Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Математическая логика и теория алгоритмов

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности

ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– контрольные работы 1, 2;(ОПК-3, ИОПК-3.1-3.3)

Пример варианта Контрольной 1.

Вариант №1.

1.1.Выяснить имеет ли место логическое следование $P \to Q \models (Q \to R) \to (P \to R)$

a) По определению.

b) Методом эквивалентных преобразований.

c) С помощью таблицы истинности.

d) Методом резолюций.

e) Для множества дизъюнктов, полученного в d), построить замкнутое семантическое дерево.

1.2.Найти неизвестную функцию $F(x,z)$ (хотя бы одну нетривиальную) от заданных переменных, которая является логическим следствием посылок $x \cup y, \bar{x} \to p, \bar{x} \cap p, z \cap x$ и сделать проверку логического следования методом резолюций.

1.3.Выразить все неизвестны высказывания X через P и Q так, чтобы высказывание $(Q \to X) \cup \overline{\overline{(P \cup Q)} \cup X}$ стало тождественно ЛОЖНО. Сделать проверку методом резолюций. Для полученного множества дизъюнктов построить замкнутое семантическое дерево (для одного из нетривиальных случаев).

1.4. Проверить будет ли множество дизъюнктов Хорновским(если нужно переименовать). Проверить выполнимость множества Хорновских дизъюнктов (стратегией от факта). Если множество выполнимо, то задать модель

$D = \{P \cap \bar{A},\ \ Q \cap \bar{A} \cap \bar{P},\ \ \bar{P} \cap Q,\ \ R,\ \ P \cap Q \cap \bar{S},\ \ P \cap \bar{S} \cap R,\ \ P \cap \bar{R},\ \ S \cap \bar{R}\}.$

Пример варианта контрольной 2.

Вариант №1.

1.1. Привести к а) предварённой б) сколемовской нормальной форме формулу:
$\exists x \forall y((Q(x,y) \wedge \forall z R(x,y,z)) \to \forall z \exists x(R(x,y,z) \vee Q(z,x)))$.

1.2. Будет ли формула тождественно истинна, выполнима, опровержима или тождественно ложна:
а) $\forall y \exists x P(x,y) \to \exists x \forall y P(x,y)$,
б) $\exists x \forall y P(x,y) \to \forall y \exists x P(x,y)$

1.3. Записать отрицание данного высказывания в положительной формулировке символами
$\forall n \in \mathbb{N}\ \forall x \in \mathbb{R}:\ a_n \leqslant 0\ \wedge\ f(x) \leqslant 1$.

1.4. Доказать методом резолюций общезначимость
$[\forall x(\exists y P(x,y) \vee Q(y))] \to [\exists y P(f(x),y) \vee Q(y)]$

1.5. Методом резолюций выяснить будет ли иметь место логическое следование
$\neg P(x), Q(x) \vee P(x) \models \exists x Q(x)$

1.6. Построить равносильную бескванторную формулу для $\langle \mathbb{Z}, <, =, S, 0\rangle$
$\exists x((x=2) \wedge (x = y+2) \wedge (y < z))$

Для получения оценки за экзамен - по практической части требуется сделать все задачи контрольных работ (задачи на знание определений и алгоритмов).

Теоретический экзаменационный билет состоит из двух частей теории и формируется из билетов Часть 1, Часть 2. К теоретическим вопросам допускаются студенты сдавшие полностью задания контрольных работ 1,2. Для получения оценки 3 достаточно сдать все задачи кр1, кр2, для оценки 4 – сдать практику и знать определения и основные алгоритмы, уметь доказывать по определению. Для оценки 5 – сдать практику, знать определения, алгоритмы и знать идеи и методы доказательства всех теорем.

Билеты Часть1. Математическая логика и теория алгоритмов. 2024. ;(ОПК-3, ИОПК-3.1-3.3)

1	Дать определения: язык нулевого порядка, формула логики высказываний, ранг формулы. Сформулировать законы алгебры логики высказываний, доказать з-ны де Моргана. Дать определение СДНФ, СКНФ. Рассказать алгоритмы приведения к СДНФ, СКНФ.	Пусть $\alpha^{\sigma} = \begin{cases} \alpha, & если \quad \sigma = 1 \\ \_ & \\ \alpha, & если \quad \sigma = 0 \end{cases}$ Пусть α формула, все буквы которой содержатся среди букв $A_1, A_2, \ldots, A_k$, и φ некоторая интерпретация. Тогда $A_1^{\varphi(A_1)}, A_2^{\varphi(A_2)}, \ldots, A_k^{\varphi(A_k)} \mid -\alpha^{\varphi(\alpha)}$.
2	Дать определения: контрарная пара литер, элементарная конъюнкция, дизъюнкция, ДНФ, КНФ. Рассказать алгоритм приведения к ДНФ и к КНФ. Доказать критерий тождественной истинности формулы через КНФ (критерий ТЛ через ДНФ).	Доказать, что тавтология является выводимой формулой (в дедуктике Клини).
3	Дать определения: интерпретация языка нулевого порядка, продолжение интерпретации на множество формул логики высказываний. ТИ, ТЛ, выполнимость, эквивалентность на языке интерпретаций. Выполнимое (невыполнимое) множество формул, модель множества формул. Примеры.	Доказать теорему о семантической полноте дедуктики Клини: для любой формулы α множества формул Γ выполняется $\Gamma \mid = \alpha \quad \Rightarrow \Gamma \mid - \alpha$
4	Дать определение: формула α является логическим следствием множества формул $\Gamma \quad \Gamma \mid = \alpha$, $\varnothing \mid = \alpha$. Доказать принцип дедукции: $\Gamma \mid = \alpha \to \beta \quad \Leftrightarrow \quad \Gamma, \alpha \mid = \beta$.	Дать определение непротиворечивости исчисления (дедуктики). Доказать, что исчисление высказываний непротиворечиво.
5	Доказать, что следующие утверждения для произвольных формул $\alpha_1, \alpha_2, \ldots \alpha_n, \beta$ логики высказываний эквивалентны: $\alpha_1, \alpha_2, \ldots \alpha_n \mid = \beta$; $\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n \mid = \beta$;	Доказать семантическую корректность дедуктики Клини.

	$\models \alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \to \beta$; $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n, \overline{\beta}$ невыполнимо	
6	Дать определение: формула α выводима из множества Γ с помощью дедуктики D, вывод формулы α, Дедуктика Клини (Аксиомы 1-10, MP).	Доказать теорему компактности логики высказываний.
7	Доказать, следующие утверждения: для каждой формулы α выполняется $\vdash \alpha \to \alpha$; каждая аксиома является выводимой формулой; если $\Gamma \subseteq \Gamma'$ и $\Gamma \vdash \alpha$, то $\Gamma' \vdash \alpha$	Доказать, что любая резольвента двух данных дизъюнктов является их логическим следствием. Дать определение резолютивного вывода. Доказать теорему о семантической корректности метода резолюций.
8	Доказать свойства выводимости: $\Gamma, \alpha \vdash \alpha$ пр-ло повторения посылки; Если $\Gamma \vdash \alpha$, то $\Gamma, \beta \vdash \alpha$ пр-ло введения посылки; Если $\Gamma \vdash \alpha \to \beta$, то $\Gamma, \alpha \vdash \beta$ пр-ло удаления импликации	Доказать теорему о полноте метода резолюций (в логике высказываний).
9	Доказать свойства выводимости: $\Gamma, \alpha, \beta \vdash \alpha \wedge \beta$ пр-ло введения конъюнкции; $\Gamma, \alpha \wedge \beta \vdash \alpha$; $\Gamma, \alpha \wedge \beta \vdash \beta$ пр-ло удаления конъюнкции; $\Gamma, \alpha \vdash \alpha \vee \beta$; $\Gamma, \beta \vdash \alpha \vee \beta$ пр-ло введения дизъюнкции	Доказать теорему компактности логики высказываний. Замкнутое семантическое дерево (определение, пример). Всегда ли для невыполнимого множества существует замкнутое семантическое дерево?
10	Доказать свойства выводимости: $\Gamma, \overline{\overline{\alpha}} \vdash \alpha$ удаление отрицания; Если $\Gamma \vdash \alpha$, $\Gamma \vdash \alpha \to \beta$, то $\Gamma \vdash \beta$ пр-ло MP;	Сформулировать алгоритм проверки логического следования методом резолюций в логике высказываний. Обосновать шаги. Привести пример.
11	Доказать теорему дедукции для исчисления высказываний (в дедуктике Клини).	Дать определения: хорновский дизъюнкт, единичный дизъюнкт, позитивный дизъюнкт. Рассказать алгоритм проверки множества хорновских дизъюнктов на выполнимость (от факта). Привести примеры.

Билеты к экзамену по математической логике и теории алгоритмов. Часть 2. ;
(ОПК-3, ИОПК-3.1-3.3)

1.1.Дать определение терма языка 1 порядка. 1.2. Пусть сигнатура языка содержит целые числа в качестве констант, двуместные функциональные символы + и r , предикатный символ J и пусть x,y – переменные. Какие из следующих выражений будут термами в данной сигнатуре: А) xr $(y+2)$ Б) x В) xJ $(y+2)$ Г) $y+2$	1.3. Доказать (пояснить алгоритм), что интерпретация (алгебраическая система) $\langle \ddot{y}, =, <, S \rangle$ допускает элиминацию кванторов. 1.4. Расскажите алгоритм приведения формулы языка 1 порядка к Сколемовской нормальной форме, приведите пример.

2.1.Дать определение сигнатуры языка 1 порядка, формулы языка 1 порядка. 2.2.Пусть сигнатура языка содержит целые числа в качестве констант, двуместные функциональные символы + и г , предикатный символ J и пусть x,y – переменные. Какие из следующих выражений будут формулами в данной сигнатуре: А) xг $(y+2)$ Б) x В) xJ $(y+2)$ Г) xг $(y+2)$J 0	2.3. Пусть P -- одноместный предикатный символ, f -- одноместный функциональный символ. Выяснить будет ли формула $"xP(x)$® $P(f(x))$ выполнимой, общезначимой, опровержимой, противоречием ? 2.4. Рассказать алгоритм элиминации кванторов для $\langle$¤ ,=,< $\rangle$. Элиминировать кванторы $\$x((x$J yЩ$x>z)$Ъ$(x>u))$
3.1.Дать определение общезначимой (тождественно истинной) формулы языка 1 порядка. 3.2. Какие из следующих формул являются общезначимыми для произвольной формулы $A(x)$с одной свободной переменной для любой сигнатуры А) $"yA(y)$® $\$xA(x)$ Б) $\$yA(y)$® $"xA(x)$ С) $"y\overline{(A(y)$Щ$\overline{A(y)})}$ Ответ объясните.	3.3. Дайте определение аксиоматической теории 1 порядка. 3.4. Какие из следующих формул не являются равносильными $\forall xA(x)\vee\forall xB(x)\equiv\forall x(A(x)\vee B(x))$ $\exists x(A(x)\vee B(x))\equiv\exists xA(x)\vee\exists xB(x)$ $\exists x\exists yP(x,y)\equiv\exists y\exists xP(x,y)$ Докажите.
4.1.Дать определение выполнимой формулы языка 1 порядка. 4.2. Какие из следующих формул являются выполнимыми для произвольной формулы $A(x)$с одной свободной переменной А) $"x(A(x)$Щ$\overline{A(x)})$ Б) $\$xA(x)$® $"yA(y)$ С) $\overline{"yA(y)$® $\$xA(x)}$ Ответ объясните.	4.3. Дайте определение вывода формулы из множества формул для аксиоматической теории. 4.4. Дать определение общезначимой формулы. Доказать, что из $\alpha_1\wedge\alpha_2\wedge\ldots\wedge\alpha_n\to\beta$ общезначима, следует, что $\alpha_1\wedge\alpha_2\wedge\ldots\wedge\alpha_n,\overline{\beta}$ невыполнимо.
5.1. Рассказать алгоритм приведения к Сколемовской нормальной форме формулы языка 1 порядка. Привести пример. 5.2. Доказать, что из $\alpha_1\wedge\alpha_2\wedge\ldots\wedge\alpha_n,\overline{\beta}$ невыполнимо, следует, что $\alpha_1,\alpha_2,\ldots\alpha_n\models\beta$	5.3. Доказать, что интерпретация (алгебраическая система) $\langle$ў ,=, $S,0\rangle$ допускает элиминацию кванторов. 5.4. Приведите пример элиминации кванторов для $\langle$ў ,=, $S,0\rangle$.

6.1. Дать определение истинностное значение формулы $\$x_1 P(x_1, x_2)$ языка 1 порядка в интерпретации на оценке. 6.2. Задан некоторый язык 1 порядка с константами a и b, с одноместным предикатным символом P. Пусть задана интерпретация, с областью интерпретации $M = \{a, b\}$ и интерпретация предикатов: $P(a) = 1, P(b) = 0$. Найдите истинностное значение формулы в данной интерпретации: $\$xP(x) Ъ "xP(x)$ будет ли данная формула выполнимой?	6.3. Известно, что формула $"x\, a(x)$ общезначима. Будет ли общезначимой формула $a(x)$. Докажите. 6.4. Дать определение (записать в символической форме), что значит, формула является логическим следствием множества формул языка 1 порядка. Доказать, что из общезначимости $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \to \beta$ следует $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \models \beta$.
7.1.Дайте определение истинностного значения формулы $"x_1 P(x_1, x_2)$ языка 1 порядка в интерпретации на оценке. 7.2. Пусть задан некоторый язык 1 порядка с константами a и b, с одноместными предикатными символами P и Q. Пусть задана интерпретация, с областью интерпретации $M = \{a, b\}$ и интерпретация предикатов: $P(a) = 1, P(b) = 1, Q(a) = 1, Q(b) = 0$. Найдите истинностное значение формулы в данной интерпретации: $\$x"y(P(x) Ш Q(y))$	7.3. Какая аксиоматическая теория называется исчислением предикатов? Сформулируйте теорему Гёделя о полноте для исчисления предикатов. 7.4. Дать определение (записать в символической форме), что значит -- множество формул является выполнимым, невыполнимым. Доказать, что из $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \models \beta$ следует, что множество формул $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n, \overline{\beta}$ невыполнимо.
8.1. Дайте определение: значение терма t в интерпретации на оценке. 8.2. Что значит терм свободен в формуле для переменной ? Будет ли терм $t = f(x, y)$ свободен для переменной z в формулах $\forall y P(z, y) \to P(x, z)$ $\forall y P(x, y) \to P(x, z)$ $\forall z \exists y P(z, y) \to P(x, z)$	8.3. Дать определение общезначимой формулы. Доказать, что из $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n, \overline{\beta}$ невыполнимо следует, что $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \to \beta$ общезначима. 8.4. Записать определение, что предел последовательности $(f(n))_{n \to \infty}$ равен a в развёрнутой форме, не используя сокращений $"e > 0, \$N$ ОГ и т.п. Сигнатура $e = \{0, <, =, f, |..|, -, Г, Ў_+, a, e, n, N, ...\}$
9.1.Дайте определение: истинностное значение формулы в интерпретации на оценке. 9.2. Будет ли формула $\exists x \forall y P(x, y) \to \forall y \exists x P(x, y)$ общезначимой ? Докажите.	9.3. Рассказать алгоритм доказательства логического следования методом резолюций в логике предикатов. Привести пример. 9.4. Дать определение элементарной эквивалентности интерпретаций (алгебраических систем). Будут ли элементарно эквивалентны $\langle ¤, =, < \rangle$ и $\langle ў, =, < \rangle$? Доказать.

10.1. Дать определение эквивалентных (равносильных) формул языка 1 порядка. 10.2. Какие из следующих формул не являются равносильными $\forall xA(x) \wedge \forall xB(x) \equiv \forall x(A(x) \wedge B(x))$ $\exists x(A(x) \wedge B(x)) \equiv \exists xA(x) \wedge \exists xB(x)$ $\forall x \exists yP(x,y) \equiv \exists y \forall xP(x,y)$ Докажите.	10.3. Дать определение элементарной эквивалентности интерпретаций (алгебраических систем). Будут ли элементарно эквивалентны $\langle$Г ,=,<$\rangle$ и $\langle$ў,=,<$\rangle$? Доказать. 10.4. Рассказать алгоритм доказательства общезначимости методом резолюций. Привести пример.
11.1. Дать определение опровержимой формулы языка 1 порядка. 11.2. Задан некоторый язык 1 порядка с константами a и b, с одноместными предикатными символами P и Q. Пусть задана интерпретация, с областью интерпретации $M = \{a,b\}$ и интерпретация предикатов: $P(a)=1, P(b)=1, Q(a)=1, Q(b)=0$. Найдите истинностное значение формулы в данной интерпретации: "$x(P(x)$Ш$Q(x))$. Будет ли формула опровержимой?	11.3. Рассказать алгоритм элиминации кванторов произвольной формулы интерпретации (алгебраической системы) $\langle$¤,=,<$\rangle$. Приведите пример. 11.4. Доказать закон де Моргана для семейства множеств используя равносильные преобразования формул языка 1 порядка: $\left(\bigcup_{n \in Г} A_n\right)^c = \bigcap_{n \in Г} A_n^c$. Сигнатура языка е $= \{O, Г, A_1, \ldots, A_n, \ldots\}$.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Тест

1. Пусть сигнатура языка содержит целые числа в качестве констант, двуместные функциональные символы + и г , предикатный символ J и пусть x,y – переменные. Какие из следующих выражений будут формулами в данной сигнатуре:

А) xг $(y+2)$

Б) x

В) x J $(y+2)$

Г) xг $(y+2)$ J 0

2. Какие из следующих формул являются общезначимыми для произвольной формулы $A(x)$ с одной свободной переменной для любой сигнатуры

А) $\forall yA(y) \to \exists xA(x)$

Б) $\exists yA(y) \to \forall xA(x)$

С) $\forall y(A(y) \text{Щ} \overline{A(y)})$

3. Какие из следующих формул являются выполнимыми для произвольной формулы $A(x)$ с одной свободной переменной

А) $\forall x(A(x) \text{Щ} \overline{A(x)})$

Б) $\exists xA(x) \to \forall yA(y)$

С) $\overline{\forall yA(y) \to \exists xA(x)}$

4. Какие из следующих формул не являются равносильными

А) $\forall xA(x) \vee \forall xB(x) \equiv \forall x(A(x) \vee B(x))$

Б) $\exists x(A(x) \vee B(x)) \equiv \exists xA(x) \vee \exists xB(x)$

С) $\exists x \exists yP(x,y) \equiv \exists y \exists xP(x,y)$

5. Что значит терм свободен в формуле для переменной?

Будет ли терм $t = f(x,y)$ свободен для переменной z в формулах

А) $\forall yP(z,y) \to P(x,z)$

Б) $\forall yP(x,y) \to P(x,z)$

С) $\forall z \exists yP(z,y) \to P(x,z)$

Ключи: 1 В) и Г), 2 А) и С), 3. Б), 4. Б) и С), 5. Б) и С)

Теоретические вопросы:

1. Предикат задан на множестве. Операции над предикатами.
2. Сигнатура, терм, формула языка первого порядка. Атомарная (элементарная) формула. Язык 1 порядка. Булева комбинация атомарных формул.
3. Свободная переменная, связанная переменная. Замкнутая формула. $\exists$ - замыкание формулы. $\forall$ - замыкание формулы.
4. Интерпретация языка 1 порядка.
5. Оценка в интерпретации.

6. Значение терма в интерпретации на оценке.
7. Истинностное значение формулы в интерпретации на оценке.
8. Формула выполнимая в интерпретации, формула выполнимая, формула опровержимая в интерпретации, формула опровержимая.
9. Формула общезначимая (тождественно истинная), формула противоречивая(тождественно ложная).
10. Равносильные (эквивалентные) формулы языка 1 порядка.
11. Пренексная (предваренная) нормальная форма формулы языка 1 порядка.
12. Сколемовская нормальная " - форма языка 1 порядка.
13. Формула является логическим следствием множества формул (пустого множества).
14. Множество формул языка 1 порядка является выполнимым (совместным, непротиворечивым), невыполнимым.
15. Терм свободен для переменной в формуле.
16. Литерал. Элементарный дизъюнкт. Унификация переменных двух дизъюнктов (унифицирующая подстановка).
17. Говорят, что задана аксиоматическая теория языка 1 порядка.
18. Вывод формулы из множества формул в аксиоматической теории языка 1 порядка.
19. Исчисление предикатов (аксиомы и правила вывода можно выписать на карточку).
20. Интерпретация языка 1 порядка с заданной сигнатурой допускает элиминацию кванторов.
21. Элементарно эквивалентные интерпретации языка 1 порядка.

Список алгоритмов

1. Доказательство логического следования методом резолюций.
2. Доказательство общезначимости методом резолюций. Доказательство противоречивости методом резолюций.
3. Приведение формулы к Сколемовской нормальной форме.
4. Элиминация кванторов для $\langle$ў,=,S,0$\rangle$, $\langle$ў,=,<,$S\rangle$, $\langle$¤,=,<$\rangle$

Информация о разработчиках

Галанова Наталия Юрьевна, доцент каф. общей математики, ММФ, ТГУ