Теория формальных систем и алгоритмов

Предварительная программа экзамена

(МФТИ, осенний семестр 2017 года)

Экзамен состоит из трёх частей: определения и формулировки основных теорем; доказательства фактов из курса; решение задач.

Экзамен начинается с беседы по первой части и при неудовлетворительном ответе на ней же и заканчивается с результатом 0 баллов.

При удовлетворительном ответе на вопросы по первой части экзаменуемый получает от 10 до 20 баллов (в зависимости от полноты ответов) и ему выдаются теоретический вопрос (легкий или трудный, по выбору студента) и задача (трудность задачи на выбор студента: простая, средняя, трудная).

Полный ответ на легкий теоретический вопрос оценивается в 30 баллов.

Полный ответ на трудный теоретический вопрос оценивается в 40 баллов.

Полное решение простой задачи оценивается в 10 баллов.

Полное решение средней задачи оценивается в 20 баллов.

Полное решение трудной задачи оценивается в 40 баллов.

1 Определения, формулировки теорем

1. Формулы исчисления высказываний.
2. Семантика исчисления высказываний: определение значения формулы.
3. Определение тавтологии, определение выполнимой формулы исчисления высказываний.
4. Схемы аксиом и правила вывода в исчислении высказываний.
5. Определение выводимой в исчислении высказываний формулы.
6. Определение вывода из гипотез в исчислении высказываний.
7. Теорема дедукции в исчислении высказываний.
8. Теорема корректности исчисления высказываний.
9. Непротиворечивость исчисления высказываний.
10. Лемма Кальмара.
11. Теорема о полноте исчисления высказываний.
12. Независимость схем аксиом исчисления высказываний.
13. Определение правила резолюции.
14. Опровержение КНФ с помощью резолюций (резолютивный вывод противоречия).
15. Семантика логики первого порядка: предикаты (отношения) и функции. Кванторные операции с предикатами.
16. Определение формулы логики первого порядка.

17. Сигнатура и модель (интерпретация символов из данной сигнатуры).
18. Оценка формулы в заданной моделе при заданной оценке переменных.
19. Свободные и связанные вхождения переменных в формулу первого порядка.
20. Параметры формулы первого порядка.
21. Определение замкнутой формулы.
22. Определение предиката, выразимого формулами первого порядка в данной модели.
23. Определение эквивалентных формул логики первого порядка.
24. Определение общезначимой формулы, выполнимой формулы, эквивалентных формул.
25. Определение формулы с разделенными переменными.
26. Предваренная нормальная форма: определение
27. Предваренная нормальная форма: основное свойство.
28. Сколемизация формулы первого порядка, её основное свойство.
29. Определение возможности элиминации кванторов в модели.
30. Теорема Тарского–Зайденберга.
31. Определение машины Тьюринга.
32. Определение функции, вычислимой на машине Тьюринга.
33. Определение многоленточной машины Тьюринга.
34. Определение универсальной машины Тьюринга.
35. Теорема о неразрешимости проблемы остановки машины Тьюринга.
36. Определение разрешимого множества.
37. Определение перечислимого множества.
38. Сводимость по Тьюрингу, основные свойства.
39. m-сводимость, основные свойства.
40. Формулировка теоремы Поста о перечислимых множествах.
41. Определение проблемы достижимости в ассоциативном исчислении.
42. Определение проблемы равенства слов в полугруппе.
43. Теорема о неразрешимости множества общезначимых формул.
44. Определение бета-функции Гёделя.
45. Теорема о неперечислимости множества формул, истинных в стандартной арифметике.

2 Теоретический вопрос

2.1 Лёгкие вопросы

1. Доказательство корректности исчисления высказываний.
2. Доказательство непротиворечивости исчисления высказываний.
3. Доказательство теоремы дедукции в исчислении высказываний.
4. Доказательство выводимости формулы $A \to A$.
5. Доказательство выводимости формулы $\neg B \to (B \to C)$.
6. Доказательство выводимости формулы $\neg\neg A \to A$.
7. Доказательство выводимости формулы $A \to \neg\neg A$.
8. Доказательство выводимости формулы $(\neg B \to \neg A) \to (A \to B)$.
9. Доказательство выводимости формулы $(A \to B) \to (\neg B \to \neg A)$.
10. Доказательство выводимости формулы $\neg(B \to C)$ из гипотез B, $\neg C$.
11. Сводимость проверки выполнимости формулы исчисления высказываний к проверке выполнимости КНФ.
12. Доказательство корректности метода резолюций: существование резолютивного опровержения влечёт невыполнимость КНФ.
13. Доказательство того, что значение формулы первого порядка зависит только от значений параметров формулы.
14. Доказательство леммы о замене связанных переменных в формуле первого порядка.
15. Доказательство эквивалентности формул $\neg\exists x A$ и $\forall x \neg A$.
16. Доказательство эквивалентности формул $\neg\forall x A$ и $\exists x \neg A$.
17. Доказательство эквивалентности формул $\forall x(A \to B)$ и $A \to \forall x B$ при условии, что A не содержит параметра x.
18. Доказательство эквивалентности формул $\exists x(A \to B)$ и $A \to \exists x B$ при условии, что A не содержит параметра x.
19. Доказательство эквивалентности формул $\exists x(B \to A)$ и $(\forall x A) \to B$ при условии, что A не содержит параметра x.
20. Доказательство эквивалентности формул $\forall x(B \to A)$ и $(\exists x A) \to B$ при условии, что A не содержит параметра x.
21. Доказательство корректности сколемизации (выполнимость сколемизации равносильна выполнимости исходной формулы).
22. Формулировка метода резолюций для универсальных дизъюнктов, доказательство корректности (если существует опровержение, то формула невыполнима).
23. Доказательство теоремы Поста о перечислимых множествах.
24. Доказательство транзитивности сводимости по Тьюрингу.
25. Доказательство транзитивности m-сводимости.

26. Доказательство того, что при сводимости по Тьюрингу сохраняется разрешимость.
27. Доказательство того, что при m-сводимости сохраняется разрешимость и перечислимость.
28. Доказательство неразрешимости проблемы остановки машины Тьюринга.
29. Доказательство неразрешимости проблемы остановки машины Тьюринга на пустом входе.
30. Доказательство перечислимости множества машин Тьюринга, останавливающихся на пустом входе.
31. Доказательство неперечислимости множества машин Тьюринга, не останавливающихся на пустом входе.
32. Лемма о бета-функции Гёделя.

2.2 Трудные вопросы

В тех вопросах, где нужны многочисленные технические детали, при рассказе обязателен общий план доказательства. Необходимость рассказа доказательств технических утверждений, отвечающих этому плану, оставляется на усмотрение экзаменатора.

1. Доказательство леммы Кальмара.
2. Доказательство теоремы о полноте исчисления высказываний.
3. Доказательство полноты метода резолюций для опровержения выполнимости КНФ.
4. Доказательство теоремы о предваренной нормальной форме.
5. Доказательство общезначимости формулы $\forall x A \to A\big|_{x\leftarrow t}$, где $A\big|_{x\leftarrow t}$ — формула, которая получается подстановкой вместо переменной x терма t, причём терм t свободен для переменной x в формуле A.
6. Доказательство полноты метода резолюций для формул первого порядка (для невыполнимой формулы существует опровержение).
7. Возможность элиминации кванторов для модели $(\mathbb{Z}, 0, S, <)$, где $S(x) = x + 1$.
8. Доказательство теоремы Тарского-Зайденберга.
9. Моделирование многоленточной машины Тьюринга на одноленточной.
10. Существование универсальной машины Тьюринга (общий план конструкции и доказательства корректности).
11. Доказательство неразрешимости проблемы достижимости в ассоциативном исчислении.
12. Доказательство неразрешимости проблемы равенства слов в полугруппе.
13. Доказательство перечислимости множества общезначимых формул.
14. Моделирование машин Тьюринга на машинах Минского (автоматы с несколькими счётчиками).
15. Доказательство неперечислимости множества формул, истинных в модели $(\mathbb{N}, 0, 1, <, =, +, \cdot)$ (формулы стандартной арифметики).

3 Типовые задачи

Приводятся примерные задачи, на экзамене могут быть другие похожего уровня сложности.

3.1 Простые задачи

1. Верно ли, что в исчислении высказываний $a \to b \vdash (a \to c) \to b$?

2. Может ли быть аксиомой исчисления высказываний формула вида $(A \to B) \to ((\neg B \to C) \to (C \to A))$, где A, B, C — формулы?

3. Является ли формула
$$(y \to z) \to ((\neg(z \to x) \to y) \to (\neg(y \to z) \to (\neg(z \to x) \to y)))$$
тавтологией?

4. Приведите пример тавтологии вида
$$\neg A \to (B \to A),$$
где A, B — некоторые формулы исчисления высказываний.

5. Применимо ли правило modus ponens к паре формул
$$(a \to b) \to (\neg a \to b) \quad \text{и} \quad (a \to b) \to \neg a?$$

6. Выведите из дизъюнктов $a \vee b$; $\neg a \vee \neg c$; $\neg b$, $b \vee c$ пустой дизъюнкт с помощью резолюций.

7. Укажите параметры формулы
$$\forall y(\forall y A(x, y) \to \forall x A(y, x)) \to \forall x(\forall y A(y, x) \to \forall x A(x, y))\,.$$

8. Найдите формулу в предварённой нормальной форме, эквивалентную формуле
$$\neg((\forall x B(x) \to \exists x A(x)) \to \forall x A(x)).$$

9. Какой предикат задает формула $\forall x(\forall y A(x, y) \to \forall x A(y, x))$ в интерпретации на множестве действительных чисел, если $A(x, y)$ интерпретируется как предикат «$xy = y$»?

10. Справедливо ли следующее утверждение «если переменная x не имеет свободных вхождений в формулу A первого порядка, то, заменив в формуле A все вхождения переменной x на переменную y, мы получим эквивалентную формулу»?

11. Примеры предикатов, выразимых в модели $(\mathbb{N}, 0, 1, <, =, +, \cdot)$ (аналогичные задачам 11аб из задания).

12. Постройте бескванторную формулу в алгебре Тарского с параметрами a, b, c, которая эквивалентна существованию действительного корня многочлена $ax^2 + bx + c$.

13. Докажите перечислимость объединения двух перечислимых множеств.

14. Дана машина Тьюринга M. Перечислимо ли множество тех слов, на которых M останавливается?

15. Постройте m-сводимость множества описаний машин Тьюринга, останавливающихся на входе 0, к множеству описаний машин Тьюринга, останавливающихся на входе 1.

16. Разрешима ли алгоритмическая проблема остановки машины Тьюринга M на входе w, если алфавит машины состоит из одного символа?

17. Функция $f\colon \mathbb{N} \to \mathbb{N}$ принимает конечное число значений. Верно ли, что f вычислима на машине Тьюринга? (Считайте, что числа записываются в двоичной системе счисления.)

18. Предложите алгоритм проверки достижимости в ассоциативном исчислении с двусторонними правилами $aba \leftrightarrow bab$.

3.2 Задачи средней трудности

1. Формулы A, B выводимы в исчислении высказываний. Докажите, что любая формула вида $((C \to A) \to \neg B) \to C$ также выводима в исчислении высказываний.

2. Известно, что формула A выводима в исчислении высказываний. Верно ли, что тогда любая формула вида $(A \to B) \to (B \to \neg A)$ также выводима? (B — некоторая формула.)

3. В исчислении высказываний выполнено $x \to y \vdash A$ (x, y — переменные, A — формула). Докажите, что $A \vee (\neg y \wedge x)$ — тавтология.

4. Верно ли, что
$$A, \neg B, C \vdash (A \wedge \neg C) \vee B?$$
(Использование теоремы о полноте не допускается.)

5. Изменится ли множество выводимых формул, если к исчислению высказываний добавить еще одно правило вывода
$$\frac{A, \quad (B \to A) \to A}{A \to B}\ ?$$

6. Множество Γ формул исчисления высказываний таково, что из него нельзя вывести любую формулу исчисления высказываний, но из множества $\Gamma \cup \{x, \neg y\}$ уже можно вывести любую формулу исчисления высказываний. Следует ли из этого, что из множества Γ можно вывести формулу $(\neg x \to y) \to \neg y$? ($x$, y — переменные.)

7. Дана такая невыполнимая КНФ с n переменными, что каждая переменная входит не более чем в два дизъюнкта. Докажите, что из дизъюнктов этой КНФ можно вывести резолюциями пустой дизъюнкт, добавив не более $O(n)$ дизъюнктов.

8. Можно ли из множества всех дизъюнктов вида $\neg x_i \vee x_j \vee x_k$, где i, j, k — попарно различные числа от 1 до 100, вывести резолюциями дизъюнкт $\neg x_1 \vee \neg x_2$?

9. Рассмотрим модель $(\mathbb{R}, L(x, y))$, где предикат означает «$x \leqslant y^2$». Определите значение формулы
$$\forall x \forall z((L(x, y) \wedge L(y, z)) \to L(x, z))$$
в этой модели на оценке переменных $x = 100$; $y = 25$; $z = 5$.

10. Является ли общезначимой следующая формула
$$\exists x \forall y (A(x, y) \wedge \neg A(y, x) \to (A(x, x) \equiv A(y, y)))\ ?$$

11. Проверьте общезначимость формулы $\exists x \forall y B(x, y) \to \forall y \exists x B(x, y)$ методом резолюций.

12. Возможна ли в модели $(\mathbb{Z}, 0, <)$ элиминация кванторов?

13. Докажите, что в модели $(\mathbb{N}, 0, 1, <, =, +, \cdot)$ выразим предикат «x имеет ровно 11 делителей».

14. Выразим ли в алгебре Тарского, то есть в модели $(\mathbb{R}, 0, 1, <, =, +, \cdot)$, предикат «$x$ — целое число»?

15. Выразим ли в алгебре Тарского, то есть в модели $(\mathbb{R}, 0, 1, <, =, +, \cdot)$,» предикат «$0 < x < 1$ и 20-я цифра десятичной записи x равна 1»?

16. Постройте бескванторную формулу в алгебре Тарского с параметрами p, q, , которая эквивалентна существованию кратного действительного корня многочлена $x^3 + px + q$.

17. Докажите перечислимость пересечения двух перечислимых множеств.

18. Можно ли разбить множество натуральных чисел на три непустых перечислимых неразрешимых множества?

19. Разрешимо ли множество описаний машин Тьюринга, которые вычисляют тождественную функцию? (На любом входе такая машина даёт результат, равный входу.

20. Постройте m-сводимость множества описаний машин Тьюринга, останавливающихся на входе 0, к множеству описаний машин Тьюринга, не останавливающихся на входе 1.

21. Разрешима ли задача проверки равенства слов для полугрупп, в которых левая часть каждого соотношения имеет длину 1?

22. Докажите перечислимость множества замкнутых формул первого порядка, истинных в какой-нибудь конечной модели.

23. Разрешимо ли множество замкнутых формул логики первого порядка?

24. Перечислимо ли множество выполнимых формул логики первого порядка?

3.3 Трудные задачи

1. Существует ли формула исчисления высказываний, которая встречается только в выводах длины больше 100?

2. Докажите, что для любой перестановки $\sigma \in S_n$ формула $\bigvee_j x_j \to \bigvee_j x_{\sigma(j)}$ выводится в исчислении высказываний за $O(n)$ шагов. Здесь $a \vee b$ — сокращенная запись формулы $\neg a \to b$, дизъюнкции применяются слева направо.

3. Пусть Γ — множество формул исчисления высказываний, которые содержат только одну переменную x. Докажите, что для любой тавтологии из множества Γ существует вывод в исчислении высказываний, длина которого $O(n)$, где n — длина формулы.

4. Докажите, что если у КНФ есть опровержение резолюциями, содержащее N дизъюнктов, то у отрицания этой КНФ есть вывод в исчислении высказываний длиной $\mathrm{poly}(N)$.

5. Замкнутая формула A первого порядка содержит кванторы, пропозициональные связки и бинарный предикатный символ. Известно, что A истинна в любой конечной модели (интерпретации на конечной области). Верно ли, что A общезначима?

6. Существует ли замкнутая формула первого порядка, которая истинна только в интерпретациях на множествах, содержащих ровно 5 элементов?

7. Выразим ли в модели $(\mathbb{N}, 0, 1, <, =, +, \cdot)$ тернарный предикат «$x = \binom{n}{k}$»?

8. Пусть $A(u, x, y)$ — формула логики первого порядка, у которой ровно три параметра u, x, y; P — бинарный предикатный символ, который не входит в формулу $A(u, x, y)$. Докажите, что тогда формула
$$\exists u \forall x \exists y A(u, x, y)$$
общезначима тогда и только тогда, когда общезначима формула
$$\exists u \Big(\forall x \big(\exists y A(u, x, y) \to P(u, x) \big) \to \forall x P(u, x) \Big).$$

9. Разрешимо ли множество описаний таких МТ, которые при работе на пустом входе проходят через каждую ячейку не более пяти раз?

10. Разрешимо ли множество описаний МТ, которые на любом входном слове w работают не дольше, чем $|w|$ тактов?

11. Докажите, что проблема достижимости одного слова из другого подстановками в соответствии с правилами ассоциативного исчисления над двоичными словами (то есть словами в алфавите $\{0, 1\}$) алгоритмически неразрешима.

12. Перечислимо ли множество замкнутых формул логики первого порядка, истинных во всех бесконечных интерпретациях?