Задачи по монадической логике второго порядка

I. Логика конечных слов

Обозначения и соглашения. Рассматриваются слова над конечным алфавитом Σ. Формулы интерпретируются на начальных отрезках натурального ряда. Предметные переменные обозначаются маленькими буквами из конца латинского алфавита, монадические переменные – заглавными буквами. Предметные переменные интерпретируются как номера позиций, монадические – как множества (номеров) позиций. В формулах может использоваться бинарный предикат $x \in Y$, который интерпретируется так: позиция x принадлежит множеству позиций Y. Кроме того, используются бинарные предикаты равенства $x = y$, порядка $x < y$ и следования $y = x{+}1$, которые интерпретируются естественным образом, и унарные предикаты $Q_a(x)$ для каждой буквы $a \in \Sigma$, которые интерпретируются так: $Q_a(x)$ истинен на каком-то слове $w \in \Sigma^*$, если и только если в w позиция x занята буквой a. Соответствующую логику для краткости обозначаем через MSO(<).

1. Какой язык задает формула $\forall x \Big(\neg\big(\exists y (y < x)\big) \rightarrow Q_a(x)\Big)$?
Ответ: $a\Sigma^*$, т.е. все слова над алфавитом Σ, начинающиеся с буквы a.
Примечание: На формулу из этой задачи будем ниже ссылаться как First_a.

2. Какой язык задает формула $\exists x\, Q_a(x)$?
Ответ: $\Sigma^* a \Sigma^*$.

3. Какой язык задает формула $\exists x \exists y \Big((y = x{+}1) \,\&\, Q_a(x) \,\&\, Q_b(y)\Big)$?
Ответ: $\Sigma^* ab \Sigma^*$.

4. Придумать формулу, задающую язык $\Sigma^* b$.
Ответ: $\forall x \Big(\neg\big(\exists y (x < y)\big) \rightarrow Q_b(x)\Big)$. Возможны и другие варианты.
Примечание: На формулу из этой задачи будем ссылаться как Last_b.

5. Придумать формулу, задающую язык ab^*.

6. Придумать формулу, задающую язык a^*b^*.

7. Придумать формулу, задающую язык $(ab)^*$.
Ответ:

$$\mathrm{First}_a \,\&\, \mathrm{Last}_b \,\&\, \forall x \forall y \,\big((y{=}x{+}1) \rightarrow ((Q_a(x) \rightarrow Q_b(y)) \,\&\, (Q_b(x) \rightarrow Q_a(y)))\big).$$

Возможны и другие варианты.

8. Придумать формулу, задающую язык $(a^2)^*$.
Ответ:

$$\forall x\, Q_a(x) \,\&\, \exists X \Big(\forall x \forall y \big((y{=}x{+}1) \to ((x \in X) \leftrightarrow \neg(y \in X)) \big) \,\&$$

$$\& \,\forall x \big(\big(\neg(\exists y (y < x)) \to (x \in X)\big) \,\&\, \big(\neg(\exists y (x < y)) \to \neg(x \in X)\big)\big)\Big)$$

Примечание: Можно доказать, что формулой логики первого порядка задать этот язык нельзя.

9. Придумать формулу, задающую язык всех слов нечетной длины над алфавитом Σ.

10. Показать, что предикаты следования и равенства можно выразить в логике первого порядка через предикат порядка.
Ответ: равенство $x = y$ равносильно $\neg(x < y) \,\&\, \neg(y < x)$. Следование $y = x{+}1$ равносильно $(x < y) \,\&\, \neg\big(\exists z\ ((x < z) \& (z < y))\big)$.

11. Показать, что предикат порядка можно выразить в монадической логике второго порядка через предикат следования.
Ответ: отношение $x < y$ равносильно

$$(y = x{+}1) \vee$$

$$\vee \exists X \,\Big((x \in X) \,\&\, \big(\forall z \forall t \,\big((z \in X) \,\&\, (t = z{+}1)\big) \to \big((t \in X) \vee (y = t{+}1)\big)\big)\Big).$$

Примечание: можно написать чуть менее громоздкую формулу, если разрешить использовать не только следование, но и равенство. Возникает естественный вопрос, можно ли выразить порядок через следование в логике первого порядка. Ответ: нельзя.

12. Выразить через стандартные предикаты следующие монадические предикаты: а) $\mathrm{Sing} X$ (множество X одноэлементно), б) $X \subseteq Y$ (множество X содержится в множестве Y), в) $X \subseteq Q_a$ (во всех позициях множества X стоит буква a).

13. Вася написал следующую формулу, которой, как он думает, задается язык $a^* b^*$:

$$\exists X\, \exists Y\, \forall x \forall y \Big(\big((x \in X) \,\&\, (y \in Y)\big) \to \big(Q_a(x) \,\&\, Q_b(y) \,\&\, (x < y)\big)\Big).$$

а) Прав ли Вася? б) Какой язык задает Васина формула? в) Как подправить Васину формулу, чтобы подправленная формула действительно

задавала язык a^*b^*? г) Построить автомат, распознающий a^*b^*, и преобразовать его в формулу по алгоритму из доказательства теоремы Бюхи.
Решение: а) Вася неправ. б) Васина формула задает язык Σ^*, т.е. ей удовлетворяют все слова над алфавитом Σ. Дело в том, что пустое множество является вполне легитимным значением монадической переменной. Если мы в любом слове $w \in \Sigma^*$ проинтерпретируем переменные X и Y в формуле $\forall x \forall y \Big(\big((x \in X) \,\&\, (y \in Y)\big) \to \big(Q_a(x) \,\&\, Q_b(y) \,\&\, (x < y)\big)\Big)$ как пустые множества, то формула превратится в истинное высказывание (импликация истинна в силу ложности посылки). Поэтому Васина формула верна на w. в) Достаточно дополнить Васину формулу клозом, который говорит, что любая позиция принадлежит либо X, либо Y.
Примечание: Суть задачи в том, чтобы напомнить, что монадические переменные могут интерепретироваться как пустые множества.

14. Доказать, что предикат сложения $S(x, y, z) \rightleftharpoons x + y = z$ нельзя выразить в логике MSO($<$).
Решение: От противного. Пусть существует формула $\Phi(x, y, z)$ логики MSO($<$), выражающая этот предикат. Тогда формула

$$\Psi(x) \rightleftharpoons \exists z \Big(\forall y \, (y \le z) \,\&\, \Phi(x, x, z) \Big)$$

говорит, что число x – это половина длины слова, а потому формула

$$\exists x \Big(\Psi(x) \,\&\, \forall y \, \big(((y \le x) \to Q_a(y)) \,\&\, ((x < y) \to Q_b(y)) \big) \Big)$$

задает язык $\{a^n b^n \mid n = 0, 1, \dots\}$, который, как известно, не является регулярным.

15. Выразить предикат "x делится на 3" в логике MSO($<$).
Решение: Проще всего решать эту задачу, имитируя доказательство теоремы Бюхи, т.е. моделируя в MSO($<$) автомат, распознающий соответствующий регулярный язык, т.е. $(a^3)^*$. У такого автомата 3 состояния, 0 (начальное и заключительное), 1 и 2, и переходы $0 \to 1 \to 2 \to 0$. Соответственно, формула должна говорить, что x – последняя позиция слова, позиции которого разбиваются на множества X_0, X_1, X_2, так что

- начальная позиция лежит в X_1,
- если $y = z + 1$ и $z \in X_1$, то $y \in X_2$,
- если $y = z + 1$ и $z \in X_2$, то $y \in X_0$,
- если $y = z + 1$ и $z \in X_0$, то $y \in X_1$,
- позиция x лежит в X_0.

II. Логика бесконечных слов

Обозначения и соглашения. Рассматриваются бесконечные слова над конечным алфавитом Σ. Множество всех таких слов обозначается через Σ^ω. Язык $L \subseteq \Sigma^\omega$ распознается (по Бюхи) конечным недетерминированным автоматом $\mathcal{A} = (\Sigma, Q, \mathcal{E}, q_0, F)$, если L состоит в точности из всех бесконечных слов, которые можно прочесть в $\mathcal{A}$ вдоль некоторого пути, который начинается с q_0 и посещает какое-то состояние из F бесконечно много раз.

Формулы интерпретируются на натуральном ряде. Предметные переменные обозначаются маленькими буквами из конца латинского алфавита, монадические переменные – заглавными буквами. Предметные переменные интерпретируются как номера позиций, монадические – как множества (номеров) позиций. В формулах может использоваться бинарный предикат $x \in Y$, который интерпретируется так: позиция x принадлежит множеству позиций Y. Кроме того, используются бинарные предикаты равенства $x = y$, порядка $x < y$ и следования $y = x+1$, которые интерпретируются естественным образом, и унарные предикаты $Q_a(x)$ для каждой буквы $a \in \Sigma$, которые интерпретируются так: $Q_a(x)$ истинен на каком-то слове $w \in \Sigma^*$, если и только если в w позиция x занята буквой a. Соответствующую логику для краткости обозначаем через MSO(<).

1. Пусть $\mathcal{A}_1 = (\Sigma, Q_1, \mathcal{E}_1, i_1, F_1)$ и $\mathcal{A}_2 = (\Sigma, Q_2, \mathcal{E}_2, i_2, F_2)$ – два автомата; L_1 и соответственно L_2 – языки бесконечных слов, которые эти автоматы принимают (по Бюхи). Построить автомат, принимающий язык $L_1 \cap L_2$.
Решение: Положим $Q = Q_1 \times Q_2 \times \{0,1\}$ и рассмотрим автомат

$$\mathcal{A} = (\Sigma, Q, \mathcal{E}, (i_1, i_2, 1), F),$$

где

$$\mathcal{E} = \{\big((p_1,p_2,s), a, (q_1,q_2,t)\big) \mid (p_1,a,p_2) \in \mathcal{E},\ (q_1,a,q_2) \in \mathcal{E}_2 \text{ и}$$
$$t = 0 \text{ если и только если } (s=1,\ p_2 \in F_2,\ q_1 \notin F_1) \text{ или } (s=0,\ q_1 \notin F_1)\},$$
$$F = Q_1 \times F_2 \times \{1\}.$$

2. Каждое положительное натуральное число $n > 0$ можно закодировать конечным множеством натуральных чисел, используя его двоичное представление. А именно, если

$$n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_r},$$

где $i_1 > i_2 > \cdots > i_r \geq 0$, то кодом n будет множество $\{i_1, i_2, \ldots, i_r\}$. Обратно, каждое конечное множество S натуральных чисел можно считать кодом некоторого числа $n(S)$.
а) Запишите формулу логики MSO(<) с тремя свободными монадическими переменными X, Y, Z, которая истинна при тех и только тех интерпретациях, при которых X, Y, Z интерпретируются как такие конечные множества, что $n(X) + n(Y) = n(Z)$. б) Докажите разрешимость *арифметики Пресбургера*, т.е. укажите алгоритм, который по каждой формуле 1-го порядка без свободных переменных, использующей только отношение $x + y = z$, проверяет, истинна или ложна эта формула на множестве всех натуральных чисел.
Примечание: Поучительно сравнить задачу а) с задачей 1.14 (о том, что предикат сложения $S(x, y, z) \rightleftharpoons x + y = z$ нельзя выразить в логике MSO(<)). Результат задачи б) – прямое следствие задачи а) и разрешимости логики MSO(<).

3. Каждое положительное действительное число $r > 0$ можно закодировать двумя множествами натуральных чисел, используя его двоичное представление, – конечным множеством для целой части и возможно бесконечным множеством для дробной части. Обратно, каждую пару из двух множеств S, T натуральных чисел, первое из которых конечно, можно считать кодом некоторого действительного числа $r(S, T)$.
а) Запишите формулу логики MSO(<) с шестью свободными монадическими переменными X, Y, Z, X', Y', Z', которая истинна при тех и только тех интерпретациях, при которых X, Y, Z интерпретируются как конечные множества и $r(X, X') + r(Y, Y') = r(Z, Z')$. б) Укажите алгоритм, который по каждой формуле 1-го порядка без свободных переменных, использующей только отношение $x + y = z$, проверяет, истинна или ложна эта формула на множестве положительных действительных чисел.