Кайдан Н.В., Остимчук Г.С.

[1]Аспірантка механіко-математичного факультету Київського національного університету ім. Тараса Шевченка,
[2]Асистент кафедри алгебри СДПУ

Застосування циклічних кодів в теорії кодування

В статті розглянута історія виникнення кодів, питання побудови кодуючих і декодуючих пристроїв, а також питання загальної теорії лінійних та циклічних кодів.

Ключові слова: *лінійні коди, циклічні коди, скінченне поле.*

Коди з'явилися в глибокій старовині у вигляді криптограм (по-грецьки – тайнопису), коли ними користувалися для засекречування важливого повідомлення від тих, кому воно не було призначене. Вже відомий грецький історик Геродот (V століття до н. е.) наводив приклади листів, зрозумілих лише для одного адресата. Спартанці мали спеціальний механічний прилад, за допомогою якого важливі повідомлення можна було писати особливим способом, що забезпечує збереження таємниці. Власна секретна азбука була у Юлія Цезаря. В середні віки і епоху Відродження над винаходом таємних шифрів працювало багато видатних людей, в їх числі філософ Френсис Бекон, крупні математики Франсуа Вієт, Джероламо Кардано, Джон Валліс.

З часом почали з'являтися по-справжньому складні шифри. Один з них, що вживається і понині, пов'язаний з ім'ям вченого абата з Вюрцбурга Трітеміуса, якого до занять криптографією спонукала, мабуть, не тільки монастирська самота, але і потреба зберігати від розголосу деякі духовні таємниці. Різні хитромудрі прийоми кодування застосовували шифрувальники при папському дворі і дворах європейських королів. Разом з мистецтвом шифрування розвивалося і мистецтво дешифровки, або, як кажуть, криптоаналізу.

У завдання кодування входить зовсім не засекречування повідомлень, а інша мета: зробити передачу повідомлень швидкою, зручною і надійною. Призначений для цієї мети кодуючий пристрій зіставляє кожному символу тексту, який передається, а іноді і цілим словам або фразам (повідомленням) певну комбінацію сигналів (прийнятну для передачі по даному каналу зв'язку), звану кодом або кодовим словом. При цьому операцію перекладу повідомлень в певні послідовності сигналів називають кодуванням, а зворотну операцію, що поновлює по прийнятих сигналах (кодовим словам) повідомлення, яке передавали, – декодуванням.

Відмітимо відразу ж, що різні символи або повідомлення повинні кодуватися різними кодовими словами, інакше за кодовими словами не можна було б відновити повідомлення, які передавали.

Історично перший код, призначений для передачі повідомлень, пов'язаний з ім'ям винахідника телеграфного апарату Семюеля Морзе і відомий всім як азбука Морзе. У цьому коді кожній букві або цифрі зіставляється своя послідовність з короткочасних (званих крапками) і тривалих (тире) імпульсів струму, що розділяються паузами. Інший код, також широко поширений в телеграфії (код Бодо), використовує для кодування два елементарні сигнали – імпульс і паузу, при цьому кодові слова, що зіставляються буквам, складаються з п'яти таких сигналів.

Коди, що використовують два різні елементарні сигнали, називають двійковими. Зручно буває, відволікаючись від їх фізичної природи, позначати ці два сигнали символами 0 і 1. Тоді кодові слова можна представляти як послідовності з нулів і одиниць.

Перший хто зрозумів, що для кодування досить два символи, був Френсис Бекон. Двійковий код, який він використовував в криптографічних цілях, містив п'ятирозрядні (як і в коді Бодо) слова, складені з символів 0, 1.

Коди з перевірками на парність називають *лінійними кодами* (двійкові лінійні коди називають також *груповими).* Якщо кодовий підпростір в просторі L_n має розмірність k, то використовують для більшої визначеності термін лінійний (n, k)-код.

Є дуже багато причин, по яких лінійні коди є найважливішими в теорії кодування. Одна з них пов’язана зі зручностями у виявленні і виправленні помилок. Інша причина – це можливість компактного задання коду. Дійсно, у разі лінійного коду немає необхідності вказувати повний список кодових слів, адже код цілком визначений системою лінійних рівнянь:

$$\begin{aligned} &b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n}x_n = 0,\\ &b_{21}x_1 + b_{22}x_2 + \ldots + b_{2n}x_n = 0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &b_{m1}x_1 + b_{m2}x_2 + \ldots + b_{mn}x_n = 0 \end{aligned}$$

або матрицею цієї системи *(перевірочною матрицею)*:

$$H = \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{m1} & b_{m2} & \ldots & b_{mn} \end{pmatrix}.$$

Надалі ми припускатимемо, що рядки цієї матриці лінійно незалежні.

До інших переваг лінійних кодів, які пов'язані з попередніми, відносяться прості алгоритми кодування і декодування, що легко реалізуються електронними схемами перемикачів. Взагалі, можна сказати, що бурхливий розвиток теорії кодування, який відбувався в останні десятиліття, пояснюється головним чином тим, що до лінійних кодів прикладений добре розвинений апарат лінійної алгебри і теорії скінченних полів.

Серед лінійних кодів особливо важливу роль грають так звані *циклічні коди.* З ряду причин вони є найбільш цінним надбанням теорії кодування. По-

перше, вони допускають ще компактніший опис, ніж довільні лінійні коди. По-друге, алгоритми кодування і декодування, що є для лінійних кодів, можуть бути в застосуванні до циклічних кодів значно спрощені; більш того, для циклічних кодів існують свої особливі методи декодування, які не можна застосувати до інших лінійних кодів. Нарешті, по своїй структурі ці коди ідеально пристосовані до реалізації в сучасних технічних пристроях.

Серед циклічних кодів особливу практичну важливість має один спеціальний клас кодів, запропонованих американськими математиками Боузом, Чоудхурі і Хоквінгемом. Ці коди так і називаються кодами БЧХ – за початковими буквами прізвищ цих математиків. Теорія кодів БЧХ виходить за рамки цієї статті, і ми тільки пояснимо в декількох словах, яким чином вони визначаються. Для цього нам буде потрібно деякі додаткові відомості з теорії полів.

Говоритимемо, що підмножина F є підполем поля $\overline{F}$, якщо F є поле щодо операцій на $\overline{F}$. Справедлива така теорема:

Для будь-якого скінченного поля F можна вказати скінченне поле $\overline{F}$, що задовольняє наступним умовам:

1. *F є підполе поля $\overline{F}$;*
2. *$\overline{F}$ містить n коренів рівняння $X^n - 1 = 0$;*
3. *не існує поля, яке задовольняє властивостям 1 і 2 і що має менше елементів, ніж $\overline{F}$.*

Нехай тепер для поля F вказано поле $\overline{F}$ з властивостями 1–3. Нехай α – примітивний елемент поля $\overline{F}$, а числа s і l такі, що елемент α^s має порядок n і $s + l < q$, де q – число елементів поля $\overline{F}$. *Циклічний* код називається кодом БЧХ (з параметрами n, s, l), якщо він складається зі всіх многочленів степеня $\le n-1$ з коефіцієнтами із F, серед коренів яких містяться всі елементи.

$$\alpha^s,\ \alpha^{s+1},\ \alpha^{s+2},...,\alpha^{s+l}.$$

Можна довести, що кодова відстань такого коду не менша $l+2$. Отже, варіюючи параметри n, s, l, ми маємо можливість отримувати коди БЧХ з будь-якою відстанню, тобто ті, які виправляють будь-яке задане число помилок. Це доповнюється тим, що для вказаних кодів розроблені зручні алгоритми декодування, засновані на обчисленнях в скінченних полях і що легко реалізовуються автоматичними електронними пристроями.

Література

1. *Аршинов М.Н., Садовский Л.Е.* Коды и математика. – М.: Наука, Главная редакция физико-математической литературы, 1983. – 144 с.
2. *Берлекэмп Э.* Алгебраическая теория кодирования. – М.: Мир, 1971. – 479с.
3. *Венбо Мао* Современная криптография: теория и практика.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 768 с.: ил. – Парал. тит. англ.
4. *Касами Т., Токура Н., Ивадари Е., Инагаки Я.* Теория кодирования. – М.: Мир, 1978. – 576 с.