

Задачи экзамена по курсу ``Верное и доказанное''

май 2012 года

Решения экзамена можно оставлять на вахте в НМУ для Раскина, передавать мне лично, найдя в НМУ или в МГУ, или посылать по электронной почте gaskin@mcsmc.ru Экзамен проходит до 27.05.2012. В понедельник, 28.05.2011, я планирую утром взять на вахте и найти в почте последние сданные работы.

Просьба выбирать задачи так, чтобы можно было увидеть применение разных частей курса.

Предупреждение: среди задач есть умышленно вставленные очень трудные (которые я полностью решать не умею и, возможно, за разумное время их решить нельзя). Задачи не упорядочены ни по какому разумному правилу. Пункты одной задачи не обязательно делать все сразу (и даже по порядку). Неполные с точки зрения технических вычислений, но содержащие обоснованные правильные решения тоже будут оцениваться. Сдача работы до срока не лишает права сдавать дополнительно записанные задачи (в том числе, исправленные решения уже сданных) в течении оставшегося времени.

Про задания о компьютерных формальных доказательствах

Пример задания для автоматического поиска доказательства на языке ТРТР: `fof(symmetry, axiom, ![X, Y]: (equal(X, Y) => equal (Y,X))).`

`fof(transitivity, axiom, ![X, Y, Z]: ((equal(X, Y) & equal(Y,Z)) => equal (X,Z))).`

`fof(nonmoot, axiom, ![X]: ?[Y]: equal(X,Y)).`

`fof(reflexivity, conjecture, ![X]: equal(X,X)).`

System on ТРТР, где можно попрактиковаться с формальными доказательствами:

<http://www.cs.miami.edu/~tptp/cgi-bin/SystemOnTRTP>

E prover, которым можно воспользоваться на локальном компьютере:

<http://www4.informatik.tu-muenchen.de/~schulz/E/E.html>

1. Существует ли верный арифметический факт в стандартной модели натуральных чисел, недоказуемый в теории множеств с аксиомами Цермело-Френкеля?

2. Выводимы ли в исчислении Ламбека секвенции:

а) $A, (A/B) \rightarrow B$

б) $(A/C), B, (B \setminus C) \rightarrow A$

в) $(A/A), B \rightarrow B$

г) $C, (A/B), (A \setminus B), (C \setminus A) \rightarrow A$

3. Постройте автоматически доказуемые формулировки утверждений. Для сложных утверждений можно привести автоматически доказуемые леммы, а потом добавить их в аксиомы и доказать требуемое.

а) во всяком поле есть лишь один нулевой элемент;

б) во всяком поле произведение нуля с чем угодно равно нулю;

в) если для некоторой ассоциативной операции $*$ на непустом множестве уравнение $a * x = b$ имеет единственное решение при любых a, b , то эта операция задаёт группу.

г) в линейном пространстве не может быть одновременно трёхэлементного и двухэлементного базиса.

4. Какие из формул из задачи 2 можно опровергнуть с помощью модели исчисления Ламбека в виде упорядоченной полугруппы с делением? (у этой задачи тоже по одному пункту на каждую формулу)

5. Существует ли модель модальной логики, в которой верны все утверждения верные в моделях с транзитивной достижимостью и только они?

6. Существует ли модель модальной логики, в которой $\Box\varphi$ верно тогда и только тогда, когда φ является интуиционистской тавтологией?

7. Существует ли формула φ , такая что $\varphi \vee \neg\varphi$ является интуиционистской тавтологией?

8. Существует ли система аксиом в исчислении предикатов 1 порядка, которая полна относительно стандартной модели натуральных чисел?

9. Существует ли две программы, про которые PA может доказать, что одна работает сотую степень времени работы другой (если обе останавливаются), но не может доказать, что они обе останавливаются или обе не останавливаются?

10. Существует ли набор арифметических фактов, верных в стандартной модели натуральных чисел, из которых выводится непротиворечивость аксиоматики Цермело-Френкеля для теории множеств?

11. Являются ли тавтологиями в исчислении высказываний следующие формулы:

а) $A \rightarrow B$

б) $A \rightarrow ((A \rightarrow B) \rightarrow B)$

в) $((((E \rightarrow D) \rightarrow (F \rightarrow G)) \rightarrow (F \rightarrow G)) \rightarrow (((E \rightarrow D) \rightarrow (F \rightarrow G)) \rightarrow F) \rightarrow (((E \rightarrow D) \rightarrow (F \rightarrow G)) \rightarrow G))$

г) $(A \rightarrow B) \rightarrow (B \rightarrow \neg\neg A)$

12. Приведите пример утверждения в языке аксиом поля, независимого от аксиом поля.

13. Опишите с точки зрения свойств отношения достижимости все модели модальной логики, в которых выполнено $\Box\Box\varphi \rightarrow \Diamond\varphi$.

14. Верно ли, что если про программу нельзя доказать, что она останавливается, пользуясь только аксиомами PA , то из факта, что она не останавливается, следует непротиворечивость PA ?