом и среднем геометрическом для неотрицательных чисел.

Теорема (неформульно, но полуформально).

$$\forall a \forall b (a \in \boldsymbol{R} \,\&\, a \geq 0 \,\&\, b \in \boldsymbol{R} \,\&\, b \geq 0 \rightarrow \frac{a+b}{2} \geq \sqrt{ab}).$$

Доказательство.	Чем и как пользуемся
Пусть $a \in \boldsymbol{R}$, $a \geq 0$, $b \in \boldsymbol{R}$, $b \geq 0$.	Здесь мы пользуемся теоремой дедукции для языка 1+го порядка, которую мы еще не доказали, но придёт время – докажем. Кроме того, КНФ расписали в множество атомарных формул (частные случаи дизъюнктов).
$\exists c\ (c \in \boldsymbol{R} \,\&\, c \geq 0 \,\&\, c^2 = a)$ $\exists d\ (d \in \boldsymbol{R} \,\&\, d \geq 0 \,\&\, d^2 = b)$	Из теоремы о полноте $\boldsymbol{R}$ выводится утверждение $\forall x (x \in \boldsymbol{R} \,\&\, x \geq 0 \rightarrow \exists y\ (y \in \boldsymbol{R} \,\&\, y \geq 0 \,\&\, y^2 = x))$. Сняты кванторы. Затем вместо символа x **подставлен** символ a и вместо символа y **подставлен** символ c. И применён МР. Затем вместо символа x **подставлен** символ b и вместо символа y **подставлен** символ d. И применён МР.
$c - d \in \boldsymbol{R}$	Стандартный МР из аксиомы кольца $\boldsymbol{R}$: $a \in \boldsymbol{R} \,\&\, b \in \boldsymbol{R} \rightarrow a - b \in \boldsymbol{R}$
$(c - d)^2 \geq 0$	В теореме $\forall x (x \in \boldsymbol{R} \rightarrow x^2 \geq 0)$ снят квантор и вместо символа x **подставлен** терм $c - d$
$c^2 - 2cd + d^2 \geq 0$	Теорему $\forall x \forall y (x - y)^2 = x^2 - 2xy + y^2$ для ассоциативных коммутативных колец доказывают в 7-м классе. Затем делается **подстановка.**
$c^2 + d^2 \geq 2cd$ $\frac{c^2+d^2}{2} \geq cd$	Снова некоторые теоремы о неравенствах в $\boldsymbol{R}$ и подстановки в них подходящих термов вместо символов.
$\frac{a+b}{2} \geq \sqrt{ab}$	Подстановка и теорема $\sqrt{x}\sqrt{y} = \sqrt{xy}$

Посмотрите, сколько раз мы воспользовались применением подстановки! При этом обратите внимание – в левой части никаких слов и умственных усилий. Такое доказательство вполне доступно компьютеру, только он должен иметь базу данных из теорем и уметь делать нужные подстановки.

Формализуем то, что мы проделали.

Пусть $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ – набор различных предметных символов, $t_1, t_2, \ldots, t_n$ – набор термов, удовлетворяющих условию, что терм t_k не совпадает с x_{i_k}. Подстановкой называется отображение σ: $x_{i_k} \rightarrow t_k$ для всех k от 1 до n. В большинстве учебников подстановку σ записывают так: $\{x_{i_1}|\ t_1, x_{i_2}|\ t_2, \ldots, x_{i_n}|\ t_n\}$. Действием подстановки σ на слово w будем назвать одновременную замену в этом слове всех символов x_{i_k} на термы t_k. Результат действия постановки σ на слово w будем обозначать w^σ. Нам еще пригодится пустая подстановка, которую мы будем обозначать ε.

Возьмем теперь подстановку $\tau = \{x_{j_1}|\ s_1\ , x_{j_2}|\ s_2\ , \ldots, x_{j_n}|\ s_n\}$. Определим произведение подстановки σ на подстановку τ следующим образом:

1) Запишем $\{x_{i_1}|\ t_1^{\ \tau}\ ,\ x_{i_2}|\ t_2^{\ \tau}\ ,\ \ldots,\ x_{i_n}|\ t_n^{\ \tau},\ x_{j_1}|\ s_1\ ,\ x_{j_2}|\ s_2\ ,\ \ldots,\ x_{j_n}|\ s_n\}$.

2) Если x_{j_m} совпало с каким-то x_{i_k}, то вычеркнем $x_{j_m}|\ s_m$.

3) Если $t_k^{\ \tau}$ совпало x_{i_k}, то вычёркиваем $x_{i_k}|\ t_k^{\ \tau}$.

Произведение будем обозначать $\sigma \circ \tau$.

Пример: $\sigma = \{x_1|\ x_2,\ x_2|\ f_1^2 x_1 x_2,\ x_3|\ f_1^0\}$, $\tau = \{x_1|\ f_1^1 x_2,\ x_2|\ x_1,\ x_3|\ x_4,\ x_4|\ x_3\}$

1) $\{x_1|\ x_1,\ x_2|\ f_1^2 f_1^1 x_2 x_1,\ x_3|\ f_1^0,\ x_1|\ f_1^1 x_2,\ x_2|\ x_1,\ x_3|\ x_4,\ x_4|\ x_3\}$

2) $\{x_1|\ x_1,\ x_2|\ f_1^2 f_1^1 x_2 x_1,\ x_3|\ f_1^0,\ \sout{x_1|\ f_1^1 x_2},\ \sout{x_2|\ x_1},\ \sout{x_3|\ x_4},\ x_4|\ x_3\}$

3) $\{\sout{x_1|\ x_1},\ x_2|\ f_1^2 f_1^1 x_2 x_1,\ x_3|\ f_1^0,\ x_4|\ x_3\}$

$\sigma \circ \tau = \{x_2|\ f_1^2 f_1^1 x_2 x_1,\ x_3|\ f_1^0,\ x_4|\ x_3\}$.

Упражнение. Доказать, что $\sigma \circ \varepsilon = \varepsilon \circ \sigma = \sigma$.

Теорема. Для любого слова верно $(w^\sigma)^\tau = w^{\sigma\circ\tau}$.

Доказательство.

…

Подстановка σ называется **обобщением** подстановки τ, если существует такая подстановка ρ, для которой $\tau = \sigma \circ \rho$.

Теорема. Отношение обобщения рефлексивно и транзитивно.

Доказательство.

…

Литералом будем теперь называть атомарную формулу или её отрицание.

Унификатором множества слов w_1, w_2, … w_n называется такая подстановка σ, для которой $w_1^{\ \sigma} = w_2^{\ \sigma} = \ldots = w_n^{\ \sigma}$.

Множество слов называется **унифицируемым**, если для него существует унификатор.

Пример. Рассмотрим множества $M_1 = \{P_1^3 x_1 x_1 x_2,\ P_1^3 x_3 f_1^1 x_4 f_1^1 x_3\}$ и $M_2 = \{P_1^2 x_1 x_2,\ P_1^2 f_1^1 x_4 f_1^1 x_3\}$. Первое множество не унифицируемо, а второе очевидно унифицируемо подстановкой $\sigma = \{x_1|\ f_1^1 x_4,\ x_2|\ f_1^1 x_3\}$

Лемма. Если σ – унификатор двух литералов и $x_i|\ t \in \sigma$, то x_i не содержится в записи t.

Доказательство.Пусть w_1 и w_2 – два литерала, унифицируемые подстановкой σ. Поскольку они унифицируемы, то либо они оба начинаются с одинакового предикатного символа, либо с отрицания, стоящего пред одинаковыми предикатными символами. Это означает, что без ограничения общности можно считать $w_1 = P_n^m t_1 t_2 \ldots t_m$ и $w_2 = P_n^m s_1 s_2 \ldots s_m$, где t_1, t_2, …, t_m и s_1, s_2, …, s_m – термы. Поскольку $w_1^{\ \sigma} = w_2^{\ \sigma}$, для каждого i справедливо $t_i^{\ \sigma} = s_i^{\ \sigma}$. Если ни t_i, ни s_i не являются переменными, то каждый из них записывается как $f_l^k p_1 p_2 \ldots p_r$ и $f_l^k q_1 q_2 \ldots q_k$ соответственно, причём совпадение функционального символа не случайность, а обязательность. Для термов p_i и q_i ситуация та же, что и для t_i и s_i. В конце концов, мы придём к ситуации, когда какая-то переменная x_i из записи w_1 подстановкой σ унифицируется либо с какой-то переменной x_j из записи w_2, причём $i \neq j$ по определению подстановки, либо с каким-то термом t из записи w_2, или наоборот, какая-то переменная x_i из записи w_2 подстановкой σ унифицируется либо с какой-то переменной x_j из записи w_1, причём $i \neq j$ по определению подстановки, либо с каким-то термом t из записи w_1. Это как раз

означает, что σ содержит $x_i| t$, т.е. $t = x_i^{\sigma} = t^{\sigma}$, что возможно лишь при условии, что t не содержит в своей записи x_i.

Унификатор называется **максимально общим**, если для него нет обобщающего унификатора.

Пусть множество слов состоит из литералов и p – их наибольший общий префикс. Вычеркнем из каждого литерала этот префикс. Из каждого оставшегося слова выпишем самый короткий префикс, являющийся литералом или термом. То, что выписано, называется м**ножеством рассогласований** для данного множества литералов.

Обозначим через W конечное множество литералов.

Доказательство приведённой выше леммы делает естественным следующий алгоритм построения унификатора множества W.

Пусть n – количество элементов в множестве W.

Положить $\sigma = \varepsilon$.

Если $n = 1$, то W унифицировано и унификатором выступает σ. Алгоритм работу закончил.

Если $n > 1$, находим множество D рассогласований для W.

Пока D не пусто

Если в D есть символ x_i и терм t, который не совпадает с x_i, то $\sigma := \sigma \circ \{x_i| t\}$, после чего $W := W^{\sigma}$. Иначе W не унифицируемо, алгоритм работу закончил.

W унифицировано и унификатором выступает σ. Алгоритм работу закончил.

Теорема (об унификации). Если W унифицируемо подстановкой τ, то алгоритм унификации заканчивает работу, выдавая унификатор σ, обобщающий τ.

Доказательство. Пусть τ – некоторый унификатор. В ходе исполнения алгоритма появляется последовательность подстановок σ: $\sigma_0 = \varepsilon, \sigma_1, \ldots \sigma_k, \ldots$. Покажем индукцией по k, что существуют такие подстановки ρ_k, для которых $\tau = \sigma_k \circ \rho_k$.

Для $k = 0$ очевидно.

Ш.И. Пусть D_k – множество рассогласований для $W^{\sigma_{k-1}}$. По предположению индукции $\tau = \sigma_{k-1} \circ \rho_{k-1}$. Поскольку τ унифицирует W, это означает, что ρ_{k-1} унифицирует $W^{\sigma_{k-1}}$. Значит, ρ_{k-1} применимо к D_k. Поэтому в D_k есть некоторая переменная x_i и терм t, не совпадающий с x_i, причем $x_i| t \in \rho_{k-1}$. Можно считать, что алгоритм при построении σ_k выбирается именно эта подстановка, т.е. $\sigma_k = \sigma_{k-1} \circ \{x_i| t\}$. Положим $\rho_k = \rho_{k-1} \setminus \{x_i| t\}$. Очевидно, что $\rho_{k-1} = \{x_i| t\} \circ \rho_k$. Поэтому $\tau = \sigma_{k-1} \circ \rho_{k-1} = \sigma_{k-1} \circ \{x_i| t\} \circ \rho_k = \sigma_k \circ \rho_k$.

Фактически теорема утверждает наличие коммутативной диаграммы, где τ – произвольный унификатор множества W, а σ – унификатор, максимально обобщающий τ: