Секция «Дискретная математика и математическая кибернетика»

Вычислительная сложность определения локальности кода

Научный руководитель – Пантелеев Павел Анатольевич

Валинуров Денис Юрьевич
Аспирант
Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра математической теории
интеллектуальных систем, Москва, Россия
E-mail: denis.valinurow@yandex.ru

В настоящее время в теории кодирования большой интерес для приложений представляют *локально восстанавливаемые коды* - коды с таким свойством, что каждый символ кодового слова можно восстановить по небольшому множеству других символов. Существование быстрого алгоритма, проверяющего такое свойство кода, позволило бы более эффективно конструировать такие коды. Однако ниже покажем, что задача определения локальности линейного кода является NP-полной.

Пусть $\mathbb{F}_q$ — конечное поле из q элементов. Линейным $[n, k]$ кодом (над $\mathbb{F}_q$) называется произвольное k-мерное линейное подпространство $C \subseteq \mathbb{F}_q^n$. Порождающая матрица линейного $[n, k]$ кода это матрица размера $k \times n$, содержащая k линейно независимых слов в кодовом пространстве.

Определение 1. Говорим, что $[n, k]$ код обладает свойством r-локальности, если выполняется следующее: для любого $i \in [n]$ существует подмножество $R_i \subseteq [n] \setminus i, |R_i| \leq r$ такое, что ограничения множества $C(i, a) = \{x \in C : x_i = a\}$ на R_i имеют пустое пересечение для $a \neq a'$, то есть $C|_{R_i}(i, a) \bigcap C|_{R_i}(i, a') = \varnothing$.

Линейный код с таким свойством называется LRC $[n, k, r]$ кодом (locally recoverable code)[1]. Используя введённые понятия, задача определения локальности кода может быть сформулирована следующим образом:
Задача 1 Локальность кода C.
Дано: Порождающая матрица G линейного $[n, k]$ кода C над полем $\mathbb{F}_q$. Целое положительное число $r < n$.
Вопрос: Является ли C LRC кодом с параметрами $[n, k, r]$?

В литературе широко известно доказательство NP-полноты задачи определения минимального расстояния кода [2]. В некоторых случаях эта задача является двойственной к сформулированной выше задаче, поскольку кодовые слова являются проверочными соотношениями в двойственном коде. Однако в общем случае NP-полноту задачи определения локальности можно доказать сведением следующей известной NP-полной задачи [3]:
Задача 2 Трёхмерное сочетание.
Дано: $U \subseteq T \times T \times T$, где T - конечное множество.
Вопрос: Существует ли подмножество $W \subseteq U$, $|W| = |T|$ такое, что никакие два элемента W не совпадают ни в какой координате?

Используя полиномиальное сведение задачи 2 к задаче 1, получаем справедливость следующей теоремы:

Теорема 1. *Задача определения локальности кода для произвольного фиксированного конечного поля является NP-полной.*

Нетрудно привести алгоритм, решающий задачу определения локальности полным перебором за экспоненциальное время $\mathcal{O}(n^4\binom{n-1}{r})$.

Источники и литература

1) Tamo I., Barg A. A family of optimal locally recoverable codes // IEEE Transactions on Information Theory, 2014, V. 80, № 8. P. 4661–4676.
2) Vardy A. Algorithmic Complexity in Coding Theory and the Minimum distance Problem // The Twenty-Ninth annual ACM symposium, 1997, P. 92–109.
3) Garey M., Johnson D. Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman, 1979.