# Задачи экзамена по курсу ``Верное и доказанное''

сентябрь 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 raskin@mccme.ru Экзамен проходит до 14.10.2012. В понедельник, 15.10.2012, 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 TPTP: `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 TPTP, где можно попрактиковаться с формальными доказательствами:

`http://www.cs.miami.edu/~tptp/cgi-bin/SystemOnTPTP`

E prover, которым можно воспользоваться на локальном компьютере:

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

**1.** Выводимы ли в исчислении Ламбека секвенции:

а) $A, (A/B), (B/C) \to C$

б) $(A\backslash B), (B\backslash C) \to C$

в) $((A/B)\backslash(B/A)), A \to C$

г) $C, (A/B), (A\backslash B), (C\backslash A) \to A$

д) $A, (A\backslash(B/C)), (C/A), A \to B$

е) $A, (A\backslash(B/C)), (C/A), A \to$

**2.** Какие из формул из задачи 1 можно опровергнуть с помощью модели исчисления Ламбека в виде упорядоченной полугруппы с делением? (у этой задачи тоже по одному пункту на каждую формулу)

**3.** Существует ли модель модальной логики, в которой верны все утверждения, верные во всех моделях с фундированной достижимостью, и только они?

Достижимость называется фундированной, если всякая цепочка, в которой следующий мир достижим из предыдущего, конечна.

**4.** Существует ли непустой конечный непротиворечивый набор аксиом, из которых выводятся все истинные в стандартной модели натуральных чисел утверждения длины не больше, чем количество аксиом в наборе?

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

а) в группе у элемента есть только один обратный

б) поле не может иметь характеристику два и характеристику три одновременно

в) в частично упорядоченном множестве два максимальных элемента несравнимы

г) отношение «быть подмножеством» транзитивно

**6.** Операция $RecBox$ переводит формулы исчисления высказываний в модальные формулы, добавляя перед каждой подформулой (включая всю формулу и пропозициональные переменные) $\Box$. Например, $RecBox(A \wedge (B \to \neg C)) = \Box(\Box A \wedge \Box(\Box B \to \Box\neg\Box C))$. Существует ли такая модель Крипке, что $\varphi$ является интуиционистской тавтологией тогда и только тогда, когда в модели выполнено $RecBox(\varphi)$?

**7.** Приведите пример утверждения в языке арифметики Пеано, независимого от аксиом $ZFC$.

**8.** Рассмотрим следующие свойства программы:
1) она останавливается (в стандартной модели натуральных чисел, а не за «расширенное» количество шагов)
2) в $PA$ доказуемо, что она останавливается
3) в $PA$ из того факта, что эта программа останавливается, следует непротиворечивость $PA$

Какие из 8 комбинаций этих трёх свойств возможны?

**9.** Существует ли утверждение, ложное в стандартной модели натуральных чисел, добавление которого к $PA$ позволяет доказать непротиворечивость $PA$, но не делает аксиоматику противоречивой?

**10.** Мы хотим построить модель исчисления Ламбека следующим образом: формулы переводятся в формулы модальной логики, задаётся класс моделей Крипке и верными объявляются формулы, верные (для всех интерпретаций) во всех мирах всех моделей из выбранного класса.

Можно ли так построить модель, относительно которой исчисление Ламбека будет:
а)Корректно? б)Полно? в)Полно и корректно?

**11.** Существует ли набор аксиом модальной логики, верных во всех моделях, где каждое ребро графа достижимости входит в цикл из трёх рёбер с учётом направления, и только в них?

**12.** Существуют ли две программы, такие что:
1) $PA$ может доказать, что если они обе останавливаются, то время работы каждой их них не больше $10$-й степени времени работы другой;
2) $PA$ не может доказать ни про одну из них ни то, что она останавливается, ни то, что она не останавливается;
3) $PA$ не может доказать, что они либо обе останавливаются, либо обе не останавливаются?