Полиномиальная интерполяция над кольцами вычетов $\mathbb{Z}/n\mathbb{Z}$

Канжелева О.Ю.
Научный руководитель: Васильев Н.Н.

Санкт-Петербургский Государственный Политехнический Университет

Цели и задачи

Цель работы:

- Исследование задачи полиномиальной интерполяции над кольцами вычетов

Решаемые задачи:

- Реализация алгоритма полиномиальной интерполяции
- Построение и исследование базисов Грёбнера идеалов нуль-полиномов
- Перечисление полиномиальных перестановок над кольцами вычетов

Постановка задачи

Для заданного кольца R и множества значений (x, y), $x \in S \subset R$, $y \in R$ необходимо построить полином $P(x) : \forall x \in S \ P(x) = y$, если такой полином существует. Полином, реализующий заданные значения будем называть *интерполяционным*, а процесс его построения – *интерполяцией*.

Методы интерполяции Лагранжа и Ньютона не работают в случае кольца, так как в кольце обратный элемент определен не для каждого элемента.

Алгоритм интерполяции

P.Gopalan предложил алгоритм интерполяции, который основывается на следующих идеях:

- Каждый полином может быть представлен в виде линейной комбинации базисных полиномов

$$N_0 = 1, N_i(x) = \prod_{j=0}^{i-1}(x-j), i > 0 \tag{1}$$

- Для каждого кольца существует множество, называемое интерполяционным, значения полиномиальной функции на котором определяют ее на всем кольце вычетов.

Для составного $m = \prod_{i=0}^{t} p_i^{k_i}$ интерполяционный полином над $Z_m = Z/mZ$ может быть построен с помощью *китайской теоремы об остатках*, используя результаты интерполяции над $Z_{p_i^{k_i}}$.

Интерполяционное множество

Определение

Для заданного кольца R множество $S = \{\alpha_0, ..., \alpha_k\}, S \subset R$ называется *интерполяционным*, если зная значения любого полинома в точках S, можно однозначно определить его на всем кольце. Мы будем рассматривать минимальное интерполяционное множество.

Для построения интерполяционного множества в кольце R будем искать такое подмножество $S \subset R$, которое задает нулевую функцию на всем S.

Можно построить жадный алгоритм, используя

$$N_i^S(x) = \prod_{j<i}(x - \alpha_i) \tag{2}$$

в качестве базисной функции.

Для кольца Z_n интерполяционное множество S может быть вычислено за линейное время от $|S|$.

Будем искать множество $S \subset Z_n$, задающее 0. Таким образом, необходимо найти множество:

$$\{0, ..., k-1\} : N_i(x) \equiv 0 \ \forall x = \overline{0, n} \ \forall i \geq k,$$

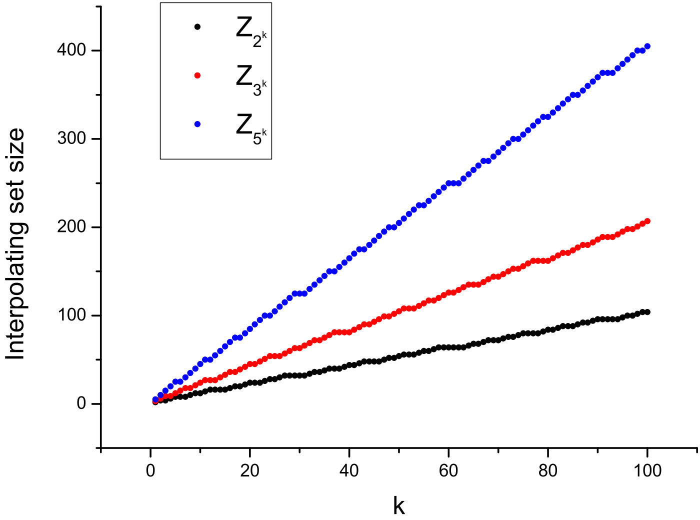
где $N_i(x)$ определено по формуле (1).

$$\forall x \text{ и } i > k \text{ или } x = \overline{0, i-1} \ \ N_i(x) \equiv 0.$$
$$N_i(i) = i! \text{ и } N_i(i+a) = \frac{(i+a)!}{a!}.$$

Значит, если $N_i(i) \equiv 0$, тогда $N_i(i+a) \equiv 0 \ \ \forall a$.
Таким образом, минимальное $k : k! \equiv 0 \mod n$ ограничивает размер интерполяционного множества.

- Сложность данного алгоритма $O(k)$

Динамика роста интерполяционного множества



Поскольку каждый полином является линейной комбинацией базисных полиномов:

$$f(x) = \sum_{i=0}^{k} c_i N_i^S(x), \quad k = |S| \tag{3}$$

интерполяционный полином может быть построен за k шагов, при условии, что интерполяционное множество S и базисные полиномы $N_i^S(x)$ известны.

Нуль-полиномы

Определение

Полином P будем называть *нуль-полиномом* над заданным кольцом R, если $\forall x \in R \;\; P(x) \equiv 0$.

Нуль-полином минимальной степени для Z_m может быть построен следующим образом:

$$\frac{m}{p}(x^p - x),$$

где p – минимальный делитель m.
Теоретические значения минимальной степени нормированного нуль-полинома для некоторых колец были получены Shujun Li.

Ясно, что эта степень совпадает с размером интерполяционного множества для кольца Z_n.

Вычисление базисов идеалов нуль-полиномов

Нуль-полиномы образуют идеал. Среди образующих базиса Грёбнера идеала полиномов всегда есть нормированный нуль-полином и нуль-полином минимальной степени. Про остальные составляющие базиса мало известно.

Основываясь на вычислении базиса Грёбнера в CAS "Singular", мы строили базисы идеалов нуль-полиномов. "Singular" был выбран как пакет, поддерживающий вычисление базиса Грёбнера в кольцах.

Решаемые задачи:

1. Проверка оценок значений, полученных Shujun Li
2. Построение базисов Грёбнера идеалов нуль-полиномов

Построенные базисы для некоторых колец

Z_{16}

$$8x^2 + 8x$$
$$2x^4 + 12x^3 + 14x^2 + 4x$$
$$x^6 + 15x^5 + 15x^4 + 13x^3 + 8x^2 + 12x$$

Z_{32}

$$16x^2 + 16x$$
$$4x^4 + 24x^3 + 28x^2 + 8x$$
$$2x^6 + 30x^5 + 30x^4 + 26x^3 + 8x$$
$$x^8 + 2x^5 + 3x^4 + 6x^3 + 12x^2 + 8x$$

Z_{64}

$$32x^2 + 32x$$
$$8x^4 + 16x^3 + 24x^2 + 16x$$
$$4x^6 + 4x^5 + 4x^4 + 28x^3 + 24x^2$$
$$x^8 + 2x^6 + x^4 + 28x^2 + 32x$$

Анализ полученных степеней нуль-полиномов

Полученные результаты согласуются с теоретическими оценками S.Li.

степень p в основании Z_{p^k}	минимальная степень норм. нуль-полинома
$k < p+1$	pk
$k = p+1$	p^2
$p+2 <= k <= 2p+1$	$p(k-1)$
$k = p(p+1)+1$	p^3

степень 2 в основании Z_{2^k}	минимальная степень норм. нуль-полинома
$k = 2$	4
$k = 3$	4
$k = 4$	6
$k = 5$	8
$k = 6$	8
$k = 7$	8

Определение

Полином $f(x) \in K[x]$ называется *пермутационным*, если он задает биективную функцию в кольце K.

Для конечного поля F_p существует $p!$ пермутационных полиномиальных функций.

Над кольцами несколько полиномов могут реализовывать одну и ту же перестановку. Например, для кольца Z_{16} полиномы

$$f(x) = x^6 + 15x^5 + 15x^4 + 13x^3 + 8x^2 + 13x$$

$$g(x) = x$$

определяют одну и туже перестановку.

Нашей целью является вычисление количества $N(m)$ пермутационных полиномиальных функций в кольце Z_m.

$N(m)$ является мультипликативной функцией, поэтому будем рассматривать только $N(p^k)$.

Рекуррентная формула количества пермутационных полиномиальных функций над Z_{p^k}

Нами была выведена рекуррентная формула количества пермутационных полиномиальных функций $N(p^k)$.

$$N(p^k) = \begin{cases} p! & \text{if} \quad k = 1 \\ p!(p-1)^p p^p & \text{if} \quad k = 2 \\ N(p^{k-1}) p^{S(p^k)} & \text{if} \quad k > 2 \end{cases} \tag{4}$$

где $S(p^k)$ – размер интерполяционного множества для Z_{p^k}.
Таким образом, $N(p^k)$ является функцией от $S(p^k)$.

Алгоритм перечисления пермутационных полиномиальных функций над кольцом Z_{p^k}

Алгоритм перечисления перестановок базируется на следующих идеях:

- Будем перечислять не все перестановки, а только сохраняющие 0
- Полиномы определяются значениями в точках интерполяционного множества, поэтому будем перечислять все подмножества длины $|S|$ перестановок, где S – интерполяционное множество для Z_{p^k}

Для колец Z_{2^k} может была произведена дополнительная оптимизация.

Используемые технологии

- Задача перечисления полиномиальных перестановок требует больших временных затрат. Поэтому, вычисления велись на 12-ядерном узле кластера delta-force.cluster.spbstu.ru. Алгоритм был реализован на языке C с использованием библиотеки OpenMPI.
- Перечисления нуль-полиномов были реализованы на языке Java.
- Базисы Грёбнера считались с помощью системы "Singular"

Численные результаты

основание кольца	число полиномиальных перестановок
8	128
9	1296
16	8192
25	384000000
27	25509168
32	2097152
64	536870912

Результаты

- Реализован эффективный алгоритм полиномиальной интерполяции над кольцами вычетов
- Разработан и реализован алгоритм построения базисов Грёбнера идеалов нуль-полиномов
- Выведена рекуррентная формула количества пермутационных полиномиальных функций над кольцами вычетов
- Реализован алгоритм перечисления пермутационных полиномиальных функций над кольцами вычетов

Спасибо за внимание