

КОМПЛЕКТ ПРОГРАММ ДЛЯ АВТОМАТИЧЕСКОГО СИНТЕЗА КОМПЬЮТЕРНЫХ ПРОГРАММ СОВРЕМЕННОЙ КОМПЬЮТЕРНОЙ АЛГЕБРЫ

ТИП ПРЕДЛАГАЕМОЙ ПРОДУКЦИИ/УСЛУГИ

- программный продукт

ОБЛАСТЬ ЗНАНИЙ

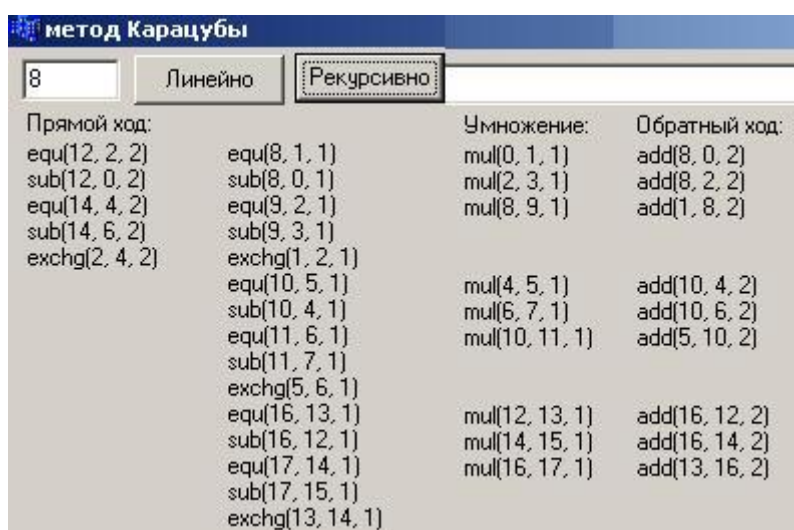
27	Математика
27.17	Алгебра
27.17.27	Поля и многочлены
50	Автоматика и вычислительная техника
50.41	Программное обеспечение вычислительных машин, комплексов и сетей
50.41.25	Прикладное программное обеспечение

ОБЛАСТИ ПРИМЕНЕНИЯ

1. Образование.
2. Научные исследования.

ПРИМЕРЫ ПРИМЕНЕНИЯ

Используется в учебном процессе кафедры Математического моделирования по дисциплинам «Дискретная математика», «Современная компьютерная алгебра» и «Методы защиты информации и распознавания образов».



метод Карацубы

8 Линейно Рекурсивно

Прямой ход:		Умножение:	Обратный ход:
equ(12, 2, 2)	equ(8, 1, 1)	mul(0, 1, 1)	add(8, 0, 2)
sub(12, 0, 2)	sub(8, 0, 1)	mul(2, 3, 1)	add(8, 2, 2)
equ(14, 4, 2)	equ(9, 2, 1)	mul(8, 9, 1)	add(1, 8, 2)
sub(14, 6, 2)	sub(9, 3, 1)		
exchg(2, 4, 2)	exchg(1, 2, 1)		
	equ(10, 5, 1)	mul(4, 5, 1)	add(10, 4, 2)
	sub(10, 4, 1)	mul(6, 7, 1)	add(10, 6, 2)
	equ(11, 6, 1)	mul(10, 11, 1)	add(5, 10, 2)
	sub(11, 7, 1)		
	exchg(5, 6, 1)		
	equ(16, 13, 1)	mul(12, 13, 1)	add(16, 12, 2)
	sub(16, 12, 1)	mul(14, 15, 1)	add(16, 14, 2)
	equ(17, 14, 1)	mul(16, 17, 1)	add(13, 16, 2)
	sub(17, 15, 1)		
	exchg(13, 14, 1)		

Пример автоматически синтезированной программы умножения многочленов 7 степени.

КРАТКОЕ ОПИСАНИЕ

Комплект программ предназначен для специалистов, занимающихся разработкой алгебраических библиотек и соответствующих логических чипов. При использовании программ могут быть получены каталоги эффективных программ алгебраических операций для колец многочленов над полями малой характеристики и эффективные программы алгебраических библиотек. Комплекс включает три программы:

1. Программа для синтеза программ приведения элемента кольца многочленов над полем малой характеристики по модулю заданного многочлена - позволяет синтезировать программы приведения элементов кольца $GF(p)[X]$ многочленов над полем малой характеристики по модулю заданного многочлена $F(X)$ на языках Python и C++;. при этом оценивается эффективность синтезируемых программ относительно стандартной реализации и контролируется соответствие функционирования.
2. Программа для синтеза программ возведения элемента кольца вычетов по модулю заданного полинома в степень, равную характеристике поля - позволяет синтезировать программы возведения элементов кольца вычетов $GF(p)[X]f(X)$ по модулю заданного полинома $F(X)$ в степень, равную характеристике поля, на языках Python и C++; при этом оценивается эффективность синтезируемых программ относительно стандартной реализации и контролируется соответствие функционирования.
3. Программа синтеза программ умножения многозначных чисел и полиномов над бинарным полем - позволяет синтезировать программы умножения многозначных чисел в бинарном представлении и многочленов высокой степени над бинарным полем; при этом оценивается эффективность синтезируемых программ относительно стандартной реализации и контролируется соответствие функционирования.

ОСОБЕННОСТИ

При автоматическом синтезе программ отпадает необходимость их тестирования.

ПРАВОВАЯ ЗАЩИТА

1. Свидетельство о государственной регистрации программы для ЭВМ № 2017619370. Программа для синтеза программы возведения элемента кольца вычетов по модулю заданного многочлена в степень, равную характеристике поля.
2. Свидетельство о государственной регистрации программы для ЭВМ № 2017619371. Программа для синтеза программ приведения элемента кольца многочленов над полем малой характеристики по модулю заданного многочлена.
3. Свидетельство о государственной регистрации программы для ЭВМ №2013618583. Программа синтеза программ умножения многозначных чисел и полиномов над бинарным полем. Дата поступления 16 июня 2013 г.

КОНТАКТЫ

Разработчик: Фролов Александр Борисович,

Институт автоматики и вычислительной техники, кафедра Математического моделирования