ЛАБОРАТОРИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Среда 18 апреля 2012 г., в 11.00

Ком. 407

М.В. Зинин

(ООО "Андер Девелопмент", Москва)

Символьные алгоритмы и программы вычисления булевых базисов Грёбнера

(по материалам кандидатской диссертации)

Булевы базисы Гребнера являются универсальным алгоритмическим инструментом решения задач алгебраического криптоанализа и булевой выполнимости. Еще одним многообещающим применением таких базисов является моделирование квантовых вычислений на классическом компьютере. В докладе будут кратко описаны наиболее распространенные алгоритмы вычисления указанных базисов Грёбнера и вариант инволютивного алгоритма для эффективного решения этой задачи. Затем будет подробно представлена программная реализация вышеупомянутого алгоритма на языке C++ и в виде специализированных пакетов, встроенных в системы компьютерной алгебры с открытым кодом REDUCE и Macaulay2. Завершают доклад результаты сравнения быстродействия представленной реализации с другими системами и пакетами, позволяющими вычислять булевы базисы Грёбнера.