Опр. Эквивалентность конгруэнтных формул

$$Q x \Phi \equiv Q y [\Phi]^x_y$$

$$\forall x \varphi \equiv \forall y [\varphi]^x_y$$

$$\exists x \varphi \equiv \exists y [\varphi]^x_y$$

Пренексная нормальная форма:

→ все кванторы в начале
→ формула в дизъюнктивно нормальной форме

Как к ней прийти?

$$\exists x \forall y \, \varphi(x, y) \to \exists x \forall y \, \psi(x, y)$$

1. Избавление от импликации:

$$\neg(\exists x \forall y \, \varphi(x, y)) \vee \exists x \forall y \, \psi(x, y)$$

2. Переносим отрицание

$$\forall x \exists y \, (\neg \varphi(x, y)) \vee \exists x \forall y \, \psi(x, y)$$

3. Переименуем переменные справа: (связные переменные в разных формулах должны иметь разные названия, иначе возникают коллизии)

$$\forall x \exists y \, (\neg \varphi(x, y)) \vee \exists u \forall v \, \psi(u, v)$$

4. Переносим кванторы:

$$\forall x \exists y \exists u \forall v \, \underbrace{(\neg \varphi(x, y) \vee \psi(u, v))}_{ДНФ}$$

Понятие модели для множества формул

→ Структура $\mathcal{M}$ называется моделью для множества формул Γ, тогда и только тогда, когда существует такое означивание $\gamma: FV(\Gamma) \to M$, что $\mathcal{M} \models \Gamma[\gamma]$

Противоречивое множество формул

→ Множество формул Γ называется противоречивым, если $\Gamma \vdash A$ и $\Gamma \vdash \neg A$ для некоторой формулы A

В дальнейшем непротиворечивое множество формул будем обозначать как Φ.

Теорема (о полноте, Гёдель)

Пусть Φ – множество непротиворечивых формул, ψ – формула. Если $\Phi \models \psi$, то $\Phi \vdash \psi$, т.е. ψ может быть выведена из Φ.

Теорема (о достаточности/адекватности)

Пусть Φ – множество формул, ψ – формула. Тогда $\Phi \models \psi \Leftrightarrow \Phi \vdash \psi$.

Задача №1

$\boxed{\text{Предложение — формула БЕЗ свободных переменных}}$

Дано множество предложений Φ и предложение φ, определить, верно ли

$$\Phi \models \varphi$$

! Очевидно, что если рассматривать эту задачу семантически, то не существует алгоритма её решения. Но, с использованием теоремы адекватности, она может быть сведена к выводимости φ из Φ — задаче, которая может быть решена алгоритмически.

Задача №2

Дано множество предложений Φ и предложение φ, определить, верно ли

$$\Phi \vdash \varphi$$

Итак, необходимо алгоритмически определить, верно ли, что $\Phi \vdash \varphi$. Предположим, что Φ конечно

Сокращение 1

Первоначальная задача может быть переформулирована как $(n \geq 0)$:

$$\triangleright \{\varphi_1, \dots \varphi_n\} \vdash \varphi_0$$

При рассмотре конъюнкции предпосылок и вводе импликацию задача может быть сведена к вопросу о выводимости одного предложения.

Сокращение:

Первоначальная задача может быть переформулирована как:

$\triangleright \psi$

если мы введём $\psi = \bigwedge_{i=1}^{n} \phi_i \to \phi_0$

Арифметика Пеано

- 1 является натуральным числом;
- Число, следующее за натуральным, тоже является натуральным;
- 1 не следует ни за каким натуральным числом;
- Если натуральное число a непосредственно следует как за числом b так и за числом c, то b и c тождественны;

Аксиома индукции: если какое-либо предположение доказано для 1 (база индукции) и если из допущения, что оно верно для натурального числа n, вытекает, что оно верно для следующего за n натурального числа (индукционное предположение), то это предположение верно для всех натуральных чисел

Первоначальные задача была сведена к вопросу, верно ли, что $\triangleright \phi$. Но при таком подходе возникает принципиальное ограничение.

Теорема (о неполноте Геделя)

Если предложение φ достаточно сильное (а именно включает арифметику Пеано), вопрос, верно ли, что $\vartriangleright \varphi$ не разрешим, т.е. не существует алгоритма, отвечающего на этот вопрос.

Для арифметики: если формальная арифметика непротиворечива, то в ней невыводима некоторая формула, содержательно утверждающая непротиворечивость арифметики.

Обобщённо: непротиворечивость всякой аксиоматической теории не может быть доказана средствами самой этой теории

Теорема (вычислимая перечислимость)

Для любого предложения φ существует алгоритм, который либо скажет, что $\vartriangleright \varphi$, либо никогда не остановится.

Принимая во внимание вторую теорему, практический подход к автоматизированному рассуждению показывает, насколько эффективно мы можем построить упомянутый алгоритм.

Первоначальная проблема была сведена к доказуемости одной формулы φ. Но этот вопрос в свою очередь может быть сведён к вопросу о противоречивости некоторого множества.

Действительно:

Сведение к противоречивости

Для любых предложений Φ_i $\triangleright \{\Phi_1, \dots, \Phi_n\} \vdash \Phi_0$ эквивалентно утверждению о том, что множество предложений $\{\Phi_1, \dots, \Phi_n, \neg\Phi_0\}$ противоречиво.

Доказательство

Слева направо:

$$\frac{\Phi_1, \dots, \Phi_n \vdash \Phi_0}{\Phi_1, \dots, \Phi_n, \neg\Phi_0 \vdash \bot}$$

Обратное включение

$$\frac{\Phi_1, \dots, \Phi_n, \neg\Phi_0 \vdash \bot}{\Phi_1, \dots, \Phi_n \vdash \Phi_0}$$

Таким образом, вопрос о логическом следствии может быть сведён к вопросу о противоречивости.

Формула Φ называется $\forall$-формулой, тогда и только тогда, когда Φ не содержит кванторов $\exists$. Аналогично для $\exists$-формулы: Φ называется $\exists$-формулой, тогда и только тогда, когда Φ не содержит кванторов $\forall$.

Нормальная форма Сколема

Начнём с некоторой формулы $\varphi = Q_1 x_1 \dots Q_n x_n \psi$, находящейся в предваренной нормальной форме. Определим Нормальную форму Сколема (или Сколемизацию) $Sk(\varphi)$ формулы φ следующим образом.

- если φ является $\forall$-формулой, то $Sk(\varphi) = \varphi$
- в противном случае $\varphi = \forall x_1 \dots \forall x_n \exists y \psi(\bar{x}, y)$ и для некоторого нового n-местного функционального символа f возьмём

$$Sk(\varphi) = Sk(\forall x_1 \dots \forall x_n \psi(\bar{x}, f(\bar{x})))$$

Пример:

$$Sk(\forall x \exists y \forall z (p(x,y) \to q(f(y), z) \wedge$$
$$\wedge\, y = h(z))) = \forall x \forall z (p(x, g(x)) \to$$
$$\to q(f(g(x)), z) \wedge g(x) = h(z))$$

Нормальная форма Эрбрана

Начнём с некоторой формулы $\varphi = Q_1 x_1 \dots Q_n x_n \psi$, находящейся в предваренной нормальной форме. Определим Нормальную форму Эрбрана (или Эрбранизацию $Hb(\varphi)$ формулы φ следующим образом)

- если φ является $\exists$-формулой, то $Hb(\varphi) = \varphi$
- в противном случае $\varphi = \exists x_1 \dots \exists x_n \forall y \psi(\bar{x}, y)$

и для некоторого нового n-местного функционального символа f возьмём

$$Hb(\varphi) = Hb(\exists x_1 \ldots \exists x_n \psi(\bar{x}, f(\bar{x})))$$

Литерал — это атомарная формула или её отрицание.

Определение (Хорновский дизъюнкт)

Хорновский дизъюнкт — это дизъюнкция литералов, т.е. это элементарная дизъюнкция. Существует специальный Хорновский дизъюнкт — пустой дизъюнкт, обозначаемый как $\square$ и означающий ложную формулу $\bot$.

Примеры:

- $p(x, f(y)) \vee \neg q(x, x) \vee p(h(x, y), h(y, f(x)))$
- $p(x, f(y), z) \vee q(x) \vee p(h(x, y, z), h(y, f(x), x)) \vee \neg q(f(y))$
- $\neg p(f(f(f(x)))) \vee p(x)$

Соглашение. Поскольку Хорновские дизъюнкты — это просто дизъюнкции, далее будем считать, что Хорновский дизъюнкт — это множество всех литералов, входящих в его состав:

$$h = l_1 \vee \ldots \vee l_k = \{l_1, \ldots, l_k\}$$

! Метод резолюций основан на правиле резолюции

Правило резолюции: из дизъюнктов $(x \vee F)$ и $(\neg x \vee G)$ выводим дизъюнкт $(F \vee G)$. Или, другими словами, дизъюнкт $(F \vee G)$ является логическим следствием дизъюнктов $(x \vee F)$ и $(\neg x \vee G)$.

Пример: Каждого, кто любит всех животных, кто-то любит. Любого, кто убивает животных, никто не любит. Джек любит всех животных. Кота по имени Тунец убил либо Джек, либо Любопытство. Действительно ли этого кота убило Любопытство?

A_1: $\forall x\,(\forall y$ Животное$(y) \Rightarrow$ Любит$(x, y)) \Rightarrow$
$\Rightarrow (\exists z$ Любит$(z, x))$

A_2: $\forall x\,(\exists y$ Животное$(y) \wedge$ Убил$(x, y)) \Rightarrow$
$\Rightarrow (\forall z \neg$ Любит$(z, x))$

A_3: $\forall y$ Животное$(y) \Rightarrow$ Любит(Джек, y)

A_4: Кот(Тунец) $\wedge$ (Убил(Джек, Тунец) $\vee$
$\vee$ Убил(Любопытство, Тунец))

A_5: $\forall x$ Кот$(x) \Rightarrow$ Животное(x)

B: Убил(Любопытство, Тунец)

Доказываем невыполнимость формулы:

$(\forall x (\forall y$ Животное$(y) \Rightarrow$ Любит$(x, y)) \Rightarrow$
$\Rightarrow (\exists z$ Любит$(z, x))) \wedge$

$\wedge (\forall x (\exists y$ Животное$(y) \wedge$ Убил$(x, y)) \Rightarrow (\forall z \neg$ Любит$(z, x))) \wedge$

$\wedge (\forall y$ Животное$(y) \Rightarrow$ Любит$($Джек$, y)) \wedge$

$\wedge ($Кот$($Тунец$) \wedge ($Убил$($Джек$,$ Тунец$) \vee$ Убил$($Любопытство$,$ Тунец$))) \wedge$

$\wedge (\forall x$ Кот$(x) \Rightarrow$ Животное$(x)) \wedge$

$\wedge \neg$ Убил$($Любопытство$,$ Тунец$)$

$(\forall x_1 \neg (\forall y_1 \neg$ Животное$(y_1) \vee$ Любит$(x_1, y_1)) \vee (\exists z_1$ Любит$(z_1, x_1))) \wedge$

$\wedge (\forall x_2 \neg (\exists y_2$ Животное$(y_2) \wedge$ Убил$(x_2, y_2)) \vee$
$\vee (\forall z_2 \neg$ Любит$(z_2, x_2))) \wedge$

$\wedge (\forall y_3 \neg$ Животное$(y_3) \vee$ Любит$($Джек$, y_3)) \wedge$

$\wedge ($Кот$($Тунец$) \wedge ($Убил$($Джек$,$ Тунец$) \vee$ Убил$($Любопытство$,$ Тунец$))) \wedge$

$\wedge (\forall x_4 \neg$ Кот$(x_4) \vee$ Животное$(x_4)) \wedge$

$\wedge \neg$ Убил$($Любопытство$,$ Тунец$)$

$(\forall x_1 (\exists y_1\ \text{Животное}(y_1) \wedge \neg\text{Любит}(x_1, y_1)) \vee$

$\vee (\exists z_1\ \text{Любит}(z_1, x_1))) \wedge$

$\wedge (\forall x_2 (\forall y_2\ \neg\text{Животное}(y_2) \wedge \neg\text{Убил}(x_2, y_2)) \vee$

$\vee \forall z_2\ \neg\text{Любит}(z_2, x_2))) \wedge$

$\wedge (\forall y_3\ \neg\text{Животное}(y_3) \vee \text{Любит}(\text{Джек}, y_3)) \wedge$

$\wedge (\text{Кот}(\text{Тунец}) \wedge \text{Убил}(\text{Джек}, \text{Тунец}) \vee$

$\vee \text{Убил}(\text{Любопытство}, \text{Тунец})) \wedge$

$\wedge (\forall x_4\ \neg\text{Кот}(x_4) \vee \text{Животное}(x_4)) \wedge$

$\wedge \neg\text{Убил}(\text{Любопытство}, \text{Тунец})$

$((\text{Животное}(f(x_1)) \wedge \neg\text{Любит}(x_1, f(x_1))) \vee$

$\vee \text{Любит}(g(x_1), x_1)) \wedge$

$\wedge (\neg\text{Животное}(y_2) \vee \neg\text{Убил}(x_2, y_2) \vee \neg\text{Любит}(z_2, x_2)) \wedge$

$\wedge (\neg\text{Животное}(y_3) \vee \text{Любит}(\text{Джек}, y_3)) \wedge$

$\wedge \text{Кот}(\text{Тунец}) \wedge (\text{Убил}(\text{Джек}, \text{Тунец}) \vee \text{Убил}(\text{Любопытство}, \text{Тунец})) \wedge$

$\wedge (\neg\text{Кот}(x_4) \vee \text{Животное}(x_4)) \wedge$

$\wedge \neg\text{Убил}(\text{Любопытство}, \text{Тунец})$

После завершение перевода в сколемовскую конъюнктивную нормальную форму получаем предложение:

C_1: $\text{Животное}(f(x)) \vee \text{Любит}(g(x), x)$

C_2: $\neg\text{Любит}(x, f(x)) \vee \text{Любит}(g(x), x)$

C_3: ¬Животное (y) ∨ Любит (Джек, y)

C_4: ¬Животное (y) ∨ Любит (Джек, y)

C_5: Кот (Тунец)

C_6: Убил (Джек, Тунец) ∨ Убил (Любопытство, Тунец)

C_7: ¬Кот (x) ∨ Животное (x)

C_8: ¬Убил (Любопытство, Тунец)

— — — — — — — — — —

C_9: Животное (Тунец) → резольвента C_5 и C_7 ←

C_{10}: ¬Убил (x, Тунец) ∨ ¬Любит (z, x) → рез. C_3 и C_9 ←

C_{11}: Убил (Джек, Тунец) → рез. C_6 и C_8 ←

C_{12}: ¬Любит (z, Джек) → рез. C_{10} и C_{11} ←

C_{13}: ¬Животное (f (Джек)) ∨ Любит (g (Джек), Джек)
→ рез. C_2 и C_4 ←

C_{14}: Любит (g (Джек), Джек) → рез. C_1 и C_{13} ←

C_{15}: $\bot$ → рез. C_{12} и C_{14} ←

→ противоречие ⇒ кота не могло не убить Любопытство

⇒ Кота убило Любопытство

swap

$\{x := x+y;$ | $x \quad y$
$y := x-y;$ | $x+y \quad y$
$x := x-y\}$ | $x+y \quad x$
| $y \quad x$

$\{x = a \wedge y = b\}$ swap $\{x = b \wedge y = a\}$

$\{x = a \wedge y = b\}\ x := x+y\ \{x - y = a \wedge y = b\}$

$\{x - y = a \wedge y = b\}\ y := x-y\ \{y = a \wedge x = b\}$

$\{(\varphi)^x_e\}\ x := e\ \{\varphi\}$

I $\quad \dfrac{\{\varphi\}\pi\{\chi\} \quad \{\chi\}\sigma\{\psi\}}{\{\varphi\}\pi;\sigma\{\psi\}}$

II $\quad \dfrac{\{\varphi \wedge \chi\}\pi\{\psi\} \quad \{\varphi \wedge \neg\chi\}\sigma\{\psi\}}{\{\varphi\}\ \text{if } \chi \text{ then: } \pi \text{ else } \sigma\{\psi\}}$

III $\quad \dfrac{\{\varphi \wedge \chi\}\ \pi\ \{\varphi\}}{\{\varphi\}\ \text{while } \chi \text{ do } \pi\{\varphi \wedge \neg\chi\}}$

$\dfrac{\varphi \to \varphi' \quad \{\varphi'\}\pi\{\psi'\} \quad \psi' \to \psi}{\{\varphi\}\ \pi\ \{\psi\}}$

2. Написать тройки Хоара

a) $\left[\frac{n}{m}\right]$, $n, m \in \mathbb{N}$ x / y

$c = 0$
while $(n \geq m)$ do
$n := n - m$
$c := c + 1$

$\{n \geq 0 \wedge m > 0\}$ div $\{(c > 0 \wedge m(c-1) \leq n < m \cdot c) \vee$

$\vee (c = 0 \wedge n < m)\}$

$(n \geq 0 \wedge m > 0)$

$\{n \geq 0 \wedge m > 0\}$ div $\{ \wedge m \cdot (c-1) < n \wedge n \leq m \cdot c\}$

$\{(n \geq 0 \wedge m > 0) \wedge (m(c-1) \geq n \vee (n > mc))\}$
$n := n - m$, $c := c + 1$ $\{n \geq 0 \wedge m > 0 \wedge m \cdot (c-2) \geq$
$(n+m) \vee ((n+m) > m \cdot (c-1))\}$

---

b) $\gcd(n, m)$, $n, m \in \mathbb{N}$

while $(n \neq m)$ do (if $n \geq m$ then $n = n - m$ else $m = m - n$)

10	25
10	15
10	5
5	5

$x / y = \exists t\, (xt = y)$
$\gcd(x, y, z) = z / x \,\&\, z / y \,\&\, \forall u\, (u / x \,\&\, u / y \to u / z)$
$\underbrace{\{n \geq 0 \,\&\, m \geq 0 \,\&\, \gcd(n, m, k)\}}_{\varphi}$ R $\{n = k\}$

$\to \varphi(m, n, k) \wedge m = n$

$\varphi(n+m, m, k) \sim \varphi(n, m, k)$

$\{\varphi(n, m, k) \wedge n \geq m\}$ $n := n - m$ $\{ \wedge n + m \geq m\}$

$\{\varphi(n, m, k) \wedge n < m\}$ $m := m - n$ $\{\varphi(n, n+m, k) \wedge n < n + m\}$

$\sim \varphi(n, m, k)$

$\{\varphi\}$ if $n \geq m$ then $n = n - m$ else $m = m - n$ $\{\varphi\}$

$\{\varphi \wedge n \neq m\}$ if $n \geq m$ then $n = n - m$ else $m = m - n$ $\{\varphi\}$

$\varphi \wedge (n \neq m) \to \varphi$