Алгоритмы решения задач теории информации, приводящие к задаче о рюкзаке

С.Ю. Корабельщикова[1]

[1]*Северный (Арктический) федеральный университет им. М.В. Ломоносова, набережная Северной Двины, 17, Архангельск, Россия, 163002*

Аннотация

В статье рассматриваются задачи теории информации, для решения которых предложены алгоритмы, приводящие их к задаче о рюкзаке. Первая задача – задача нахождения помехоустойчивых циклических *(n,k)* – кодов над конечным полем *GF(q)*, где k – число информационных символов, n – длина кода, q – число элементов поля. Вторая - задача поиска всех корней *n*–ой степени из языка над данным алфавитом. Рассматривается ее решение для языков, содержащих все слова заданной длины в данном алфавите. Разработаны алгоритмы решения, приведены результаты программной реализации.

Ключевые слова

Задача о рюкзаке, циклические коды, корни из языка

1. Введение

В работе рассматриваются две задачи теории информации, имеющие аналогию в предложенном автором методе решения. Для их решения используется метод сведения к задаче о рюкзаке, различные частные случаи которой хорошо изучены и продолжают совершенствоваться [1].

2. Задача о числе циклических (*n,k*) кодов

Рассмотрим первую задачу. Широко распространенные в системах восстановления данных коды Рида - Соломона являются циклическими кодами с задаваемыми изначально на этапе выбора кода корректирующими возможностями. Таким образом, возникает задача построения допустимого множества кодов, удовлетворяющих требуемым свойствам, а также оценки их числа. Оценим число циклических кодов с заданными параметрами k, n и q, где k – число информационных символов, n – длина кода, q – число элементов поля, используя [2]. Циклический (n, k) код над конечным полем *GF(q)* однозначно определяется порождающим нормированным многочленом $g(x)$ над полем *GF(q)*, удовлетворяющим двум условиям: степень $g(x)$ равна $n-k$ и многочлен x^n-1 делится на $g(x)$ в кольце многочленов *GF(q)*[x].

Шаг 1. Генерируем элементы *0, 1, …, n-1*

Шаг 2. Разбиваем их на круговые классы $C_i=\{i, iq, iq^2, \dots\}$ по модулю n.

Шаг 3. Подсчитываем количество элементов в каждом классе, - получаем набор чисел $(m_1, m_2, \dots, m_s)$. Его можно интерпретировать как степени неприводимых многочленов, входящих в разложение x^n-1, где s – количество делителей. Заметим, что если n и q взаимно просты, то все сомножители в разложении различны, в противном случае кратность каждого сомножителя равна v - наибольшему общему делителю чисел n и q.

Шаг 4. Считаем способы представления числа $n-k$ в виде суммы чисел $(m_1, m_2, \dots, m_s)$, взятых не более чем v раз. Этот шаг эквивалентен частному случаю задачи о рюкзаке. Результат будет равен числу различных циклических кодов с фиксированными параметрами n, k и q.

Для решения поставленной задачи не обязательно находить разложение многочлена x^n-1 на неприводимые нормированные множители над полем *GF(q)*. Достаточно того, что известны степени этих многочленов.

3. Задача поиска всех корней *n*-ой степени из языка

Для заданного языка A в алфавите Σ и заданного натурального n требуется найти все языки B, такие что $A=B^n$. При этом язык B называется корнем n - ой степени из языка A.

Пусть M - конечное подмножество множества натуральных чисел. Далее будем рассматривать язык $A=\Sigma(t_1, t_2)$, содержащий всевозможные слова над алфавитом Σ длины от t_1 до t_2 $(t_1, t_2 \in N, t_1 \leq t_2)$. Отметим вполне очевидный факт: для того, чтобы корень n-й степени из языка $\Sigma(t_1,t_2)$ извлекался, необходимо и достаточно, чтобы t_1 и t_2 делились на n. Пусть $t_1 = n \cdot n_1$ и $t_2 = n \cdot n_2$.

Теорема. *Язык $B=\Sigma(M)$ является корнем n-й степени из языка $A=\Sigma(t_1, t_2)$ тогда и только тогда, когда M – подмножество множества $n_1, n_1 + 1, \ldots, n_2$, удовлетворяющее условию: каждое число от t_1 до t_2 является суммой каких либо n слагаемых из множества M (не обязательно различных).*

Доказательство теоремы можно найти в [3]. Приведем алгоритм ее решения.

Шаг 1. Проверяем делимость чисел t_1 и t_2 на n.

Шаг 2. Генерируем все подмножества M_i множества $\{n_1, n_1 + 1, \ldots, n_2\}$

Шаг 3. Для каждого подмножества M_i проверяем возможность представления чисел от t_1 до t_2 в виде суммы n чисел из M_i.

Этот шаг эквивалентен частному случаю задачи о рюкзаке.

Шаг 4. Множества M_i, прошедшие проверку, включаем в ответ.

4. Заключение

Задача о рюкзаке допускает программную реализацию, что позволяет получать данные для анализа решений. В таблице представлен результат решения первой задачи для параметров n=15, q=2 и q=4 при различных значениях k.

Таблица 1

Число различных (*15,k*) циклических кодов над полем *GF(q)*

q \ *k*	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	1	1	1	3	3	3	3	3	3	3	3	1	1	1
4	3	9	19	33	51	65	75	75	65	51	33	19	9	3

Рассмотренный метод применим к достаточно широкому кругу задач теоретического и прикладного характера. Проведен анализ различных вариантов программной реализации задачи о рюкзаке с использованием параллельного программирования.

5. Литература

[1] Массобрио, Р. Виртуальный Эрудит для решения задачи о рюкзаке: обучение автоматическому распределению ресурсов / Р. Массобрио, Б. Диаз Дорронзоро, С.Е. Несмачнов Кановас // Труды ИСП РАН. – 2019. – Т. 31, № 2. – С. 21-32. DOI: 10.15514/ISPRAS-2019-31(2)-2

[2] Корабельщикова, С.Ю. О числе различных циклических кодов заданной длины / С.Ю. Корабельщикова, А.И. Чесноков // Вектор науки ТГУ. – 2013. – № 4(26). – С. 25-26.

[3] Melnikov, B.F. On the task of extracting the root from the language / B.F. Melnikov, S.Yu. Korabelshchikova, V.N. Dolgov // International Journal of Open Information Technologies. – 2019. – Vol. 7(3). – P. 1-6.