

ТЕОРЕТИЧЕСКИЕ («МАЛЫЕ») ДОМАШНИЕ ЗАДАНИЯ

Математическая логика, ИТМО, М3235-М3239, весна 2020 года

Домашнее задание №1: «знакомство с исчислением высказываний»

1. Укажите про каждое из следующих высказываний, общезначимо, выполнимо, опровержимо или невыполнимо ли оно:

- (a) $\neg A \vee \neg \neg A$
- (b) $(A \rightarrow \neg B) \vee (B \rightarrow \neg C) \vee (C \rightarrow \neg A)$
- (c) $A \rightarrow B \vee A$
- (d) $A \rightarrow B \& B \rightarrow A$
- (e) $A \rightarrow B \rightarrow \neg B \rightarrow \neg A$.

2. Будем говорить, что высказывание α *следует* из высказываний $\gamma_1, \gamma_2, \dots, \gamma_n$ (и будем записывать это как $\gamma_1, \gamma_2, \dots, \gamma_n \models \alpha$), если при любой оценке, такой, что при всех i выполнено $\llbracket \gamma_i \rrbracket = \text{И}$, также выполнено и $\llbracket \alpha \rrbracket = \text{И}$.

Пусть даны высказывания α и β , причём $\alpha \models \beta$, но $\beta \not\models \alpha$. Придумайте «промежуточное» высказывание γ , такое, что $\alpha \models \gamma$, $\gamma \models \beta$, причём $\gamma \not\models \alpha$ и $\beta \not\models \gamma$.

3. Простые высказывания. Докажите высказывания, построив полный вывод:

- (a) $\alpha, \beta \vdash \alpha \& \beta$
- (b) $\alpha, \beta \vdash \alpha \vee \beta$
- (c) $\neg \alpha, \beta \vdash \alpha \vee \beta$
- (d) $\alpha, \neg \beta \vdash \alpha \vee \beta$
- (e) $\gamma \vdash \alpha \rightarrow \gamma$
- (f) $\neg \alpha \vdash \neg \alpha$
- (g) $\alpha, \beta \vdash \alpha \rightarrow \beta$

4. Ассоциативность и коммутативность.

- (a) Докажите или опровергните: $\models \alpha \rightarrow \beta$ влечёт $\models \beta \rightarrow \alpha$.
- (b) Докажите: $\vdash \alpha \vee \beta \rightarrow \beta \vee \alpha$
- (c) Докажите: $\vdash \alpha \& \beta \rightarrow \beta \& \alpha$

5. Контрапозиция. $\vdash (\alpha \rightarrow \beta) \rightarrow \neg \beta \rightarrow \neg \alpha$.

6. Докажите следующие высказывания, построив полный вывод:

- (a) $\neg \alpha, \beta \vdash \neg(\alpha \& \beta)$
- (b) $\alpha, \neg \beta \vdash \neg(\alpha \& \beta)$
- (c) $\neg \alpha, \neg \beta \vdash \neg(\alpha \& \beta)$
- (d) $\neg \alpha, \neg \beta \vdash \neg(\alpha \vee \beta)$
- (e) $\alpha, \neg \beta \vdash \neg(\alpha \rightarrow \beta)$
- (f) $\neg \alpha, \beta \vdash \alpha \rightarrow \beta$
- (g) $\neg \alpha, \neg \beta \vdash \alpha \rightarrow \beta$
- (h) $\alpha \vdash \neg \neg \alpha$

Домашнее задание №2: «интуиционистское исчисление высказываний»

1. Долги по теореме о полноте ИВ. Докажите:

- (a) $\vdash \alpha \vee \neg \alpha$
- (b) $\Gamma, \alpha \vdash \phi$ и $\Gamma, \neg \alpha \vdash \phi$ влечёт $\Gamma \vdash \phi$

2. Постройте дерево вывода для следующих высказываний интуиционистской логики (в данных примерах $\neg \alpha$ — сокращение для $\alpha \rightarrow \perp$):

- (a) $\vdash \alpha \rightarrow \alpha$
- (b) $\alpha \rightarrow \beta \vdash \neg \beta \rightarrow \neg \alpha$
- (c) $\vdash \alpha \vee \beta \rightarrow \beta \vee \alpha$
- (d) $\vdash \alpha \& \beta \rightarrow \beta \& \alpha$
- (e) $\vdash \neg(\alpha \vee \neg \alpha)$

3. Постройте примеры частично упорядоченных множеств:

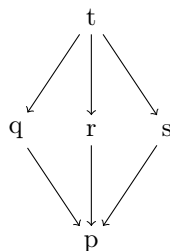
- (a) определено $a + b$, но не $a \cdot b$;
- (b) определено $a \cdot b$, но не $a + b$;
- (c) является решёткой, но не является дистрибутивной решёткой;
- (d) является дистрибутивной, но не импликативной решёткой;
- (e) является импликативной, но не имеет нуля;

4. Решётки. Покажите, что следующие утверждения выполнены в любой решётке и при любых a, b и c :

- (a) Коммутативность: $a \cdot b = b \cdot a$ и $a + b = b + a$
- (b) Ассоциативность: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ и $a + (b + c) = (a + b) + c$
- (c) Законы поглощения: $a \cdot (a + b) = a$ и $a + (a \cdot b) = a$
- (d) Верно ли, что если $a \sqsubseteq b$, то $a + c \sqsubseteq b + c$ и $a \cdot c \sqsubseteq b \cdot c$?
- (e) Верно ли, что если $a + c \sqsubseteq b + c$ или $a \cdot c \sqsubseteq b \cdot c$, то $a \sqsubseteq b$?

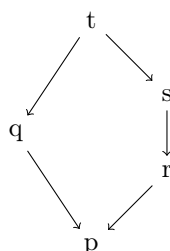
5. В любой дистрибутивной решётке

- (a) $(a \cdot b) + c = (a + c) \cdot (b + c)$.
- (b) Нет *алмазов*: таких пяти элементов p, q, r, s, t , что $p \sqsubseteq q, r, s \sqsubseteq t$, и при этом q, r и s — несравнимы.



При этом, если на данной диаграмме выполнено какое-то вычисление (например, $q + r = t$), то оно должно быть выполнено и в исходной дистрибутивной решётке.

- (c) Нет *пентагонов*: таких пяти элементов p, q, r, s, t , что $p \sqsubseteq q, r, s \sqsubseteq t$, также $r \sqsubseteq s$, элемент же q не сравним с r и s .



При этом, если на данной диаграмме выполнено какое-то вычисление (например, $q + r = t$), то оно должно быть выполнено и в исходной дистрибутивной решётке.

6. Покажите, что в импликативной решётке
 - (a) выполнена дистрибутивность;
 - (b) Из $a \sqsubseteq b$ следует $b \rightarrow c \sqsubseteq a \rightarrow c$ и $c \rightarrow a \sqsubseteq c \rightarrow b$;
 - (c) Из $a \sqsubseteq b \rightarrow c$ следует $a \cdot b \sqsubseteq c$;
 - (d) $a \sqsubseteq b$ выполнено тогда и только тогда, когда $a \rightarrow b = 1$;
 - (e) $b \sqsubseteq a \rightarrow b$;
 - (f) $a \rightarrow b \sqsubseteq ((a \rightarrow (b \rightarrow c)) \rightarrow (a \rightarrow c))$;
 - (g) $a \sqsubseteq b \rightarrow a \cdot b$;
 - (h) $a \rightarrow c \sqsubseteq (b \rightarrow c) \rightarrow (a + b \rightarrow c)$
7. Рассмотрим топологию $\langle X, \Omega \rangle$ (напомним, что здесь Ω — множество всех открытых подмножеств множества X). Рассмотрим множество Ω , частично упорядоченное отношением «быть подмножеством». Покажите, что получившаяся конструкция:
 - (a) решётка;
 - (b) дистрибутивная решётка;
 - (c) импликативная решётка;
 - (d) псевдобулева алгебра;
 - (e) не является булевой алгеброй.
8. Покажите, что булева алгебра — булева алгебра.
9. Покажите, что подмножества некоторого множества, упорядоченные отношением «быть подмножеством» — булева алгебра.
10. Покажите недоказуемость следующих высказываний интуиционистской логики, построив *конечные* псевдобулевы алгебры (т.е. частично упорядоченные множества с конечным количеством элементов), в которых следующие высказывания не истинны:
 - (a) $A \vee \neg A$
 - (b) $((A \rightarrow B) \rightarrow A) \rightarrow A$
 - (c) $(A \rightarrow (B \vee \neg B)) \vee (\neg A \rightarrow (B \vee \neg B))$
 - (d) $\neg A \vee \neg \neg A$
11. Теорема о полноте алгебр Гейтинга как моделей для интуиционистского исчисления высказываний. Уточним определения, данные на лекции:
 - (a) Будем писать $\alpha \sqsubseteq \beta$, если $\alpha \vdash \beta$.
 - (b) Будем писать $\alpha \approx \beta$, если имеет место $\alpha \sqsubseteq \beta$ и $\beta \sqsubseteq \alpha$.
 - (c) Будем писать $[\alpha]$ для класса эквивалентности, порождённого по формуле α : $[\alpha] = \{\phi \mid \phi \approx \alpha\}$

Интуиция здесь такая: высказывание тем ближе к 0 (к лжи), чем меньше ситуаций, в которых оно истинно. Поэтому если $\alpha \vdash \beta$, то α не больше β : возможно, β истинно ещё в каких-то ситуациях, в которых ложно α (но не наоборот).

Тогда докажите следующие утверждения:

 - (a) (\approx) есть действительно отношение эквивалентности.
 - (b) $[\alpha \& \beta]$ — наибольшая нижняя грань $[\alpha]$ и $[\beta]$ в алгебре Линденбаума. То есть, $\alpha \& \beta \sqsubseteq \alpha$, $\alpha \& \beta \sqsubseteq \beta$, и из $\tau \sqsubseteq \alpha$ и $\tau \sqsubseteq \beta$ следует $\tau \sqsubseteq \alpha \& \beta$. Также поясните, почему нам достаточно доказать эти утверждения для отдельных представителей, чтобы доказать свойства для классов эквивалентности.
 - (c) $[\alpha \vee \beta]$ — наименьшая верхняя грань $[\alpha]$ и $[\beta]$.
 - (d) $[\alpha \rightarrow \beta]$ — псевдодополнение $[\alpha] \rightarrow [\beta]$.
 - (e) $[\perp]$ — ноль.
 - (f) $[\neg \alpha]$ — псевдодополнение до нуля $\sim [\alpha]$.

Домашнее задание №3: «корректность и дизъюнктивность интуиционистского исчисления высказываний»

1. Теорема о корректности: если $\vdash \alpha$, то $\models \alpha$ в любой алгебре Гейтинга. Поскольку в принятом нами интуиционистском исчислении высказываний доказываются не высказывания, а некоторые сложные условные выражения (записи вида $\Gamma \vdash \alpha$), то и оценкой для данных выражений мы выберем неравенство. А именно, если $\Gamma = \{\gamma_1, \dots, \gamma_n\}$, $g_i = \llbracket \gamma_i \rrbracket$ и $a = \llbracket \alpha \rrbracket$, то выражению $\Gamma \vdash \alpha$ мы сопоставим неравенство

$$g_1 \cdot g_2 \cdot \dots \cdot g_n \sqsubseteq a$$

и записывать его будем как $\Gamma \sqsubseteq a$. Также, на случай $G = \emptyset$ положим, что $\emptyset \sqsubseteq a$ означает $a = 1$ (это естественно предположить, поскольку к любому G всегда можно добавить некоторое $g_0 = 1$, при этом смысл выражения $g_0 \cdot g_1 \cdot g_2 \cdot \dots \cdot g_n \sqsubseteq a$ останется прежним).

Отметим, что следующие утверждения очевидны (или уже показаны ранее):

- *Аксиома.* $G, a \sqsubseteq a$.
- *Введение ($\&$).* Если $G \sqsubseteq b$ и $G \sqsubseteq c$, то $G \sqsubseteq b \cdot c$.
- *Удаление ($\&$).* Если $G \sqsubseteq a \cdot b$, то $G \sqsubseteq a$ и $G \sqsubseteq b$.
- *Введение (\vee).* Если $G \sqsubseteq b$, то $G \sqsubseteq b + c$ и $G \sqsubseteq c + b$.

Теперь осталось заполнить промежутки и получить полноценное доказательство. А именно, покажите, что:

- (a) *Введение (\rightarrow).* Если $G, a \sqsubseteq b$, то $G \sqsubseteq a \rightarrow b$. Убедитесь, что если $a \sqsubseteq b$, то $\emptyset \sqsubseteq a \rightarrow b$.
- (b) *Удаление (\rightarrow).* Если $G \sqsubseteq a \rightarrow b$ и $G \sqsubseteq a$, то $G \sqsubseteq b$.
- (c) *Удаление (\vee).* Если $G, a \sqsubseteq c$, $G, b \sqsubseteq c$ и $G \sqsubseteq a + b$, то $G \sqsubseteq c$.
- (d) *Удаление лжи.* Если $G \sqsubseteq 0$, то $G \sqsubseteq b$ при любом b .
- (e) Основываясь на доказанных выше утверждениях, покажите теорему о корректности в целом.
2. Поясните, как соотносится $G \sqsubseteq a$ со следующими системой (подзадача а) и совокупностью (подзадача б) неравенств:

$$(a) \quad \left\{ \begin{array}{l} g_1 \sqsubseteq a \\ g_2 \sqsubseteq a \\ \dots \\ g_n \sqsubseteq a \end{array} \right. \quad (b) \quad \left[\begin{array}{l} g_1 \sqsubseteq a \\ g_2 \sqsubseteq a \\ \dots \\ g_n \sqsubseteq a \end{array} \right.$$

То есть, следует ли какое-нибудь утверждение из какого-нибудь другого, и если да, то докажите, если нет — предложите контрпример.

3. Покажите, что $\Gamma(\mathcal{A})$ — алгебра Гейтинга, если \mathcal{A} — алгебра Гейтинга.
4. Покажите или опровергните, что если $\Gamma(\mathcal{B})$ — алгебра Гейтинга, то и \mathcal{B} — алгебра Гейтинга.
5. Покажите, что отображение $\varphi : \Gamma(\mathcal{A}) \rightarrow \mathcal{A}$, определённое как:

$$\varphi(g) = \begin{cases} g, & \text{если } g \sqsubset \omega \\ 1_{\mathcal{A}}, & \text{если } g = \omega \text{ или } g = 1_{\Gamma(\mathcal{A})} \end{cases}$$

действительно является гомоморфизмом.

6. Является ли требование на сохранение нуля в определении гомоморфизма алгебр Гейтинга обязательным?

Если точнее, пусть $\varphi : \mathcal{A} \rightarrow \mathcal{B}$ — отображение алгебр Гейтинга, сохраняющее операции: $\varphi(a \star b) = \varphi(a) \star \varphi(b)$ и $\varphi(\neg a) = \neg \varphi(a)$. Всегда ли $\varphi(0_{\mathcal{A}}) = 0_{\mathcal{B}}$ и φ — гомоморфизм.

7. Покажем, что если α доказано в интуиционистском исчислении высказываний в стиле Гильберта (с изменённой 10 аксиомой: $\alpha \rightarrow \neg \alpha \rightarrow \beta$), то оно может быть доказано и в интуиционистской.

Для этого покажите, что:

- (a) Все аксиомы 1-9 выполнены (подзадачи а.1 — а.9): если α — аксиома, то $\vdash_{\text{и}} \alpha$.
- (b) $\vdash_{\text{и}} \alpha \rightarrow \neg \alpha \rightarrow \beta$.
- (c) Покажите правило Modus Ponens: если $\vdash_{\text{и}} \alpha$ и $\vdash_{\text{и}} \alpha \rightarrow \beta$, то $\vdash_{\text{и}} \beta$.
- 8. Как доказать, что если $\vdash_{\text{и}} \alpha$, то $\vdash_{\text{к}} \alpha$? Придумайте схему доказательства, для доказательства отдельных утверждений можно пользоваться теоремой о полноте К.И.В.
- 9. Как доказать, что если $\vdash_{\text{и}} \alpha$, то $\vdash \alpha$ в интуиционистском исчислении высказываний в стиле Гильберта? Придумайте схему доказательства.
- 10. Покажем теорему Гливленко. Для этого покажем следующее:
 - (a) Если $\vdash_{\text{и}} \alpha$, то $\vdash_{\text{и}} \neg \neg \alpha$.
 - (b) $\vdash_{\text{и}} \neg \neg (\neg \neg \alpha \rightarrow \alpha)$.
 - (c) Вспользовавшись предыдущими пунктами и задачами, докажите теорему Гливленко.

Домашнее задание №4: «Исчисление предикатов»

1. Докажите следующие формулы в исчислении предикатов:
 - (a) $\forall x. \phi \rightarrow \phi$
 - (b) $(\forall x. \phi) \rightarrow (\exists x. \phi)$
 - (c) $(\forall x. \forall y. \phi) \rightarrow (\forall x. \phi)$
 - (d) $(\forall x. \phi) \rightarrow (\neg \exists x. \neg \phi)$
 - (e) $(\exists x. \phi) \rightarrow (\neg \forall x. \neg \phi)$
 - (f) $(\forall x. \neg \phi) \rightarrow (\neg \exists x. \phi)$
 - (g) $(\exists x. \neg \phi) \rightarrow (\neg \forall x. \phi)$
2. Опровергните формулы $\phi \rightarrow \forall x. \phi$ и $(\exists x. \phi) \rightarrow (\forall x. \phi)$
3. Все правила и аксиомы с кванторами имеют дополнительные ограничения на свободу переменных (свободу для подстановки). Для каждого из правил и каждой из аксиом найдите по примеру, когда эти ограничения существенны (они запрещают доказательства, выводящие опровержимые формулы).
4. Рассмотрим формулу α с двумя свободными переменными x и y (мы предполагаем, что эти метаварьиные соответствуют разным переменным). Определите, какие из сочетаний кванторов выводятся из каких — и приведите соответствующие доказательства или опровержения:
 - (a) $\forall x. \forall y. \alpha, \forall y. \forall x. \alpha$
 - (b) $\exists x. \exists y. \alpha, \exists y. \exists x. \alpha$
 - (c) $\forall x. \forall y. \alpha, \forall x. \exists y. \alpha, \exists x. \forall y. \alpha, \exists x. \exists y. \alpha$
 - (d) $\forall x. \exists y. \alpha, \exists y. \forall x. \alpha$
5. Научимся выносить квантор всеобщности «наружу»:
 - (a) Покажите, что если x не входит свободно в α , то

$$\vdash (\alpha \vee \forall x. \beta) \rightarrow (\forall x. \alpha \vee \beta) \quad \text{и} \quad \vdash ((\forall x. \beta) \vee \alpha) \rightarrow (\forall x. \beta \vee \alpha)$$
 - (b) Покажите, что

$$\vdash ((\forall x. \alpha) \vee (\forall y. \beta)) \rightarrow \forall p. \forall q. \alpha[x := p] \vee \beta[y := q]$$
 где p и q — свежие переменные, не входящие в формулу. Заметим, что в частном случае x может совпадать с y .
 - (c) Докажите аналогичные утверждения для $\&$.
 - (d) Как будут сформулированы аналогичные утверждения для \rightarrow и \neg ? Сформулируйте и докажите их.
6. Научимся вносить квантор всеобщности «внутрь»:

(а) Покажите, что если x не входит свободно в α , то

$$\vdash (\forall x.\alpha \vee \beta) \rightarrow (\alpha \vee \forall x.\beta) \quad \text{и} \quad \vdash (\forall x.\beta \vee \alpha) \rightarrow ((\forall x.\beta) \vee \alpha)$$

(б) Покажите, что если p не входит свободно в β и q не входит свободно в α , то

$$\vdash (\forall p.\forall q.\alpha \vee \beta) \rightarrow (\forall x.\alpha[p := x]) \vee (\forall y.\beta[q := y])$$

при условии, что x свободно для подстановки вместо p в α и y свободно для подстановки вместо q в β .

(с) Докажите аналогичные утверждения для $\&$.

(д) Как будут сформулированы аналогичные утверждения для \rightarrow и \neg ? Сформулируйте и докажите их.

7. Сформулируйте и докажите аналогичные предыдущим пунктам утверждения для квантора существования.

8. Научимся работать со спрятанными глубоко кванторами. Пусть $\vdash \alpha \rightarrow \beta$, тогда:

(а) Докажите:

$$\vdash \psi \vee \alpha \rightarrow \psi \vee \beta \quad \vdash \psi \& \alpha \rightarrow \psi \& \beta \quad \vdash (\psi \rightarrow \alpha) \rightarrow (\psi \rightarrow \beta) \quad \vdash (\beta \rightarrow \psi) \rightarrow (\alpha \rightarrow \psi)$$

(б) Сформулируйте и докажите аналогичное свойство для отрицания.

(с) Докажите $\vdash (\forall x.\alpha) \rightarrow (\forall x.\beta)$. Надо ли наложить на формулы α и β какие-либо ограничения?

(д) Докажите $\vdash (\exists x.\alpha) \rightarrow (\exists x.\beta)$. Надо ли наложить на формулы α и β какие-либо ограничения?

9. Формулой исчисления предикатов с *поверхностными* кванторами (формулой в предварённой форме) назовём формулу, соответствующую нетерминалу ψ в грамматике

$$\psi ::= \forall x.\psi \mid \exists x.\psi \mid \sigma$$

где σ — это формула, не содержащая кванторов. Иными словами, это формула, в которой все кванторы снаружи — квантор не может быть указан внутри конъюнкции, дизъюнкции, импликации или отрицания.

Опираясь на доказанные выше леммы, докажите, что если α — формула, то для неё найдётся такая формула β с поверхностными кванторами, что:

(а) $\vdash \alpha \rightarrow \beta$

(б) $\vdash \beta \rightarrow \alpha$

Домашнее задание №5: арифметика

1. Докажите следующие утверждения в Аксиоматике Пеано:

(а) $a + (b + c) = (a + b) + c$

(б) $a \cdot b = b \cdot a$

(с) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(д) $a \cdot (b + c) = a \cdot b + a \cdot c$

2. Будем считать, что $a \leq b$ если либо $a = 0$, либо $p \leq q$ при $p' = a$ и $q' = b$.

(а) Покажите, что если $a \leq b$, то $a + c \leq b + c$.

(б) Покажите, что если $a \leq b$ и $c \leq d$, то $a \cdot c \leq b \cdot d$.

(с) Покажите, что при любых a и b выполнено $a \leq b$ или $b \leq a$.

(д) Покажите, что если $a \leq b$ и $b \leq a$, то $a = b$.

3. Докажите следующие утверждения в формальной арифметике:

(а) $\vdash 0 + a = a + 0$

$$(b) \vdash a = b \rightarrow a + 0' = b + 0'$$

$$(c) \vdash a = b \rightarrow a + c = b + c$$

4. Определим новое обозначение: будем писать $x \leq y$ вместо $\exists a. x + a = y$ (и воспринимать это новое обозначение как своего рода макроподстановку). Также, введём обозначение для записи натуральных чисел в формальной арифметике:

$$\bar{n} = \begin{cases} 0, & n = 0 \\ (\overline{n-1})', & n > 0 \end{cases}$$

Естественно, данные обозначения целиком принадлежат мета-языку. Покажите в формальной арифметике следующие утверждения:

$$(a) \vdash a = b \rightarrow a \leq b$$

$$(b) \vdash a \leq b \rightarrow a' \leq b'$$

$$(c) \vdash a \leq b \rightarrow \forall c. a + c \leq b + c$$

$$(d) \vdash a \leq b \vee b \leq a$$

$$(e) \text{ Обозначим за } \phi_n(x) \text{ формулу } x = 0 \vee x = 0' \vee x = 0'' \vee \dots \vee x = \bar{n}. \text{ Покажите тогда, что при любом натуральном } n \text{ выполнено } \vdash a \leq \bar{n} \rightarrow \phi_n(a)$$

$$(f) \text{ При любом натуральном } n \text{ выполнено } \vdash \phi_n(a) \rightarrow a \leq \bar{n}$$

Домашнее задание №6: выразимость и представимость в арифметике

Введем обозначение. Если в тексте вводится некоторая формула $\alpha(x_1, \dots, x_n)$, то по умолчанию считается, что эта формула имеет n свободных переменных с именами x_1, \dots, x_n

Внутри же выражения запись $\alpha(y_1, \dots, y_n)$ мы будем трактовать, как $\alpha[x_1 := y_1, \dots, x_n := y_n]$, при этом мы подразумеваем, что y_1, \dots, y_n свободны для подстановки вместо x_1, \dots, x_n в α .

Также, запись $B(x_1, \dots, x_n) \equiv \alpha(x_1, \dots, x_n)$ будет означать, что мы определяем новую формулу с именем B и n свободными переменными x_1, \dots, x_n . Данная формула должна восприниматься только как сокращение записи, макроподстановка.

Определение 1. Отношение R называется *выразимым* (в формальной арифметике), если существует такая формула $\alpha(x_1, \dots, x_n)$ с n свободными переменными, что для любых натуральных чисел $k_1 \dots k_n$

1. если $(k_1, \dots, k_n) \in R$, то доказуемо $\alpha(\overline{k_1}, \dots, \overline{k_n})$
2. если $(k_1, \dots, k_n) \notin R$, то доказуемо $\neg \alpha(\overline{k_1}, \dots, \overline{k_n})$.

Определение 2. Введем следующее сокращение записи: пусть $\exists! y. \phi(y)$ означает

$$(\exists y. \phi(y)) \ \& \ \forall a. \forall b. \phi(a) \ \& \ \phi(b) \rightarrow a = b$$

Здесь a и b — некоторые переменные, не входящие в формулу ϕ свободно.

Определение 3. Функция f от n аргументов называется *представимой* в формальной арифметике, если существует такая формула $\alpha(x_1, \dots, x_{n+1})$ с $n+1$ свободными переменными, что для любых натуральных чисел $k_1 \dots k_{n+1}$

1. $f(k_1, \dots, k_n) = k_{n+1}$ тогда и только тогда, когда доказуемо $\alpha(\overline{k_1}, \dots, \overline{k_{n+1}})$.
2. Доказуемо $\exists! b. \alpha(\overline{k_1}, \dots, \overline{k_n}, b)$

Задания:

1. Покажите, что пустое отношение (без единой пары) представимо в формальной арифметике.
2. Покажите, что функция $f(x) = 0$ представима в формальной арифметике.
3. Покажите, что отношение равенства представимо в формальной арифметике формулой $x_1 = x_2$. А именно:

$$(a) \text{ Покажите, что если } x_1 = x_2, \text{ то } \vdash \overline{x_1} = \overline{x_2};$$

- (b) Покажите, что если $x_1 \neq x_2$, то $\vdash \neg \overline{x_1} = \overline{x_2}$.
4. Покажите, что функция $f(x) = x + 1$ представима в формальной арифметике формулой $x_2 = x_1 + 1$. А именно:
- (a) Покажите, что $\vdash \overline{x + 1} = \overline{x} + 1$;
- (b) Покажите, что $\exists! x_2. x_2 = x_1 + 1$.
- (c) Покажите, что если $y \neq x + 1$, то $\vdash \neg \overline{y} = \overline{x} + 1$.
5. Назовём характеристическим отношением для функции f отношение
- $$C_f = \{x_1, \dots, x_n, y \mid f(x_1, \dots, x_n) = y\}$$
- Покажите, что:
- (a) Если функция f представима в формальной арифметике, то C_f выразимо в формальной арифметике;
- (b) Если характеристическое отношение C_f некоторой функции f выразимо в формальной арифметике, то функция f представима в формальной арифметике.
6. Какую формулу выбрать для выражения отношения «два числа имеют одинаковую чётность» в формальной арифметике? Наметьте план доказательства выразимости.
7. Какую формулу выбрать для представления функции «деление с остатком»? Наметьте план доказательства представимости.
8. Какую формулу выбрать для представления функции «факториал»? Наметьте план доказательства представимости.

Домашнее задание №7: рекурсивные функции

Определение 4. Рассмотрим следующие примитивы.

- $Z : \mathbb{N}_0 \rightarrow \mathbb{N}_0, Z(x) = 0$
- $N : \mathbb{N}_0 \rightarrow \mathbb{N}_0, N(x) = x'$
- Проекция. $U_i^n : \mathbb{N}_0^n \rightarrow \mathbb{N}_0, U_i^n(x_1, \dots, x_n) = x_i$
- Подстановка. Если $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$ и $g_1, \dots, g_n : \mathbb{N}_0^m \rightarrow \mathbb{N}_0$, то $S\langle f, g_1, \dots, g_n \rangle : \mathbb{N}_0^m \rightarrow \mathbb{N}_0$. При этом $S\langle f, g_1, \dots, g_n \rangle(x_1, \dots, x_m) = f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$
- Примитивная рекурсия. Если $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \rightarrow \mathbb{N}_0$, то $R\langle f, g \rangle : \mathbb{N}_0^{n+1} \rightarrow \mathbb{N}_0$, при этом

$$R\langle f, g \rangle(x_1, \dots, x_n, y) = \begin{cases} f(x_1, \dots, x_n) & , y = 0 \\ g(x_1, \dots, x_n, y - 1, R\langle f, g \rangle(x_1, \dots, x_n, y - 1)) & , y > 0 \end{cases}$$

- Минимизация. Если $f : \mathbb{N}_0^{n+1} \rightarrow \mathbb{N}_0$, то $\mu\langle f \rangle : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$, при этом $\mu\langle f \rangle(x_1, \dots, x_n)$ — такое минимальное число y , что $f(x_1, \dots, x_n, y) \neq 0$. Если такого y нет, результат данного примитива неопределен.

Первые три из них — обычные функции на натуральных числах. Оставшиеся три подобны шаблонам в C++ или функциям высшего порядка в Хаскеле/Окамле.

Например, функция $f(x) = x + 2$ может быть выражена через данные примитивы так: $f(x) = S\langle N, N \rangle(x)$.

Определение 5. Функция называется примитивно-рекурсивной, если возможно построить выражение только из первых пяти примитивов, такое, что оно при всех аргументах возвращает значение, равное значению требуемой функции.

Если функция может быть выражена с помощью всех шести примитивов, она называется рекурсивной.

Данное задание в целом сводится к демонстрации того, что различные функции являются примитивно-рекурсивными (рекурсивными). В отличие от предыдущих заданий, в данном задании это необходимо показывать при помощи демонстрации соответствующей программы на языке примитивно-рекурсивных (рекурсивных) функций. Данный язык, например, легко эмулируется языком шаблонов C++ (как подсказывает синтаксис рекурсивных выражений), также возможно использовать любой другой интерпретатор. Важно! Функции должны работать — демонстрация решения должна включать запуск программы на тестах, предложенных преподавателем и/или товарищами.

1. Покажите, что следующие функции — примитивно-рекурсивные:

- (a) сложение;
- (b) умножение;
- (c) ограниченное вычитание 1 (0 для 0, для остальных натуральных чисел совпадает с обычным вычитанием 1);
- (d) ограниченное вычитание (0, если $a < b$, и $a - b$, если $a \geq b$);
- (e) меньше: $m(a, b) = 1$, если $a < b$, иначе 0.
- (f) побитовая конъюнкция (операция $\&$ в языке Си);
- (g) побитовое «исключающее или»;
- (h) конструкция $\text{first}\langle f \rangle(x_1, \dots, x_k, n)$: возвращает минимальный $t < n$, что $f(x_1, \dots, x_k, t) \neq 0$, либо n , если функция равна 0 при всех $t \in 0 \dots n - 1$;
- (i) деление нацело (деление с округлением вниз);
- (j) остаток от деления нацело;
- (k) возведение в степень;
- (l) *частичный логарифм* $\text{plog}_k(n)$ — максимальное p , что k^p делит n . Например, $\text{plog}_6(72) = 2$;
- (m) факториал;
- (n) упорядоченную пару, т.е. набор из трёх функций (одно задание, на подпункты не делится):
 - i. левая проекция: $\pi_l(\langle a, b \rangle) = a$;
 - ii. правая проекция: $\pi_r(\langle a, b \rangle) = b$;
 - iii. построение пары: $\langle \rangle(a, b) = \langle a, b \rangle$;
- (o) проверку числа на простоту;
- (p) простое число номер k .

2. Будем называть гёделевой нумерацией списка следующую конструкцию. Пусть $\langle a_0, \dots, a_{n-1} \rangle$ — некоторый список натуральных чисел. Пусть p_i — это простое число номер i (естественно, $p_0 = 2$). Тогда гёделева нумерация этого списка $\ulcorner \langle a_0, a_1, \dots, a_{n-1} \rangle \urcorner = 2^{a_0} \cdot 3^{a_1} \cdot \dots \cdot p_{n-1}^{a_{n-1}}$. Например, $\ulcorner \langle 7, 1, 4 \rangle \urcorner = 2^7 \cdot 3^1 \cdot 5^4 = 240000$.

Покажите, что следующие функции являются примитивно-рекурсивными:

- (a) nil: гёделев номер пустого списка;
- (b) cons($x, \ulcorner \langle a_0, \dots, a_{n-1} \rangle \urcorner$) = $\ulcorner \langle x, a_0, \dots, a_{n-1} \rangle \urcorner$;
- (c) head: функция, возвращающая голову списка;
- (d) tail: функция, возвращающая хвост списка;
- (e) получение элемента списка с номером k : $(\ulcorner \langle a_0, \dots, a_{n-1} \rangle \urcorner)_k = a_k$
- (f) len: длина списка;
- (g) (@): конкатенация списков;

3. Назовём функцией Аккермана следующую функцию:

Определение 6. Функцией Аккермана мы назовем так определенную функцию:

$$A(m, n) = \begin{cases} n + 1, & \text{если } m = 0 \\ A(m - 1, 1), & \text{если } m > 0, n = 0 \\ A(m - 1, A(m, n - 1)), & \text{если } m > 0, n > 0 \end{cases}$$

Покажите, что функция Аккермана — рекурсивная (8 баллов). К сожалению, примитивно-рекурсивной данная функция не является.

Домашнее задание №8: рекурсивные функции

1.

Определение 7. Характеристической функцией отношения $R \subseteq \mathbb{N}_0^n$ назовём функцию $C_R : \subseteq \mathbb{N}_0^n \rightarrow \mathbb{N}_0$, что

$$C_R(x_1, \dots, x_n) = \begin{cases} 1, & \text{если } \langle x_1, \dots, x_n \rangle \in R \\ 0, & \text{иначе} \end{cases}$$

- (a) Покажите, что если R — выразимо в формальной арифметике, то C_R — представима в формальной арифметике.
 - (b) Покажите, что если C_R — представима, то R — выразимо.
2. В условии лабораторной С будем задавать строки как длинное число, записанное кодировкой ASCII по основанию 256: например, строка $0' = 0$ превращается в число $48 + (39 \cdot 256) + (61 \cdot 256^2) + (48 \cdot 256^3)$. Расширим определение переменных и предикатов — будем считать, что переменные и предикаты задаются не одной буквой, а любой последовательностью букв.
- (a) Напишите рекурсивную функцию, преобразующую символ из языка гёделевой нумерации в строку языка из лабораторной С. В частности, придумайте вложение занумерованных идентификаторов (например, x_n) в строки алфавита $(abcd)$.
 - (b) Напишите рекурсивную функцию, преобразующую символ из языка из лабораторной С в язык гёделевой нумерации. В частности, придумайте вложение строк алфавита $(abcd)$ в занумерованные идентификаторы (например, x_n).
 - (c) Напишите рекурсивную функцию, преобразующую строку доказательства из языка гёделевой нумерации в язык лабораторной С.
 - (d) Напишите рекурсивную функцию, преобразующую строку доказательства из языка лабораторной С в язык гёделевой нумерации.
3. Лемма об автоссылках: пусть $\psi(x_1)$ — формула с единственной свободной переменной x_1 . Тогда существует формула φ , что $\vdash \varphi \rightarrow \psi(\overline{\varphi})$ и $\vdash \psi(\overline{\varphi}) \rightarrow \varphi$
- (a) Найдите формулу φ для $\psi(x_1)$.
 - (b) Покажите, что $\vdash \varphi \rightarrow \psi(\overline{\varphi})$.
 - (c) Покажите, что $\vdash \psi(\overline{\varphi}) \rightarrow \varphi$.

Дополнительное домашнее задание

В данном разделе предложены дополнительные задачи для желающих добрать баллы. Проверяются отдельно, по договорённости.

1. Докажите, что $\vdash (a + b) \cdot (a - b) = a^2 - b^2$. Доказательство должно быть формальным, в виде файла, который будет успешно верифицирован программой из лабораторной С (9 баллов).