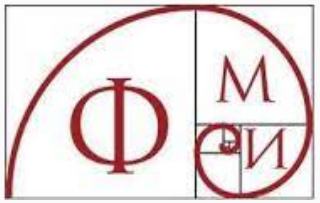
:q ls

БЧХ кодове

Кристиян Стоименов

23 септември 2023 г.



Факултет по математика и информатика,

Увод в теорията на кодирането

Съдържание

История

- БЧХ кодовете са открити от Bose и Ray-Chaudhuri с [BR60], както и независимо от Hocquenghem в [HOC59].
- По първоначалните резултати употребата се свежда единствено до бинарни кодове с дължина на кодовите думи $2^m - 1, m \in \mathbb{Z}$.
- Впоследствие Gorenstein и Zierler в [GZ61] разширяват способностите му до $GF(q)$, което в последствие се свързва с развитие на Reed-Solomon кодовете.

Dijen K. Ray-Chaudhuri - математик, чието име се свързва най-често с решението на т.нар задача на Kirkman за ученичката.

Raj Chandra Bose (1901 - 1987) - индийско-американски математик, известен най-вече с ролята си в развитието на БЧХ кодовете и понятието силно свързан граф.

Какво е БЧХ код?

Дефиниция

Нека n и q са взаимно прости числа, а F_{q^m} е разширание на F_q, което съдържа всички n корена на полинома $x^n - 1$. Нека също α е примитивен n-ти корен на 1 над полето F_q. БЧХ код над F_q с дължина n и конструктивно разстояние δ е цикличен код с дължина n и пораждащ полином

$$g(x) = [M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \ldots, M_{\alpha^{b+\delta-2}}(x)],$$

където M_{α^s} е минималния полином на елемента α^s над F_q.

Дефиниция

Нека n и q са взаимно прости числа, а F_{q^m} е разширание на F_q, което съдържа всички n корена на полинома $x^n - 1$. Нека също α е примитивен n-ти корен на 1 над полето F_q. БЧХ код над F_q с дължина n и конструктивно разстояние δ е цикличен код с дължина n и пораждащ полином

$$g(x) = [M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \ldots, M_{\alpha^{b+\delta-2}}(x)],$$

където M_{α^s} е минималния полином на елемента α^s над F_q.

Дефиниция

Нека n и q са взаимно прости числа, а F_{q^m} е разширание на F_q, което съдържа всички n корена на полинома $x^n - 1$. Нека също α е примитивен n-ти корен на 1 над полето F_q. БЧХ код над F_q с дължина n и конструктивно разстояние δ е цикличен код с дължина n и пораждащ полином

$$g(x) = [M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \ldots, M_{\alpha^{b+\delta-2}}(x)],$$

където M_{α^s} е минималния полином на елемента α^s над F_q.

Дефиниция

Нека n и q са взаимно прости числа, а F_{q^m} е разширание на F_q, което съдържа всички n корена на полинома $x^n - 1$. Нека също α е примитивен n-ти корен на 1 над полето F_q. БЧХ код над F_q с дължина n и конструктивно разстояние δ е цикличен код с дължина n и пораждащ полином

$$g(x) = [M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \ldots, M_{\alpha^{b+\delta-2}}(x)],$$

където M_{α^s} е минималния полином на елемента α^s над F_q.

Дефиниция

Нека n и q са взаимно прости числа, а F_{q^m} е разширание на F_q, което съдържа всички n корена на полинома $x^n - 1$. Нека също α е примитивен n-ти корен на 1 над полето F_q. БЧХ код над F_q с дължина n и конструктивно разстояние δ е цикличен код с дължина n и пораждащ полином

$$g(x) = [M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \ldots, M_{\alpha^{b+\delta-2}}(x)],$$

където M_{α^s} е минималния полином на елемента α^s над F_q.

Дефиниция

Нека n и q са взаимно прости числа, а F_{q^m} е разширание на F_q, което съдържа всички n корена на полинома $x^n - 1$. Нека също α е примитивен n-ти корен на 1 над полето F_q. БЧХ код над F_q с дължина n и конструктивно разстояние δ е цикличен код с дължина n и пораждащ полином

$$g(x) = [M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \ldots, M_{\alpha^{b+\delta-2}}(x)],$$

където M_{α^s} е минималния полином на елемента α^s над F_q.

Да се опитаме да го дешифрираме.

Корени на 1

Дефиниция

Ако $n \in \mathbb{N}$, то корените на полинома $x^n - 1$ се наричат *n-ти корени на единицата.*

Корени на 1

Дефиниция

Ако $n \in \mathbb{N}$, то корените на полинома $x^n - 1$ се наричат *n-ти корени на единицата.*

Можем да забележим обаче, че за фиксирано n всички корени са числата

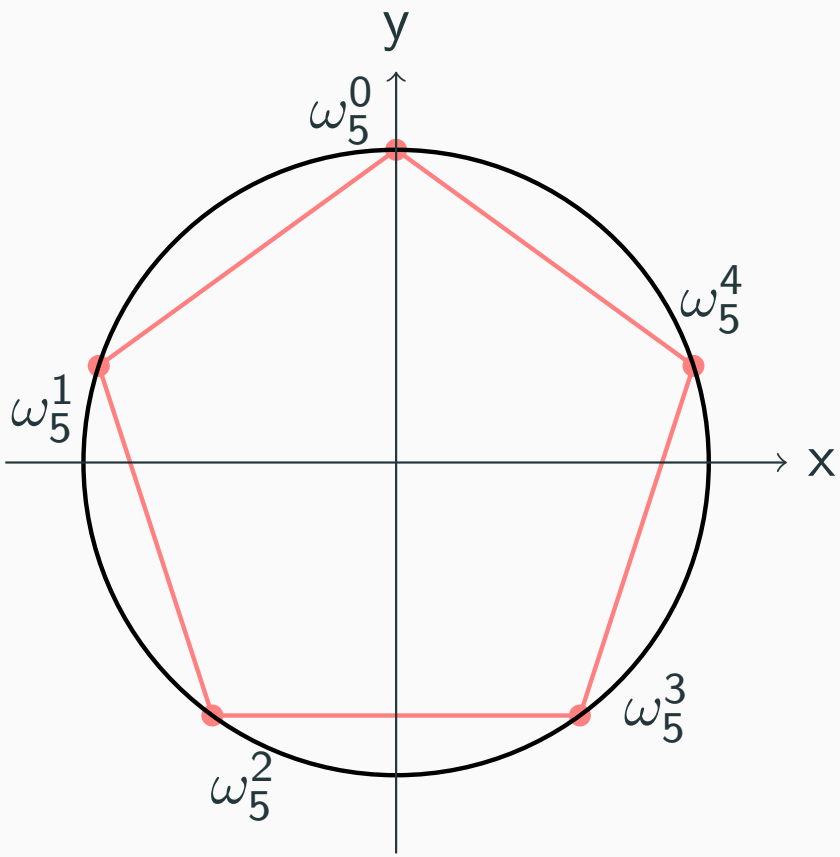
$$\omega^0, \omega^1, \omega^2, \ldots, \omega^{n-1}$$

при

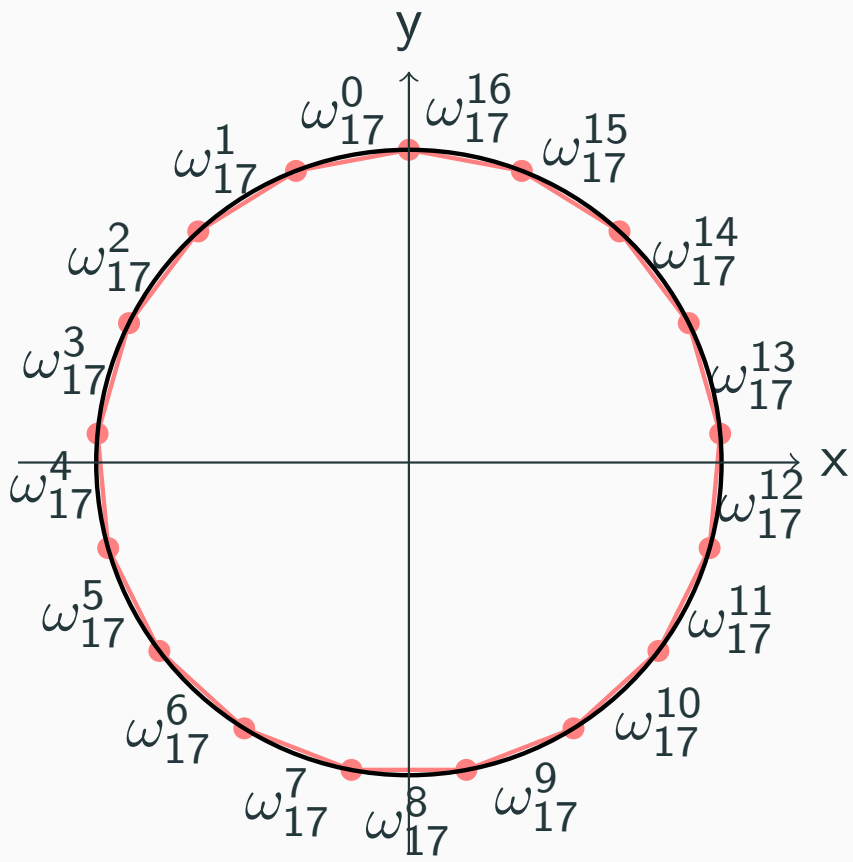
$$\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$

Корени на 1

И така получаваме точно елементите на цикличната група $\mathbb{C}_n$.



Цикличната група $\mathbb{C}_5$



Цикличната група $\mathbb{C}_{17}$

Корени на 1

За да си обясним какво означава, че корените са *примитивни*, е необходимо да използваме и следното понятие:

Дефиниция

Нека α е n-ти корен на 1. Казваме, че α принадлежи на *показател* d, ако

$$\begin{cases} \alpha^d = 1 \\ \alpha^m \neq 1 \quad 0 < m < d \end{cases}$$

т.е показателят е редът на елемента $\alpha \in \mathbb{C}_n$.

Корени на 1

Тогава

Дефиниция

Ако α принадлежи на показател n, ще казваме, че е *примитивен n-ти корен на 1*.

т.е α е примитивен n-ти корен на 1 *тстк* $\mathbb{C}_n = \langle \alpha \rangle$.

Конструктивно разстояние δ

Това понятие се основава на следното важно твърдение, известно още като БЧХ граница:

Теорема
Нека α е примитивен корен на 1 над полето F_q. Ако C е цикличен код с дължина n и пораждащ $g(x)$, за който

$$\exists \delta, b \in \mathbb{Z},$$

такива че

$$g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0,$$

тогава $d(C) >= \delta$.

Минимален полином на елемент над поле

Припомняме, че ако F_q е подполе на $\mathbb{C}$, $F_q < \mathbb{C}$, то число $\alpha \in \mathbb{C}$ наричаме *алгебричен елемент* F_q, ако α е корен на ненулев $f \in F_q[x]$.

Всеки такъв алгебричен елемент си има специален полином, зададен от следната

Дефиниция

Ненулевият полином от най-ниска степен, на който α е корен и който е унитарен[1], се нарича *минимален полином на α над F_q*.

[1] Със старши коефициент единица.

Цикличен код

Последното понятие, използвано в определението на БЧХ кодове, което не сме припомнили досега, е *цикличен код*. Макар, че вече го използвахме неведнъж, го споменаваме накратко, тъй като това е по-общия клас, в който попада класът на БЧХ кодовете по същия начин както цикличните кодове са по-тесен клас на линейните блокови.

Това означава, че всеки алгоритъм за кодиране и декодиране, свойства и граници на циклични кодове важи в пълна степен и за БЧХ кодовете, които от своя страна поради особеностите си предоставят по-ефикасни методи и по-ясни свойства.

Цикличен код

Дефиниция

Цикличен код е вид линеен код, за който важи следното свойство. Ако C е цикличен код, то

$$\forall c = (a_0, a_1, \ldots, a_{n-1}) \in C \implies c' = (a_{n-1}, a_0, \ldots, a_{n-2}) \in C.$$

Някои от по-интересните свойства, които БЧХ кодовете "наследяват", поради своята цикличност включват

- съществуване на пораждащ полином,
- способност за систематично и несистематично кодиране единствено чрез действия с полиноми,
- възможност за декодиране чрез декодера на Мегит.

Свойства на БЧХ кодовете

Общо за БЧХ кодовете

- Основната идея на този вид кодове е, че те са циклични кодове, които се определят от корените на своя пораждащ полином.
- Тяхната главна цел е чрез пораждащия полином $g(x)$ и началната стойност b, поставена за степен на α, да се зададе такова конструктивно разстояние δ, че да се състави код със способност за поправяне на повече на брой грешки.

Процедура за получаване на БЧХ код

Нека разгледаме основните стъпки при конструиране на БЧХ код със способност за поправяне на t грешки над поле $GF(q)$.

1. Търсим примитивен n-ти корен на единицата в разширение на $GF(q) < GF(q^m)$ (възможност най-малкото такова).
2. Избираме $\delta - 1 = 2t$, последователни степени на α, започващи от α^b, $b \in \mathbb{Z}^+$ - корени на
3. $g(x) \in GF(q)[x]$ - НОК на минималните полиноми на избраните степени на α спрямо $GF(q)$.

Циклотомични класове

Преди да можем да разгледаме пример за БЧХ кодове трябва да въведем още едно понятие, което се основава на следната

Лема

Нека F_{q^m} е разширение на F_q, $F_q < F_{q^m}$. Ако $f \in F_q[x]$ и $\beta \in F_{q^m}$ е такъв че $f(\beta) = 0$, то тогава и $f(\beta^q) = 0$.

Следствие

Ако α^i е корен на неразложим полином, то тогава α^{iq} също е корен за α - примитивен n-то корен на 1 над F_q.

Тогава

Дефиниция

Циклотомичен клас относно q по модул n, определен от i, се нарича множеството от остатъци при деление на n

$$\mathcal{C}_i := \{i, iq, \ldots, iq^{s-1}\} \pmod{n}.$$

т.е всички степени на α от един и същи циклотомичен клас са корени на един и същ минимален полином.

За двата основни вида БЧХ кодове

Съществуват следни два основни вида БЧХ кодове:

- т.нар **narrow-sense**, за които имаме $b = 1$ и
- **примитивни**, за които $n = q^m - 1$.

Едно от най-важните свойства на БЧХ кодовете е следното твърдение за примитивните такива:

Теорема

За всеки две целочислени mt, такива че $t <= 2^{m-1} - 1$ съществува БЧХ код над полето $GF(2)$ с дължина $n = 2^m - 1$, който има способност да поправи до t на брой грешки.

Пример (Narrow-sense БЧХ код)

Пример (Примитивен БЧХ код)

За минимално разстояние на БЧХ код

- Както забелязваме, понякога се случва така, че БЧХ границата не ни дава съвсем точна представа за минималното разстояние на кода, с който работим.
- Тогава се налага да направим допълнителен анализ за да се открие *действителната* стойност на $d(C)$.
- Един подход за това е представен в [LW86].

Относно преимуществата на БЧХ кодовете

- Както вече видяхме, едно от основните предимства на БЧХ кодовете е възможността за конструиране на код, който поправя до t грешки според теоремата за примитивни БЧХ кодове.
- Другата важна тяхна характеристика е наличието на много ефикасен алгоритъм за декодиране.

Алгоритъм за декодиране на Peterson–Gorenstein–Zierler

Приложения

БЧХ кодовете срещат голяма популярност, поради свойствата, които притежават. Друг фактор, който трябва да се вземе предвид е, че те са обобщение на Reed-Solomon кодовете [RS60], при които двете полета $GF(q)$ и $GF(q^m)$ съвпадат, т.е се разглеждат при $m = 1$. Така, освен конкретните употреби на БЧХ кодове, трябва да се включи и разпространението на Reed-Solomon кодовете.

Някои конкретни примери за употреба на БЧХ в практиката:

- Според [CP88] БЧХ кодовете са един от способите, използвани за шумозащитно кодиране в мисията за *Phobos Lander*.
- Намират приложение и в новоразвиващата се сфера на т.нар quantum-resistant криптография - [Mel20].
- Употребата им в реализацията на flash памети се счита за стандартна - [MM18].

Литература

[BR60] R.C. Bose и D.K. Ray-Chaudhuri. **“On a class of error correcting binary group codes”.** B: *Information and Control* 3.1 (1960), с. 68—79. ISSN: 0019-9958. DOI: https://doi.org/10.1016/S0019-9958(60)90287-4. URL: https://www.sciencedirect.com/science/article/pii/S0019995860902874.

[CP88] K. M. Cheung и F. Pollara. **“Phobos Lander Coding System: Software and Analysis”.** B: *Communications Systems Research* (1988). URL: https://ipnpr.jpl.nasa.gov/progress_report/42-94/94V.PDF.

[GZ61] Daniel Gorenstein и Neal Zierler. **“A Class of Error-Correcting Codes in pm Symbols”.** B: *Journal of the Society for Industrial and Applied Mathematics* 9.2 (1961), с. 207—214. DOI: 10.1137/0109020. eprint: https://doi.org/10.1137/0109020. URL: https://doi.org/10.1137/0109020.

[HOC59] A. HOCQUENGHEM. **“Codes correcteurs d’erreurs”.** B: *Chiffers* 2 (1959), с. 147—156. URL: https://cir.nii.ac.jp/crid/1573387450087403264.

[LW86] Jacobus H. van Lint и Richard M. Wilson. **“On the minimum distance of cyclic codes”.** B: *IEEE Trans. Inf. Theory* 32 (1986), с. 23—40. URL: https://api.semanticscholar.org/CorpusID:24903470.

[Mel20] Carlos A. Melchor. **“Hamming Quasi-Cyclic (HQC)”.** B: (2020). URL: https://pqc-hqc.org/doc/hqc-specification_2020-05-29.pdf.

[MM18] Alessia Marelli и Rino Micheloni. **“BCH Codes for Solid-State-Drives”.** B: *Inside Solid State Drives (SSDs)*. Под ред. на Rino Micheloni, Alessia Marelli и Kam Eshghi. Singapore: Springer Singapore, 2018, с. 369—406. ISBN: 978-981-13-0599-3. DOI: 10.1007/978-981-13-0599-3_11. URL: https://doi.org/10.1007/978-981-13-0599-3_11.

[Moo05] Todd K. Moon. **“BCH and Reed-Solomon Codes: Designer Cyclic Codes”.** B: *Error Correction Coding*. John Wiley & Sons, Ltd, 2005. Гл. 6, с. 235—292. ISBN: 9780471739210. DOI: https://doi.org/10.1002/0471739219.ch6. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/0471739219.ch6. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/0471739219.ch6.

[Ple98] Vera Pless. **“Bose-Chaudhuri-Hocquenghem (BCH) Codes”.** B: *Introduction to the Theory of Error-Correcting Codes*. John Wiley & Sons, Ltd, 1998. Гл. 7, с. 109—222. ISBN: 9781118032749. DOI: https://doi.org/10.1002/9781118032749.ch7. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118032749.ch7. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118032749.ch7.

[RC99] Irving S. Reed и Xuemin Chen. **“BCH Codes”.** В: *Error-Control Coding for Data Networks*. Boston, MA: Springer US, 1999, с. 189—231. ISBN: 978-1-4615-5005-1. DOI: 10.1007/978-1-4615-5005-1_5. URL: https://doi.org/10.1007/978-1-4615-5005-1_5.

[RS60] I. S. Reed и G. Solomon. **“Polynomial Codes Over Certain Finite Fields”.** В: *Journal of the Society for Industrial and Applied Mathematics* 8.2 (1960), с. 300—304. DOI: 10.1137/0108018. eprint: https://doi.org/10.1137/0108018. URL: https://doi.org/10.1137/0108018.

[Вел01] Евгения Великова-Бандова. ***Записки по кодиране: Циклични кодове.*** 2001.

[Вел04] Евгения Великова-Бандова. ***Записки по кодиране: Двоични шумозащитни кодове.*** 2004.

Благодаря за вниманието!