Тернарная машинная арифметика: история, проблемы, приложения

В.М. Чернов
П.С. Богданов

Институт систем обработки изображений РАН

Мотивация I
Троичная арифметика

Задача:

Возможность представления как можно большего диапазона чисел с использованием как можно меньшего общего количества состояний.

Если общее количество состояний (т.е. количество представимых чисел) равно m, то количество триггеров примерно равно $\frac{m}{b}$, а количество представимых ими чисел соответственно - $b^{\frac{m}{b}}$. Как функция от b, это выражение достигает максимума при b равном числу $e=2{,}718281828\ldots$. При целых значениях b максимум достигается для $b=3$. Таким образом, “наиболее экономичными” является троичные системы счисления.

Мотивация I
Троичная арифметика

1840г. **Томас Фоулер** (DeMorgan, A. Description of a calculating machine, invented by Mr. Thomas Fowler of Torrington in Devonshire. AP.23.24. London: The Royal Society, June 1840.)

- Механическая троичная вычислительная машина

1893г. **Д.И. Менделеев** (Гашков, С. Б. Системы счисления и их применение. — М.: МЦНМО,2004.)

- разработал цифровой ряд значений весов разновеса для взвешивания на лабораторных весах, который используется по сей день

1920г. **Я. Лукасевич** (Łukasiewicz, J. O logice trójwartościowej (in Polish). 1920.)

- Троичная логика

"*Люди делятся на живущих, умерших и тех, кто плавает в океане*"

1956г. **Н.П. Брусенцов** (Брусенцов, Н.П., Альварес, Р. Троичные ЭВМ "Сетунь" и "Сетунь 70".)

- Троичная ЭВМ "Сетунь"

Технологическая проблема – надежность "троичных триггеров"

Наши дни

• Лаборатория Электронно-вычислительных машин факультета Вычислительной математики и кибернетики МГУ им. М.В. Ломоносова

Кроме того:

1. http://trinary.ru/.
2. http://3niti.org
3. http://jeff.tk//wiki/.

"Троичная уравновешенная система счисления" (цифры $\{-1,0,1\}$)

Мотивация I
Троичная арифметика

Можно ли рассматривать другие тернарные системы счисления?

Можно!

Но … зачем?

Мотивация II

Быстрые умножения больших целых чисел

Задача определения асимптотической сложности умножения $M(n)$ двух n-битовых чисел была поставлена впервые А.Н. Колмогоровым около 1956 г. и проблема поведения $M(n)$ при $n \to \infty$ была первой абсолютно нетривиальной проблемой теории быстрых вычислений. За почти более чем полувековую историю разработано довольно много различных алгоритмов в той или иной степени позволяющих “быстро” производить умножение чисел, то есть со сложностью, меньшей квадратичной по отношению к битовой длине сомножителей: алгоритмы Карацубы, Тоома-Кука, Шёнхаге-Штрассена, Фюрера и др. До появления алгоритма Фюрера наиболее быстрым алгоритмом умножения считался алгоритм Шёнхаге-Штрассена, основная идея которого заключалась в сведении умножения целых, представленных в той или иной позиционной системе счисления, к вычислению циклической свертки спектральным методом (с помощью дискретного преобразования Фурье (ДПФ) или его модулярных аналогов (теоретико-числовые преобразования, ТЧП). Сами авторы работы использовали аналог ДПФ по модулю чисел Ферма $p = 2^{2^n} + 1$ элементов, не располагая в то время алгоритмами вычисления ДПФ, более быстрыми, чем классический алгоритм Кули-Тьюки (БПФ) в комплексной или модулярной версии.

Мотивация II

“История О.”*)

$$M(N) = O(N \log N \log\log N) \quad (1)$$

(“При”? “Где”?)

---

*) Не путать!

“История О” (фр. *Histoire d'O*) — французский кинофильм, эротическая драма с элементами садо-мазо. Экранизация написанного в 1954 году романа “История О”, автор которого — Полин Реаж. В 1975 году по книге был снят фильм мастером эротического кино Жюстом Жакеном, известным по фильмам “Эмманюэль” и “Любовник леди Чаттерлей”.

Фильм получил широкую известность в видеопрокате Советского Союза, при том что фильм мог быть основанием для уголовного наказания за “распространение порнографии”.

Мотивация II
“История О.”(анализ)

1. Квазилинейная функция, стоящая под знаком “O” характеризует сложность вычисления комплексного ДПФ длины, равной степени простого числа, и значения базисных функций которого - комплексные иррациональности, вычисляемые с погрешностью. Для ряда задач (криптографии, к примеру) приближенный ответ ответом не является.

Мотивация II
“История О.”(анализ)

2. Использование модулярных версий ДПФ по простому модулю ($mod\ p$) сталкивается с ограничением делимости $N \mid (p\text{-}1)$ и возможным отсутствием среди делителей числа $(p\text{-}1)$ чисел N, для которых есть алгоритмы ДПФ с оценкой сложности $O(N\ log\ N)$. Попытка подбора простого модуля p так, чтобы выполнялось, например, соотношение $2^k \mid (p\text{-}1)$ переводит проблему в трудную задачу теории чисел о нахождении минимального простого в арифметической прогрессии.

Мотивация II
“История О.”(анализ)

2. Несмотря на то, что эта задача решена в 1944 г. Ю.В. Линником, форма, в которой получен результат, не позволяет извлечь что-то полезное для рассматриваемой нами задачи. Именно, доказано, что наименьшее простое число в арифметической прогрессии c разностью k не превосходит k^c - достаточно большая абсолютная постоянная. Заметим, что очень заниженное значение константы c, следующее из доказательства Ю.В. Линника (или К. Родосского) не меньше 20.

Мотивация II
“История О.”(анализ)

3. Использование в качестве модуля составных чисел может привести (но не обязательно!) к нарушению ортогональности базисных функций модулярного ДПФ (ТЧП) из-за наличия делителей нуля в кольце классов вычетов по составному модулю.

4. Модулярные операции не относятся к элементарным компьютерным операциям, что несколько замедляет вычисление ТЧП с “экспонентой” общего вида. Существуют немногочисленные примеры вычисления ТЧП без умножений - посредством циклического сдвига битового вектора цифр и сложений для “редких” значений N: $N=q$ для чисел Мерсенна, $p=2^q-1$ и $N=2B$ для чисел Ферма, $p=2^B-1$, $B=2^k$ для чисел Ферма.

Мотивация II
“История О.” (анализ)

5. Сложность ДПФ произвольной длины не подчиняется оценке (1), а зависит от тонкой арифметической природы числа N. В частности, с точки зрения существования быстрых алгоритмов ДПФ (или ТЧП), встречаются “плохие” числа $N=2M+1$, где M - также простое число (например, $N=47$, $M=23$) и так далее. Применение метода Рейдера синтеза быстрых алгоритмов ДПФ для таких длин N порождает алгоритмы, арифметическая сложность которых больше тривиальной. Вопрос о количестве “плохих” чисел связан, в частности, с открытым вопросом о бесконечности простых чисел Софи Жермен.

Схема Рейдера:

$$ДПФ(N) \to Conv(N-1)$$

$$47 = 2\cdot\boxed{23}+1 = 2\cdot\left(2\cdot\boxed{11}+1\right)+1 = 2\cdot\left(2\cdot\left(2\cdot\boxed{5}+1\right)+1\right)+1$$

Сколько плохих простых?

Квадратичные поля и кольца целых чисел

Пусть $Q\left(\sqrt{d}\right)$ - квадратичное поле:

$$Q(\sqrt{d}) = \left\{ z = a + b\sqrt{d};\ a, b \in Q \right\}$$

где d – целое число, свободное от квадратов, $S\left(\sqrt{d}\right)$ - кольцо целых элементов этого поля, то есть множество таких чисел $z = a + b\sqrt{d} \in Q(\sqrt{d})$, что их норма $Norm(z)$ и след $Tr(z)$ есть целые числа:

$$\mathrm{Norm}(z) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in Z,$$

$$\mathrm{Tr}(z) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in Z.$$

Канонические системы счисления

Целое алгебраическое число α называется основанием канонической системы счисления в кольце $S\left(\sqrt{d}\right)$ целых элементов поля $Q\left(\sqrt{d}\right)$, если любой целый элемент этого поля однозначно представим в форме конечной суммы

$$z = \sum_{j=0}^{k(z)} a_j \alpha^j$$

Пара $\{\alpha, I\}$ - называется канонической системой счисления в кольце $S\left(\sqrt{d}\right)$, а I – алфавитом этой системы.

- Katai I., Kovacs B. Canonical number systems in imaginary quadratic fields. // Acta Math. Acad. Sei. Hungaricae. 1981. Vol. 37. P. 159–164.
- Kovacs A. Generalized binary number system // Annales Univ. Sci. Budapest, Sect. Comp. 2001. Vol. 20. P. 195–206.

Квазиканонические системы счисления

Целое алгебраическое число α называется основанием квазиканонической системы счисления в кольце $S\left(\sqrt{d}\right)$ целых элементов поля $Q\left(\sqrt{d}\right)$, если любой целый элемент этого поля однозначно представим в форме конечной суммы

$$z = \sum_{j=0}^{k(z)} a_j \alpha^j, \ a_j \in I$$

где множество I состоит из целых алгебраических чисел, по норме меньших нормы основания α.

Пара $\{\alpha, I\}$ - называется квазиканонической системой счисления в кольце $S\left(\sqrt{d}\right)$, а I – алфавитом этой системы.

Мнимые квадратичные кольца с тернарными квазиканоническими системами счисления:

$$S\left(i\sqrt{2}\right), \quad S\left(i\sqrt{3}\right), \quad S\left(i\sqrt{11}\right)$$

Квазиканонические тернарные системы счисления в кольце Эйзенштейна $S\left(i\sqrt{3}\right)$

Теорема 1.

В кольце целых алгебраических чисел $S\left(i\sqrt{3}\right)$ существуют ровно 24 тернарные квазиканонические системы счисления, а именно, системы счисления с основаниями $\alpha_k = i\sqrt{3}\cdot\omega^{k-1}$ и множествами цифр

$$\{0,1,\omega\},\{0,\omega,\omega^2\},\{0,\omega^2,\omega^3\},$$

$$\{0,\omega^3,\omega^4\},\{0,\omega^4,\omega^5\},\{0,\omega^5,\omega^6\}$$

где $\omega=\frac{1}{2}\left(1+i\sqrt{3}\right)$ и $k=1,2,3,4.$

Арифметика в кольце целых чисел Эйзенштейна

$$\alpha_k = -i\sqrt{3}, \quad I = \{0, 1, \omega\}$$

+	0	ω	1
0	0	ω	1
ω	ω	$2\omega = \alpha^3 + \omega\alpha^2 + \omega\alpha + 1$	$1 + \omega = \alpha^4 + \omega\alpha^3 + \alpha^2 + \alpha$
1	1	$1 + \omega = \alpha^4 + \omega\alpha^3 + \alpha^2 + \alpha$	$2 = \omega\alpha + \omega$

×	ω	1
ω	$\omega^2 = \alpha^3 + \omega\alpha^2 + \alpha + 1$	ω
1	ω	1

Численные результаты

При $1 \le n \le 100,$ $m = \left(\alpha^n \pm 1\right)\left(\bar{\alpha}^n \pm 1\right)$ и $\alpha,$ равному одному из чисел множества

$$\left\{ i\sqrt{3}, -i\sqrt{3}, \frac{-3+i\sqrt{3}}{2}, \frac{-3-i\sqrt{3}}{2} \right\}$$

вычисление свертки длины

n=2, 3, 4, 5, 7, 8, 11, 13, 16, 17, 19, 23, 29, 31, 32, 37, 41, 43, 47, 53, 59, 61, 64, 67, 71, 73, 79, 83, 89, 97

можно реализовать без умножений.

Обобщения

Метод исследования приведенный в данной работе распространяется и на случай колец $S\left(i\sqrt{2}\right)$ и $S\left(i\sqrt{11}\right)$.

В $S\left(i\sqrt{2}\right)$ и $S\left(i\sqrt{11}\right)$ наряду с троичными каноническими системами счисления существуют и квазиканонические системы счисления.

Теорема 2.

В кольце целых алгебраических чисел $S\left(i\sqrt{2}\right)$ существуют ровно 4 тернарные квазиканонические системы счисления, а именно, системы счисления с основаниями $\alpha = \pm 1 \pm i\sqrt{2}$ и множеством цифр $I = \{0,1,-1\}$.

Теорема 3.

В кольце целых алгебраических чисел $S\left(i\sqrt{11}\right)$ существуют ровно 4 тернарные квазиканонические системы счисления, а именно, системы счисления с основаниями $\alpha = \dfrac{\pm 1 \pm i\sqrt{11}}{2}$ и множеством цифр $I = \{0,1,-1\}$.

Открытые проблемы

Перенесение анонсированных результатов на случай расширений полей высших степеней.

Что известно:

Теоремы чистого существования канонических систем счисления в полях разложения некоторых многочленов и классификация этих многочленов.

Что неизвестно:

- Основания канонических систем счисления в этих полях
- Алгоритмы нахождения цифр
- Алгоритмы арифметических операций

Спасибо за внимание