Санкт-Петербургский государственный политехнический университет
Физико-механический факультет
Кафедра прикладная математика

Диссертация допущена к защите
Зав. кафедрой
__________________ **В.Е. Клавдиев**

«____»____________________________

ДИССЕРТАЦИЯ
на соискание степени МАГИСТРА

Тема: ***Схемы вычисления полиномов и их приложения***

Направление: 010500 – Прикладная математика и информатика
Магистерская программа: 510209 –
Математическое и программное обеспечение компьютерных систем

Выполнил студент гр. 6057/2 М.П. Кожевников

Руководитель, к.ф.-м.н., с.н.с. Н.Н. Васильев

Консультанты:
по охране труда, к.т.н., доц. В.В. Монашков

Санкт-Петербург
2010

Содержание

1 Постановка задачи **4**

1.1 Схемы вычисления полиномов . . . 4

1.1.1 Схема как алгоритм подстановки . . . 5

1.1.2 Критерии качества . . . 5

1.1.3 Полиномы одной переменной . . . 5

1.1.4 Полиномы многих переменных . . . 6

1.1.5 Схемы для нескольких полиномов . . . 6

1.2 Вычисление значений полиномов . . . 6

1.3 Редукция полиномов . . . 7

1.4 Работы . . . 7

1.5 Эксперименты . . . 7

2 Методы построения схем **8**

2.1 Структура схемы . . . 8

2.2 Задача построения оптимальной схемы и ее сложность . . . 8

2.3 Обобщенный метод Горнера . . . 8

2.4 Метод минимального покрывающего дерева . . . 8

2.5 Совместное вычисление мономов . . . 8

2.6 Комбинированный метод . . . 8

2.7 Схемы специального вида . . . 8

2.8 Оптимальная схема для плотного полинома . . . 8

3 Метод инкрементальной редукции **9**

3.1 Кеширование нормальных форм . . . 9

3.2 Наращивание схемы . . . 9

4 Детали реализации **10**

4.1 Прототипирование . . . 10

4.2 Представление мономов . . . 10

4.3 Представление полиномов . . . 10

4.4 Кеширование нормальных форм мономов . . . 10

5 Результаты **11**

Введение

Предметом данной работы являются различные схемы вычисления полиномов и их приложения к

- эффективному *вычислению полиномов с предобработкой* без обработки коэффициентов
- редукция[1] систем полиномов относительно полиномиального базиса методом *инкрементальной редукции*

Целью работы является сравнительный анализ различных подходов к построению таких схем в контексте указанных приложений, а также их эффективная реализация.

Синтез вычисляющих программ

Вычисление полиномов с предобработкой обычно относят к *синтезу вычисляющих программ*, несмотря на то, что, зачастую, программой результат предобработки можно назвать лишь в довольно общем смысле – как правило, это некоторая форма описания последовательности действий, которые необходимо произвести над значениями переменных с тем, чтобы получить значение полинома от этих переменных. Разумеется, такая последовательность может быть записана в форме программы на интерпретируемом языке или, чаще, исполняемого модуля компилируемого языка, откуда и происходит термин.

Синтез вычисляющих программ как подход к вычислению значений функций сформировался достаточно давно – в конце пятидесятых годов прошлого века. Его задача заключается в построении эффективной процедуры вычисления значения заданной функции, что было вдвойне актуально с учетом мощности ЭВМ того времени. В большинстве случаев вычисление значения искомой функции так или иначе сводилось к вычислению значения некоторого полинома – например, через разложение в ряд или интерполяцию.

Несмотря на интенсивный рост производительности процессоров, задача актуальна и сейчас – для некоторых алгоритмов симуляции или численного решения дифференциальных уравнений, а также в тех случаях, где вычисления производятся с высокой точностью и, как следствие, существенно возрастает стоимость каждой арифметической операции.

В данной работе мы рассматриваем схемы вычисления полиномов многих переменных без обработки коэффициентов – эта область несколько менее изучена по сравнению с полиномами одной переменной. Данная задача рассматривалась и ранее, например, в [7, 8]. Нас же интересует сравнительный анализ различных подходов к построению схем в терминах их сложности и практической эффективности.

[1] В данном контексте можно было бы использовать термин «нормализация», однако он является не вполне корректным, так как относительно произвольного полиномиального базиса полином может не иметь нормальной формы

Редукция

Схема вычисления полинома может применяться не только для вычисления его значений, но и для выполнения произвольной операции подстановки (см. 1.1.1). В частности, схему можно использовать для более эффективной редукции полинома или системы полиномов относительно полиномиального базиса (см. 3). Последняя же задача представляет интерес как сама по себе, так и в качестве компонента для алгоритма вычисления базиса Грёбнера [1], чья эффективность во много определяется эффективностью алгоритма редукции [5]. Совместная редукция нескольких полиномов может также быть полезна в ряде алгоритмов [2].

Задачи

Изначально мы рассчитывали, что данная работа будет преимущественно ориентирована на создание эффективного символьно-численного интерфейса для различных типов полиномов, такого, как СПРИНТ [8]. Однако, в процессе работы мы обнаружили, что обоснование актуальности такой системы и ее сравнение с существующими аналогами представляет определенную сложность, так как

- ни один из известных нам программных пакетов общего назначения не содержит специальных средств для многократного вычисления полиномов с предобработкой, и, следовательно, сравнение с этими пакетами было бы не вполне «честным»
- количество практических задач, где возникают достаточно сложные полиномы высоких степеней весьма ограничено [**?**]
- для тех задач, где это требуется, обычно разрабатываются специальные системы с учетом особенностей задачи, что существенно осложняет сравнительный анализ

Кроме того, данная тема достаточно хорошо изучена и на сегодняшний день существенно новых результатов логично ожидать лишь для задач, где возникают полиномы специального вида, либо в области параллельных вычислений.

В свете вышесказанного было решено не делать сравнить потенциальную эффективность рассматриваемых схем лишь между собой, а основной темой работы сделать методы редукции полиномов на основании схем подстановки. Однако, так как разработка была

1 Постановка задачи

Мы будем рассматривать преимущественно полиномы с целыми или рациональными коэффициентами, либо с коэффициентами в некотором конечном поле. Бо̀льшая часть утверждений верна для любого типа коэффициентов. В тех случаях, когда это не так, тип коэффициентов будет оговорен отдельно.

1.1 Схемы вычисления полиномов

Схемы вычисления полиномов можно рассматривать как алгоритм вычисления значения полинома, записанный в терминах умножения и сложения полиномов, а также умножения полинома на число (коэффициент). В некоторых случаях возведение в спепень также рассматривают а качестве элементарной операции.

Такие схемы удобно изображать в виде диаграмм (рис. 1), где корневыми элементами являются переменные и единица, а промежуточными – операции. Входящие дуги при этом указывают, откуда берутся операнды.

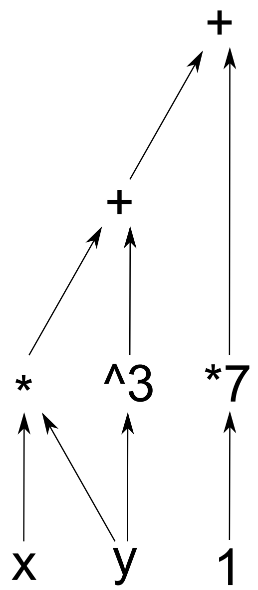

Рис. 1: Две схемы для полинома $xy + xz$

Для большинства полиномов схема вычисления, очевидно, неуникальна. Например, обе схемы на диаграмме 2 соответствуют полиному $xy + xz$. Может возникнуть впечатление, что каждая схема однозначно соответствует некоторой расстановке скобок – на диаграмме 1 это $xy + xz$ слева и $x(y + z)$ справа. Это не совсем верно, так как расстановка скобок не указывает, являются ли два вхождения одного и того же монома ссылками на один узел схемы или на два различных узла. Например, диаграмма 3 изображает две схемы вычисления полиномов, соответствующие (в смысле расстановки скобок) выражению $xy(xy+1)$.

1.1.1 Схема как алгоритм подстановки

В более широком смысле, схема вычисления полинома является схемой подстановки значений в этот полином, причем в качестве значений могут выступать элементы любого кольца, допускающие умножение на коэффициенты рассматриваемого полинома. В частности, в зависимости от типа коэффициентов это могут быть комплексные, вещественные, рациональные или целые числа, либо целые числа по заданному модулю. Кроме того, очевидно, это могут быть полиномы того же типа, что и рассматриваемый.

Таким образом, метки «+» и «*» в узлах схемы соответствуют умножению и сложению в соответствующем кольце. Следует обратить внимание, что умножение на коэффициент не обязательно совпадает с умножением в кольце. В качестве примера можно рассмотреть подстановку векторов с покомпонентным умножением и сложением в полином с целыми коэффициентами.

1.1.2 Критерии качества

Нас интересуют схемы, которые позволяют решать определенные задачи более эффективно. Следовательно, естественным критерием качества, как правило, является скорость решения соответствующей задачи. Однако, использование такого критерия на практике часто оказывается неудобным, поэтому используются различные упрощенные критерии. Для задачи вычисления в качестве упрощенного критерия может выступать общее количество операций, возможно, с весами.

Выбор подходящего критерия качества представляет собой чрезвычайно важный фактор при разработке алгоритма построения схем вычисления полиномов. Критерии, используемые для других приложений, мы обсудим позже.

1.1.3 Полиномы одной переменной

Для случая полиномов одной переменной существует два основных способа построения схем. Первый – очевидный – способ состоит в последовательном вычислении всех мономов и сложении результатов, а второй известен как «схема Горнера». Следует обратить внимание, что семантика слова «схема» в данном названии отлична от используемой в

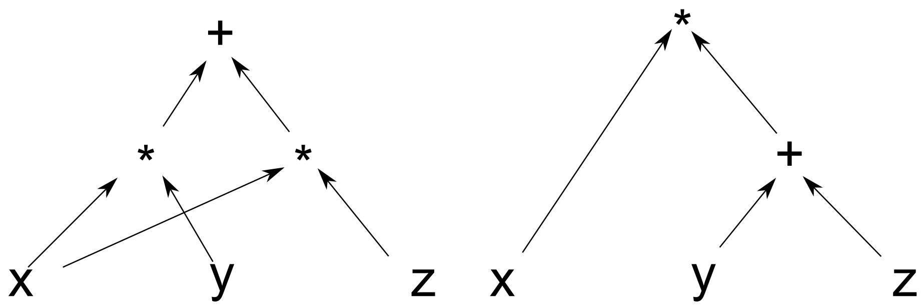

Рис. 2: Две схемы для полинома $xy + xz$

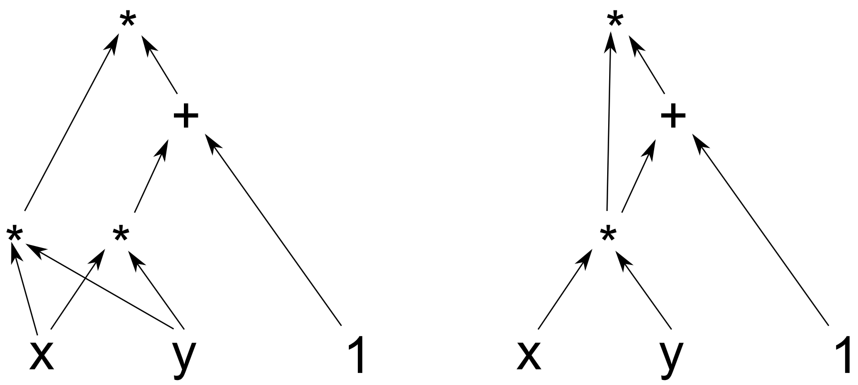

Рис. 3: Две схемы для полинома $xy(xy+1)$

нашем контексте, поэтому здесь и далее мы будем говорить о методе Горнера.

[модификация с возведением в степень]

[для большинства прилоджений схема горнера близка к оптимальной]

1.1.4 Полиномы многих переменных

В случае полиномов многих переменных построение схемы, оптимальной в смысле заданного критерия качества, является нетривиальной проблемой. Для полиномов высоких степеней построение такой схемы может быть слишком сложным с вычислительной точки зрения.

В большинстве случаев можно эффективно построить схемы, близкие к оптимальной. Это оправдано также и тем, что используемый приближенный критерий качества может не вполне соответствовать истинному критерию, и, как следствие, оптимальная схема не будет, на самом деле, наиболее эффективной.

1.1.5 Схемы для нескольких полиномов

Понятие схемы естественным образом обобщается на случай совместного вычисления нескольких полиномов. Это актуально преимущественно в задачах вычисления значений полиномов, однако совместная редукция набора многочленов относительно заданного базиса также может иметь свои приложения – например, такая задача возникает при реализации алгоритма F4 вычисления базиса Грёбнера [2].

1.2 Вычисление значений полиномов

Задача вычисления значений полиномов традиционно пользуется меньшим вниманием по сравнению, например, с задачей умножения полиномов, так как является вычислительно менее трудоемкой. В большинстве случаев схема Горнера оказывается достаточно эффективной. Однако, в тех случаях, когда значение полинома требуется вычислять многократно, выгодно подготовить схему вычисления полинома заранее.

В тех случаях, когда речь идет о вычислении значений полинома одной переменной, часто применяются схемы с обработкой коэффициентов. Описание таких схем можно найти, например, в [3, 14, 15]. Так как нас интересуют преимущественно полиномы многих переменных, мы будем заниматься лишь схемами без обработки коэффициентов.

[Нетривиальные методы вычисления значений полиномов применяются лишь тогда, когда время]

[обработка коэффициентов]

1.3 Редукция полиномов

...

1.4 Работы

Sprint, structures, Sing::monomials

1.5 Эксперименты

...

2 Методы построения схем

2.1 Структура схемы

[совместное вычисление мономов + остаток]

2.2 Задача построения оптимальной схемы и ее сложность

...

2.3 Обобщенный метод Горнера

...

2.4 Метод минимального покрывающего дерева

...

2.5 Совместное вычисление мономов

...

2.6 Комбинированный метод

...

2.7 Схемы специального вида

...

2.8 Оптимальная схема для плотного полинома

[как строится, почему оптимальная, частный случай mintree]

3 Метод инкрементальной редукции

[количество промежуточных членов]

[верно ли, что подстановка всегда дает тот же результат, что и обычная редукция. существует ли последовательность, приводящая к такому же результату?]

Метод инкрементальной редукции основан на двух свойствах нормальных форм **??**. Первое из них – линейность оператора нормализации. Второе заключается в том, что нормальная форма произведения двух полиномов равна нормальной форме произведения их нормальных форм.

$$NF(\lambda p + \mu q) = \lambda NF(p) + \mu NF(q)$$

[количество промежуточных членов]

[количество промежуточных членов]

[количество промежуточных членов]

3.1 Кеширование нормальных форм

...

3.2 Наращивание схемы

...

4 Детали реализации

...

4.1 Прототипирование

...

4.2 Представление мономов

...

4.3 Представление полиномов

...

4.4 Кеширование нормальных форм мономов

...

5 Результаты

...

Заключение

...

Список литературы

[1] Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. Москва, Мир 2000

[2] Александров Д.Е., Галкин В.В., Зобнин А.И., Левин М.В. Распараллеливание матричных алгоритмов вычисления базисов Грёбнера. Фундаментальная и прикладная математика, 2008, том 14, № 4, с. 35—64.

[3] Knuth D. The Art of Computer Programming, vol. 2, Addison-Wesley 1981

[4] Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов, Москва, Мир, 1979

[5] Клискунов А.Н. Эффективные вычисления нормальных форм в алгоритме Бухбергера. Магистерская диссертация, СПбГПУ ФизМех, 2006

[6] Vasiliev N.N., Joint Evaluations of Sparse Polynomials and the Synthesis of Evaluating Programms. Proceedings of International Conf. «Systems and Methods of Analytical Computations with Computers in Theor. Phys.» Dubna, 1985, pp. 154-159, (In Russian)

[7] Vasiliev N.N., Creation of efficient symbolic-numeric interface. Lecture Notes in Computer Science. V378 , Springer, 1989, pp. 118-119

[8] Vasiliev N.N., The System for the Synthesis of evaluating programms for polynomial-trigonometric expressions. Proceedings of International Conference «Analytical Computations with Computers in Theor. Phys.» Dubna, 1983. pp.120-124

[9] Bini D., Pan V. Parallel polynomial computations by recursive processes, Proc. ACM SIGSAM Intern. Symp. on Symbolic and Algebraic Comp., 294, 1990

[10] Bini D., Gemignani L., Pan V. Improved parallel computations with matrices and polynomials, Proc. 18-th Intern. Symposium on Automata, Languages and Programming, Lectures Notes in Computer Science, 510, 520-531, Springer 1991

[11] Vasiliev N.N. Complexity of monomial evaluations and duality. in «Computer Algebra in Scientifig Computing», V.G.Ganzha and .. (ed.) 479-485, Springer, 1999

[12] Brauer, Otto M. Addition-Subtraction Chains, Diplomarbeit, University Paderborn, 2001

[13] Кочергин В.В. Об асимптотике сложности аддитивных вычислений систем целочисленных линейных форм, Дискретный анализ и исследование операций, Апрель-Июнь 2006. Серия 1. Том 13, № 2. 38–58

[14] Белага Э.Г. О вычислении значений многочленов от одного переменного с предварительной обработкой коэффициентов. Проблемы кибернетики, вып. 5. М., Физматлит, 1961. С. 7-16

[15] Пан В.Я. Некоторые схемы для вычисления многочленов с действительными коэффициентами. Проблемы кибернетики, вып. 5. М., Физматлит, 1961. С. 17-30

[16] Olivos J. On vectorial addition chains. Journal of Algorithms, Elsevier, 1981, 13-21