УДК 512.624.3:004.021

СКЛАДНІСТЬ ЗАДАЧ, ПОВ'ЯЗАНИХ ІЗ СИСТЕМАМИ ЛІНІЙНИХ ЗАБОРОН НАД СКІНЧЕННИМ ПОЛЕМ

Курінний Олег, Яковлєв Сергій

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут

Анотація

У роботі введено нотацію лінійних заборон над скінченним полем. Сформульовано та доведено властивість, яка описує структуру множини розв'язків системи лінійних заборон з нульовими правими частинами. Сформульовано задачі розпізнавання та пошуку розв'язку системи лінійних заборон та доведено еквівалентність за Тюрінгом цих задач. Оцінено складність деяких часткових випадків задачі існування розв'язку системи лінійних заборон. Запропоновано імовірнісний поліноміальний алгоритм пошуку розв'язку системи лінійних заборон у випадку обмеженої кількості заборон.

Abstract

In this paper we introduced a notion of linear restrictions over finite field. We formulated and proved a property that describes solution set structure of the system of linear restrictions with right-hand side set to zero. We formulated decision and search problems for the solution of linear restrictions system and proved that these problems are Turing equivalent. We evaluated complexity of several partial cases of decision problem. We proposed polynomial probabilistic algorithm for finding solution of the system of linear restrictions in the size-limited case.

Вступ

В алгебраїчному криптоаналізі потокових шифрів [1] виникає задача відновлення невідомого вектору за деякою системою поліноміальних рівнянь над скінченним полем. Оскільки розв'язування таких систем, як правило, складне з обчислювальної точки зору, то розглядаються випадки, коли про невідомий вектор можна отримати часткову інформацію, яка пов'язана з особливостями каналу зв'язку або практичною реалізацією криптосистеми. Такою частковою інформацією можуть бути обмеження на можливі значення лінійних співвідношень із невідомим вектором. Виникає необхідність формалізації описаної задачі, тому в роботі визначаються поняття лінійної заборони та системи лінійних заборон над скінченним полем, досліджуються властивості системи лінійних заборон та складність деяких задач, пов'язаних із системами лінійних заборон.

Означення та властивості системи лінійних заборон над скінченним полем

Визначимо поняття лінійної заборони та системи лінійних заборон за аналогією до лінійного рівняння та системи лінійних рівнянь.

Означення 1. *Лінійною забороною* над полем $GF(2^k)$, де $k \geq 1$, будемо називати виразу типу

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \neq a_0,$$

де $a_i \in GF(2^k)$ для $i = \overline{0,n}$, $x_i \in GF(2^k)$ для $i = \overline{1,n}$.

Якщо позначити $a = (a_1, a_2, \ldots, a_n)$, то можна переписати лінійну заборону у вигляді $(a, x) \neq a_0$, де (a, x) – скалярний добуток векторів a та x. *Розв'язком лінійної заборони* будемо називати такий вектор $x_0 \in GF(2^k)^n$, що $(a, x_0) \neq a_0$. *Множиною розв'язків лінійної заборони* будемо називати множину векторів $\left\{x \in GF(2^k)^n \mid (a, x) \neq a_0\right\}$. Було доведено, що потужність множини розв'язків лінійної заборони становить $2^{kn} - 2^{k(n-1)}$.

Означення 2. *Системою лінійних заборон* над полем $GF(2^k)$ будемо називати систему співвідношень виду

$$\begin{cases} (a^{(1)}, x) \neq a_0^{(1)} \\ (a^{(2)}, x) \neq a_0^{(2)} \\ \dots \\ (a^{(m)}, x) \neq a_0^{(m)} \end{cases}$$

де $m > 1$ та $a^{(j)} = (a_1^{(j)}, a_2^{(j)}, \dots, a_n^{(j)})$ для $j = \overline{1,m}$, $a_i^{(j)} \in GF(2^k)$ для $i = \overline{0,n}$, $j = \overline{1,m}$.

Якщо позначити $a_0 = (a_0^{(1)}, a_0^{(2)}, \dots, a_0^{(m)})$ та $A = \left\{a_i^{(j)}\right\}_{i=\overline{1,n}}^{j=\overline{1,m}}$, то систему лінійних заборон можна записати у вигляді $Ax \neq a_0$. В даному випадку символ «$\neq$» означає, що вектори Ax та a_0 не збігаються одночасно у всіх координатах.

У випадку $a_0 = \bar{0}$ (де $\bar{0}$ – це вектор, який складається з нулів) було доведено таку властивість множини розв'язків системи лінійних заборон.

Твердження 1. Нехай D – це множина розв'язків системи лінійних заборон $Ax \neq \bar{0}$. Тоді $|D|$ ділиться націло на $2^k - 1$.

Це твердження описує структуру розв'язків системи лінійних заборон: множина розв'язків розбивається на декілька класів еквівалентності, де відношення еквівалентності (будемо називати його *відношенням пропорційності*) визначається таким чином: два вектори $z^{(1)}$ та $z^{(2)}$ знаходяться у відношенні пропорційності, якщо існує елемент $b \in GF(2^k)^*$ такий, що $z^{(1)} = b \cdot z^{(2)}$, де $b \cdot z^{(2)} = (b \cdot z_1^{(2)}, b \cdot z_2^{(2)}, \dots, b \cdot z_n^{(2)})$.

Зауважимо, що наведене твердження виконується також для однієї лінійної заборони, оскільки $2^{kn} - 2^{k(n-1)} = 2^{k(n-1)}(2^k - 1)$.

Складність деяких задач, пов'язаних із системами лінійних заборон

Сформулюємо задачу існування розв'язку системи лінійних заборон.

Задача 1. (SLR-decision)

Вхід. $GF(2^k)$, матриця A розміру $m \times n$, вектор a_0 розміру $m \times 1$.

Необхідно з'ясувати чи існує розв'язок у системи лінійних заборон $Ax \neq a_0$.

Вихід. «Так», якщо розв'язок існує, «Ні», інакше.

Зауважимо, що сформульована таким чином задача є *задачею розпізнавання* [2]. Було доведено твердження щодо складності цієї задачі.

Твердження 2. Задача SLR-decision належить класу складності NP.

На практиці у багатьох випадках необхідно знайти сам розв'язок, а не перевірити його існування, тому сформулюємо відповідну задачу.

Задача 2. (SLR-search)

Вхід. $GF(2^k)$, матриця A розміру $m \times n$, вектор a_0 розміру $m \times 1$.

Необхідно знайти хоча б один розв'язок системи лінійних заборон $Ax \neq a_0$, якщо він існує.

Вихід. Розв'язок системи лінійних заборон $Ax \neq a_0$ або «$\perp$», якщо його не існує.

Зауважимо, що сформульована задача є *задачею пошуку* [2]. Було доведено твердження, яке, в певному сенсі, надає змогу звести розв'язок однієї задачі до розв'язку іншої.

Твердження 3. Задача розпізнавання SLR-decision та задача пошуку SLR-search є еквівалентними та Тюрінгом [3].

Розглянемо декілька часткових випадків задачі SLR-decision.

1. Задача $GF(2)$-SLR-decision – це задача SLR-decision, в якій поле фіксоване і дорівнює $GF(2)$.
2. Max-SLR-decision – це задача SLR-decision, в якій необхідно знайти розв'язок, який задовольняє щонайменше l лінійних заборон, де $1 \le l \le m$.
3. Restricted-SLR-decision – це задача SLR-decision, в якій для всіх входів виконується умова $m \le 2^{k-1}$.

Зауважимо, що Restricted-SLR-decision є *задачею типу promise* [2], тобто не на всі можливі входи необхідно надати відповідь «Так» або «Ні», оскільки на входи, для яких не виконується $m \le 2^{k-1}$, можна не повертати жодної відповіді.

Була оцінена складність наведених задач.

Теорема. Виконуються такі твердження:

1. Задача $GF(2)$-SLR-decision належить класу складності P.
2. Задача Max-SLR-decision є NP-повною.
3. Задача Restricted-SLR-decision належить класу складності RP.

Оскільки задача Restricted-SLR-decision належить RP, то для неї існує імовірнісний поліноміальний алгоритм з односторонньою помилкою, імовірність якої обмежена константою 0,5. Якщо застосувати цей алгоритм d разів, то помилка алгоритму буде обмежена значенням 2^{-d}. Таким чином, можна побудувати алгоритм, який перевіряє існування розв'язку системи лінійних заборон з експоненційно малою імовірністю помилки. Цей результат було скомбіновано з результатом твердження 3 для побудови імовірнісного алгоритму відновлення розв'язку. Оскільки кількість звернень до оракула у звідності за Тюрінгом є поліноміальною, то запропонований алгоритм буде теж поліноміальним від довжини вхідних даних. Помилка у разі декількох викликів алгоритму перевірки існування розв'язків буде накопичуватись, але кількість таких викликів є поліноміальною, а зі збільшенням d помилка зменшується експоненційно, тому можна обрати значення d таким чином, щоб запобігти накопиченню помилки.

Висновки

У даній роботі було формалізовано задачу відновлення невідомого вектору за певною частковою інформацією про лінійні співвідношення над його координатами. У результаті цього було визначено окремий математичний об'єкт – систему лінійних заборон над скінченним полем. Виявилось, що за своєю структурою множина розв'язків системи лінійних заборон з нульовими правими частинами складається з набору класів еквівалентності, які породжені відношенням пропорційності. Доведено, що задачі перевірки існування та пошуку розв'язку системи лінійних заборон є еквівалентними за Тюрінгом. Для часткових випадків сформульовано окремі задачі та показано, що вони належать відповідним класам складності в залежності від типу умов, накладених на вхідні дані. Для випадку обмеженої кількості заборон в системі було запропоновано поліноміальний імовірнісний алгоритм із односторонньою помилкою, імовірність якої не перевищує 0,5 при однократному запуску.

Список використаних джерел

1. Bard G.V. Algebraic Cryptanalysis / Gregory V. Bard. – Springer Science+Business Media, LLC, 2009. – 368 pp. – ISBN 978-0-387-88756-2.

2. Goldreich O. Computational Complexity: A Conceptual Perspective / Oded Goldreich. – New York: Cambridge University Press, 2008. – 632 с.

3. Arora S. Computational Complexity: A Modern Approach / S. Arora, B. Barak. – New York: Cambridge University Press, 2009. – 608 с.