Софийски Университет "Св. Климент Охридски"

Факултет по Математика и Информатика

ДИПЛОМНА РАБОТА

на

Николай Борисов Матеев

Ф.№ 9426

Радиуси на покритие и спектри на лидерите на съседни класове на двоични линейни кодове

Научен ръководител:

/доц. Красимир Манев/

София, 1994г.

Съдържание

Увод **2**

1 Линейни кодове и минимален радиус на покритие **4**

1.1 Линейни кодове . . . 4
1.2 Нормални кодове . . . 5
1.3 Радиус на покритие. Основни граници. Конструкции на нови кодове . . . 6
1.4 Минимален радиус на покритие . . . 8
1.5 Таблица за $t[n, k]$ при $n \leq 64$ . . . 9

2 Минимален радиус на покритие на самодопълнителни кодове **16**

2.1 Самодопълнителни линейни кодове . . . 16
2.2 Основни граници за минималния радиус на покритие на самодопълнителни кодове . . . 16
2.3 Самодопълнителни кодове с размерност шест . . . 19
2.3.1 Метод на търсене . . . 20
2.3.2 Изчисления и резултати . . . 23
2.4 Таблица за $t^s[n, k]$ при $n \leq 64$ . . . 26

3 Спектър на лидерите на съседни класове за кодове с повтарящи се координати **33**

3.1 Произволни двоични линейни кодове . . . 33
3.2 Самодопълнителни кодове . . . 35
3.3 Оценки за сложността на пресмятане на $\{L_i\}$ . . . 37

Библиография **38**

Увод

През последните четиридесет години основна концентрация на теорията на кодирането са били оптимизационни задачи, включващи трите параметъра на линейните кодове—дължината n, размерността k и минималното разстояние d. Някои конкретни задачи са максимизирането на k и d (за фиксирано n) и намирането на линейни $[n, k, d]$ кодове с прости алгоритми за декодиране. Напоследък обаче се наблюдава нарастващ интерес към кодове с оптимален радиус на покритие [5]. Установено е, че радиусът на покритие е основен геометричен параметър на кода и има множество важни приложения (виж Коен и др. [5]). След излизането на обзорната статия [5] през 1985г. следва бурно развитие в областта на *покриващите кодове*—ново понятие, въведено за контраст с *кодове, поправящи грешки*. Също през 1985г. Греъм и Слоен [9] въвеждат понятието *норма* на код, помагащо при изследването на радиуса на покритие, и публикуват единствената досега таблица за известните стойности на $t[n, k]$—минималния радиус на покритие на $[n, k]$ кодове, при $n \leq 64$. От 1985г. насам се отделя голямо внимание на покриващите кодове, отделена им е дори собствена класификация (94B65) в *1980 Mathematics Subject Classification (1990 Revision)*.

Настоящата дипломна работа е посветена на въпроси, свързани с радиуса на покритие.

В първа глава са дадени основните сведения от теорията на кодирането, необходими за работата ни, и е направен обзор на основните конструкции за получаване на оптимални покриващи кодове. Таблицата за $t[n, k]$ от [9] е актуализирана с всички известни ни подобрения, като в процеса на работа са получени и нови 3 долни и 3 горни граници.

Във втора глава са разгледани самодопълнителните кодове. През 1985г. Коен и др. [5] поставят въпроса дали $t[n, k]$ винаги се достига и от самодопълнителни кодове. През 1988г. Ст. Додунеков, Кр. Манев и Вл. Тончев отговарят отрицателно, доказвайки, че $t[14, 6] = 3$ не се достига от самодопълнителни кодове. Въпросът в общия случай обаче остава открит и ние го изследваме в тази глава. Дефинираме $t^s[n, k]$—минимален радиус на покритие на самодопълнителни $[n, k]$ кодове. Основният резултат е определянето на точните стойности на $t^s[n,k]$ при $k \leq 6$ и всяко n. Построяваме и таблица за границите на $t^s[n,k]$ при $n \leq 64$.

В трета глава е разгледана задачата за намиране тегловото разпределение на лидерите на съседни класове. Освен теоретично значение, то има и важно практическо приложение—ако го знаем, можем да определим вероятността за допускане на грешка при декодиране по максимално правдоподобие. Намирането на това разпределение е трудна задача ($\prod_2^n$-пълна) и изчисленията по стандартно използвания метод са невъзможни дори и при кодове с малки размерности. За кодове с повтарящи се координати обаче доказваме твърдения, позволяващи ни да построим добър алгоритъм.

Към дипломната работа са приложени листинги на всички програми, използвани в глави втора и трета. За изчисленията бяха използвани компютри IBM PC 486DX и DEC 3100.

Изказвам искрена благодарност на научния си ръководител доц. Красимир Манев за предложената интересна тема и за помощта, която ми бе оказана. Благодаря и на всички, които по един или друг начин помогнаха за написването на тази дипломна работа.

Глава 1

Линейни кодове и минимален радиус на покритие

1.1 Линейни кодове

Нека F_2^n е n-мерното векторно пространство над крайното поле с два елемента F_2. *Двоичен линеен код* с блокова дължина n и размерност k ($[n,k]$ код) наричаме всяко k-мерно подпространство на F_2^n.

Нека $u, v \in F_2^n$. *Разстояние на Хеминг* $\mathrm{dist}(u,v)$ между u и v наричаме броя координатни позиции, в които u и v се различават. *Минимално разстояние* на кода C наричаме $d = \min\{\mathrm{dist}(u,v) \mid u, v \in C, u \neq v\}$. *Тегло на Хеминг* на вектора u наричаме разстоянието от u до нулевия вектор, т.е. $\mathrm{wt}(u) = \mathrm{dist}(u, 0)$. Тъй като C е линейно подпространство на F_2^n, то минималното тегло на C е равно на минималното ненулево тегло на вектор от C. *Радиус на покритие* на кода C наричаме най-малкото цяло число $R = R(C)$, такова че сферите с радиус R, описани около кодовите думи, покриват цялото пространство F_2^n.

С $[n,k,d]R$ ще означаваме двоичен линеен код с блокова дължина n, размерност k, минимално разстояние d и радиус на покритие R. Два кода C_1 и C_2 са *еквивалентни*, ако могат да се получат един от друг чрез пермутация на координатните позиции. За еквивалентни кодове n, k, d и R съвпадат.

Нека C е $[n,k]$ код и нека a_1, a_2, …, a_k е базис на C като линейно пространство. Матрицата $G = (a_1, a_2, \ldots, a_k)^T$, където T означава транспониране, се нарича *пораждаща матрица* на C.

Кодът $C^\perp = \{u \in F_2^n \mid u \cdot c = 0, c \in C\}$, където $u \cdot v = \sum_{i=1}^n u_i v_i$ е скаларното произведение на векторите u и v, се нарича *дуален (ортогонален)* на C. Пораждащите матрици за кода $C^\perp$ се наричат *проверочни матрици* за кода C. Ако H е проверочна матрица за C, то $Hc^T = 0, \ \forall c \in C$ и $C = \{c \in F_2^n \mid Hc^T = 0\}$. Тъй като $\dim C + \dim C^\perp = n$, то $C^\perp$ е $[n, n-k]$ код.

Ако пораждащата матрица G на кода C е преобразувана във вида $G = (I_k \mid A)$, където I_k е единичната $k \times k$ матрица, казваме, че C е зададен в *систематичен вид*. В този случай имаме $H = (-A^T \mid I_{n-k})$.

1.2 Нормални кодове

Нека C е двоичен линеен код с дължина n, размерност k и радиус на покритие R, т.е. $[n,k]R$ код. Нека i е коя да е от n-те координати. С $C_0^{(i)}$ означаваме множеството от кодови думи, за които i-тата координата е 0, а с $C_1^{(i)}$—тези, за които е 1. Можем да считаме, че множеството $C_1^{(i)}$ не е празно, в такъв случай и $C_0^{(i)}$, и $C_1^{(i)}$ съдържат по 2^{k-1} кодови думи [15]. За всяка двоична n-торка x, нека

$$\begin{aligned} f_0(x) &= \operatorname{dist}(x, C_0^{(i)}) = \min_{c \in C_0^{(i)}} \operatorname{dist}(x,c), \\ f_1(x) &= \operatorname{dist}(x, C_1^{(i)}). \end{aligned}$$

Тогава

$$N^{(i)} = \max_x \{f_0(x) + f_1(x)\} \tag{1.1}$$

се нарича *норма на C по отношение на i-тата координата*, а

$$N = \min_i N^{(i)} \tag{1.2}$$

се нарича *норма* на C. Координатните позиции i, за които $N = N^{(i)}$, се наричат *приемливи*. Кодът се нарича *нормален*, ако

$$N \leq 2R + 1. \tag{1.3}$$

Ако вземем всички кодови думи от C, чиято първа координата е 0 (считайки, че това не е целия код C) и отстраним тази координата от тези кодови думи, получаваме $[n-1, k-1, d_s]$ *скъсен (shortened) код* C_s (за който $d_s \geq d$). Проверочна матрица за C_s можем да получим, като махнем първата колона от проверочна матрица за C. Коен, Лобстейн и Слоен [6] дават следното достатъчно условие за нормалност:

Твърдение 1.1 *Нека R_s е радиусът на покритие на скъсения код C_s, получен от двоичния линеен код C. Ако $R_s \leq R+1$, то C е нормален.*

Други достатъчни условия за нормалност могат да бъдат намерени в редица статии, започвайки от Греъм и Слоен [9], където е доказано, че всички $[n,k]$ кодове с $n \leq 8$ или $k \leq 2$ са нормални. Тези резултати са разширени в Коен, Лобстейн и Слоен [6] и Слоен [20], а най-новите подобрения са в Килби и Слоен [14], Дафърти и Янва [8] (там цитират Янва и Метсон [13]), и ван Вии [23]:

Твърдение 1.2 *Двоичният линеен $[n,k,d]R$ код C е нормален, ако $n \leq 14$, или $k \leq 5$, или $d \leq 5$, или $R \leq 2$ [14], или $n = 15$, или $n-k \leq 8$ [13], или $d = 2R$, или $d = 2R+1$ [23].*

1.3 Радиус на покритие. Основни граници. Конструкции на нови кодове

Нека C е двоичен $[n,k]$ код и $x \in F_2^n$. $x + C = \{x + c \,|\, c \in C\}$ се нарича *съседен клас* на кода C. По този начин пространството F_2^n се разбива на 2^{n-k} непресичащи се съседни класа, всеки с по 2^k елемента. *Лидер на съседен клас* наричаме вектор от този съседен клас с минимално тегло.

За двоични кодове радиусът на покритие $R(C)$ на кода C е

$$R(C) = \max\{\min\{\mathrm{dist}(x,c) \,|\, c \in C\} \,|\, x \in F_2^n\}. \tag{1.4}$$

Когато кодът C е линеен, радиусът на покритие е равен на теглото на най-тежкия лидер на съседен клас. Също така, в сила е следното твърдение:

Твърдение 1.3 *[5] Ако H е проверочна матрица за кода C, то $R(C)$ е най-малкото цяло число, за което всеки синдром е сума на не повече от $R(C)$ колони от H.* (Под *синдром* разбираме произволна колона над F_2 с дължина $n-k$).

Сега ще дадем някои граници за радиуса на покритие, взети от [5], необходими в по-нататъшната ни работа.

Твърдение 1.4 (Граница на сферичното покритие) *[5] Ако C е $[n,k]$ код с радиус на покритие R, то*

$$2^{n-k} \le \sum_{i=0}^{R} \binom{n}{i}. \tag{1.5}$$

Кодът C се нарича *четен*, ако всички вектори в C са с четно тегло. Ако кодът е четен, то половината негови съседни класове имат четно, а другата половина—нечетно тегло. Затова е в сила

Твърдение 1.5 *[5] Ако кодът C е четен, то*

$$\sum_{2i \le R} \binom{n}{2i} \ge 2^{n-k-1} \qquad \text{и} \qquad \sum_{2i+1 \le R} \binom{n}{2i+1} \ge 2^{n-k-1}. \tag{1.6}$$

Твърдение 1.6 *[5] Удължаването на кода с обща проверка по четност или с добавяне на нулева координата увеличава радиуса на покритие с единица. Премахването на p координати намалява радиуса на покритие най-много с p.*

Да означим с C_p кодът, получен от C чрез премахване на първата координата (C_p се нарича *скъсен чрез премахване на координата (punctured) код*, и нека $R_p := R(C_p)$.

Лема 1.1 *За радиуса на покритие на скъсения чрез премахване на координата код е в сила $R(C) - 1 \leq R_p \leq R(C)$. Ако $R_p = R(C)$ и кодът C е нормален, то C_p също е нормален (стига поне една от приемливите координати на C да остава).*

Доказателство $R(C)-1 \leq R_p \leq R(C)$ следва непосредствено от Твърдение 1.6. Нека C е нормален код и последната му координата е приемлива. Премахваме първата координата. От дефиницията за норма е ясно, че $N(C_p) \leq N(C)$. Тогава $N(C_p) \leq N(C) \leq 2R(C) + 1 = 2R_p + 1$ и следователно C_p е нормален.

Нека C_1 и C_2 са съответно $[n_1, k_1, d_1]R_1$ и $[n_2, k_2, d_2]R_2$ кодове с норми N_1 и N_2. Кодът $C = C_1 \oplus C_2 = \{(a, b) \mid a \in C_1, b \in C_2\}$ се нарича *външна директна сума* (или само *директна сума*) на C_1 и C_2. В сила е

Твърдение 1.7 *Външната директна сума $C = C_1 \oplus C_2$ е $[n_1+n_2, k_1+k_2, \min\{d_1, d_2\}]$ код с радиус на покритие $R = R_1 + R_2$ [5] и норма $N = \min\{N_1 + 2R_2, N_2 + 2R_1\}$. Външната директна сума на два нормални кода е нормална [9].*

За нормални кодове е възможно да се спести една координата в директната сума. Греъм и Слоен [9] въвеждат скъсената директна сума по следния начин: Нека C_1 и C_2 са съответно $[n_1, k_1]R_1$ и $[n_2, k_2]R_2$ кодове с норми N_1 и N_2. Нека последната координата на C_1 и първата координата на C_2 са приемливи. *Скъсената директна сума (amalgamated direct sum)* $C = C_1 \dot{\oplus} C_2$ е $[n_1+n_2-1, k_1+k_2-1]$ кодът, състоящ се от думите $(c_1, c_2, \ldots, c_{n_1+n_2-1})$, където $(c_1, c_2, \ldots, c_{n_1})$ е дума от кода C_1 и $(c_{n_1}, c_{n_1+1}, \ldots, c_{n_1+n_2-1})$ е дума от кода C_2 (т.е. кодовете C_1 и C_2 се застъпват в една координата).

Твърдение 1.8 *[9]*

1. *Нормата на скъсената директна сума удовлетворява $N(C) \leq N_1 + N_2 - 1$ и застъпващата се координата е приемлива.*

2. *Ако C_1 и C_2 са нормални, то радиусът на покритие на $C = C_1 \dot{\oplus} C_2$ е най-много $R_1 + R_2$.*

3. *Ако C_1 и C_2 са нормални и радиусът на покритие на C е $R_1 + R_2$, то C също е нормален.*

Ако вземем за C_2 кодът $\{000, 111\}$ и приложим Твърдение 1.8 (т. 3), получаваме следното: (В този случай е ясно, че радиусът на покритие на скъсената директна сума е $R_1 + R_2$).

Твърдение 1.9 *[9] Ако C е нормален $[n, k]R$ код, то съществуват нормални $[n + 2i, k]R + i$ кодове за всяко $i \geq 0$.*

1.4 Минимален радиус на покритие

Дефинираме функцията $t[n,k]$ като минималния възможен радиус на покритие на двоичен $[n,k]$ код, т.е.

$$t[n,k] = \min_{C} R(C), \tag{1.7}$$

където C пробягва множеството от всички $[n,k]$ кодове.

Лема 1.2 *За всяко n и k съществуват кодове, несъдържащи нулева колона в пораждащата си матрица, които имат радиус на покритие $R = t[n,k]$.*

Доказателство Съществува поне един $[n,k]R$ код C, за който $R = t[n,k]$. Да допуснем, че C има нулева колона в пораждащата си матрица. Нека C_1 е $[n-1,k]R_1$ код, получен от C чрез махане на нулева колона. От Твърдение 1.6 следва, че $R_1 = R - 1$. Като добавим ненулева колона към пораждащата матрица на C_1, получаваме $[n,k]R_2$ код C_2 с $R_1 \leq R_2 \leq R_1 + 1 = R$. Тъй като R беше избран да е най-малкия възможен радиус на покритие за $[n,k]$ кодове, то $R_2 = R$. Ако в новополучения код C_2 има още нулеви колони, заменяме и тях с ненулеви по същия начин. Окончателно получаваме $[n,k]$ код без нулеви колони и с радиус на покритие $t[n,k]$.

По-нататък, като изследваме $t[n,k]$, винаги ще приемаме, че кодовете не съдържат нулева колона.

Лема 1.3

$$t[n,k] \leq t[n+1,k]. \tag{1.8}$$

Доказателство Нека C е $[n+1,k]R$ код с $R = t[n+1,k]$. Тогава C_p е $[n,k]R_p$ код и $R_p \leq R$ (Лема 1.1).

Нещо повече, ако C е нормален и $R_p = R$, то C_p също е нормален.

Лема 1.4

$$t[n,k] \leq t[n-1,k-1]. \tag{1.9}$$

Доказателство Нека C_1 е $[n-1,k-1]R$ код с $R = t[n-1,k-1]$ и $C_2 = \{0,1\}$. C_2 е $[1,1]0$ нормален код. Тогава $C = C_1 \oplus C_2$ е $[n,k]$ код и според Твърдение 1.7 има радиус на покритие $R = t[n-1,k-1]$. Тъй като $t[n,k]$ е най-малкия възможен радиус на покритие на $[n,k]$ код, то $t[n,k] \leq R(C)$ и лемата е доказана.

Ако C_1 е нормален, то C също е нормален (Твърдение 1.7).

Лема 1.5 *Ако $t[n,k]$ се достига от нормален код, то*

$$t[n+2,k] \leq t[n,k] + 1 \tag{1.10}$$

и $t[n+2,k]$ също се достига от нормален код.

Доказателство Следва от Твърдение 1.9 при $i = 1$.

Твърдение 1.10 *[5] Ако $n > 2^k - \max\{2^{(k-2)/2}, k\}$, то $[n, k]R$ кодовете C с $R = t[n, k]$ и без нулеви координати имат повтарящи се колони в пораждащите си матрици и*

$$t[n, k] \geq t[n - 2, k] + 1. \tag{1.11}$$

Килби и Слоен доказват в [14], че при фиксирано k и достатъчно голямо n минималният радиус на покритие се достига и от нормални кодове. Тогава (1.10) и (1.11) са изпълнени едновременно и получаваме, че

$$t[n + 2, k] = t[n, k] + 1 \tag{1.12}$$

за достатъчно големи n.

При $k \leq 5$ са известни точните стойности на $t[n, k]$:

$$t[n, 1] = \left[\frac{n}{2}\right] \quad \text{за } n \geq 1, \tag{1.13}$$

$$t[n, 2] = \left[\frac{n-1}{2}\right] \quad \text{за } n \geq 2, \tag{1.14}$$

$$t[n, 3] = \left[\frac{n-2}{2}\right] \quad \text{за } n \geq 3, \tag{1.15}$$

$$t[n, 4] = \left[\frac{n-4}{2}\right] \quad \text{за } n \neq 5 \qquad \text{и} \quad t[5, 4] = 1, \tag{1.16}$$

$$t[n, 5] = \left[\frac{n-5}{2}\right] \quad \text{за } n \neq 6 \qquad \text{и} \quad t[6, 5] = 1. \tag{1.17}$$

Тези стойности са доказани от Коен и др. [5] (за $k \leq 3$) и от Греъм и Слоен [9] (за $k = 4, 5$). В [9] е изказано и предположение, че за всяко естествено число m съществуват числа n_0 и n_1 (зависещи от m), такива че

$$t[n, 2m] = \left[\frac{n - 2^m}{2}\right] \quad \text{за } n \geq n_0, \tag{1.18}$$

$$t[n, 2m + 1] = \left[\frac{n - 2^m - 1}{2}\right] \quad \text{за } n \geq n_1. \tag{1.19}$$

1.5 Таблица за $t[n, k]$ при $n \leq 64$

В края на тази глава ще дадем таблица за минималния радиус на покритие, обобщаваща всички известни до момента стойности на $t[n, k]$ при $n \leq 64$. Редовете $k = 1$ до 5 са специални, тъй като за тях е известна точната стойност на $t[n,k]$ за всяко n. За $k \geq 6$, немаркираните долни граници се дават от границата на сферичното покритие (1.5). Останалите долни граници са получени съответно в: p—[2], q—[26], r—[9], s—[4], t—[19], u—[11], v—[12], w—[22], x—[10], y—[24], z—[25]. Отпечатаните с удебелен шрифт долни граници ($t[61,6] \geq \mathbf{23}$, $t[63,6] \geq \mathbf{24}$ и $t[64,6] \geq \mathbf{24}$) не са се появявали в литературата по-рано. Те следват от Твърдение 1.10 при $k = 6$.

Всички горни граници при $k \geq 6$ са получени с явни конструкции. Неотбелязаните с буква стойности се получават от някое от неравенствата (1.8), (1.9) или (1.10). Последното неравенство може да се използва, тъй като всички кодове, включени в таблицата, са нормални (евентуално с изключение на $[18,9]3$ и $[38,26]3$, те не са използвани в конструкции, изискващи нормални кодове).

Маркираните горни граници отговарят на изключително добри кодове. Означени са само стойности, които не могат да бъдат получени от някое от правилата (1.8), (1.9) или (1.10). Това са следните кодове:

а: Получени чрез скъсена директна сума на нормални кодове по формулата

$$[n_1+n_2-1, k_1+k_2-1]R_1+R_2 = [n_1,k_1]R_1 \dot{\oplus} [n_2,k_2]R_2 : \qquad (1.20)$$

$[13,7]2 = [7,4]1 \dot{\oplus} [7,4]1,$
$[25,9]6 = [7,4]1 \dot{\oplus} [19,6]5,$
$[29,15]4 = [7,4]1 \dot{\oplus} [23,12]3,$
$[35,18]5 = [7,4]1 \dot{\oplus} [29,15]4,$
$[36,17]6 = [23,12]3 \dot{\oplus} [14,6]3,$
$[37,14]8 = [7,4]1 \dot{\oplus} [31,11]7,$
$[37,22]4 = [23,12]3 \dot{\oplus} [15,11]1,$
$[41,17]8 = [23,12]3 \dot{\oplus} [19,6]5,$
$[41,21]6 = [7,4]1 \dot{\oplus} [35,18]5,$
$[41,23]5 = [23,12]3 \dot{\oplus} [19,12]2,$
$[42,20]7 = [23,12]3 \dot{\oplus} [20,9]4,$
$[44,16]10 = [31,11]7 \dot{\oplus} [14,6]3,$
$[45,23]6 = [23,12]3 \dot{\oplus} [23,12]3,$
$[47,20]9 = [23,12]3 \dot{\oplus} [25,9]6,$
$[48,29]\mathbf{5} = [26,18]2 \dot{\oplus} [23,12]3,$ (нова граница)
$[49,16]12 = [31,11]7 \dot{\oplus} [19,6]5,$
$[50,19]11 = [31,11]7 \dot{\oplus} [20,9]4,$
$[51,26]7 = [7,4]1 \dot{\oplus} [45,23]6,$
$[53,22]10 = [31,11]7 \dot{\oplus} [23,12]3,$
$[55,19]13 = [31,11]7 \dot{\oplus} [25,9]6,$
$[55,42]\mathbf{3} = [41,32]2 \dot{\oplus} [15,11]1,$ (нова граница)
$[57,29]8 = [35,18]5 \dot{\oplus} [23,12]3,$

$[58,28]9 = [45,23]6\dot{\oplus}[14,6]3,$
$[59,25]11 = [7,4]1\dot{\oplus}[53,22]11,$
$[59,33]7 = [37,22]4\dot{\oplus}[23,12]3,$
$[61,21]14 = [31,11]7\dot{\oplus}[31,11]7,$
$[62,39]\mathbf{6} = [48,29]5\dot{\oplus}[15,11]1,$ (нова граница)
$[63,28]11 = [41,17]8\dot{\oplus}[23,12]3,$
$[63,32]9 = [41,21]6\dot{\oplus}[23,12]3,$
$[63,34]8 = [41,23]5\dot{\oplus}[23,12]3,$
$[64,31]10 = [51,26]7\dot{\oplus}[14,6]3.$

b: $[58,48]2$ кодът, конструиран от Бруалди, Плес и Уилсън в [2]. Този код е нормален.

c: Три нормални кода, получени от Дафърти и Янва в [8]:

- $C_{ss}^{51} = [49,33]4$ код, получен чрез скъсяване два пъти на цикличния код C^{51} с дължина 51 и корени 1 и 5;
- $C_p^{60} = [59,39]5$ код, получен чрез изключване на координатата от цикличния код C^{60} с дължина 60 и корени 0, 0, 0, 1, 1, 1, 1 и 5;
- $C^{63} = [63,49]3$ цикличен код с дължина 63 и корени 1, 5 и 21.

d: Намерените от компютър $[18,9]3$, $[26,18]2$, $[38,26]3$ и $[41,32]2$ кодове. Ван Линт ги споменава в [21] и отбелязва, че са цитирани в [3] като частна кореспонденция между Д.Ашлок и Р.Киблер. От Твърдение 1.2 следва, че кодовете $[26,18]2$ и $[41,32]2$ са нормални. Не ни е известно дали другите два кода са нормални, затова те не са използвани в конструкцията (1.10).

e: $[31,11,11]7$ BCH кодът и $[14,6]3$ и $[19,6]5$ кодовете, посочени от Греъм и Слоен в [9]. Тези кодове са нормални.

g: $[23,12]3$ кодът на Голей и скъсеният $[19,12]2$ код на Голей, получен от първия чрез изключване на произволни четири координати. Тези кодове също са нормални [9].

h: $[2^r-1, 2^r-1-r]1$ кодове на Хеминг. И тези кодове са нормални.

ТАБЛИЦА 1

таблица за $t[n,k]$. част 1

k\n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10
2		0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9
3			0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9
4				0	1	1	1h	2	2	3	3	4	4	5	5	6	6	7	7	8
5					0	1	1	1	2	2	3	3	4	4	5	5	6	6	7	7
6						0	1	1	1	2	2	r3	3	3e	t4	4	4–5	5	5e	5–6
7							0	1	1	1	2	2	2a	3	3	q4	4	4–5	4–5	5
8								0	1	1	1	2	2	2	3	3	3–4	4	4–5	4–5
9									0	1	1	1	2	2	2	p3	3	3d	3–4	4
10										0	1	1	1	2	2	2	s3	3	3	3–4
11											0	1	1	1	1h	2	2	2–3	3	3
12												0	1	1	1	1	2	2	2g	3
13													0	1	1	1	1	2	2	2
14														0	1	1	1	1	2	2
15															0	1	1	1	1	2
16																0	1	1	1	1
17																	0	1	1	1
18																		0	1	1
19																			0	1
20																				0

таблица за $t[n,k]$. част 2

k\n	21	22	23	24	25	26	27	28	29	30	31
1	10	11	11	12	12	13	13	14	14	15	15
2	10	10	11	11	12	12	13	13	14	14	15
3	9	10	10	11	11	12	12	13	13	14	14
4	8	9	9	10	10	11	11	12	12	13	13
5	8	8	9	9	10	10	11	11	12	12	13
6	6	6–7	w7	7–8	7–8	8–9	8–9	w9–10	9–10	9–11	10–11
7	5–6	x6	6–7	6–7	7–8	7–8	7–9	8–9	8–10	w9–10	9–11
8	5	5–6	5–6	6–7	6–7	x7–8	7–8	7–9	w8–9	8–10	8–10
9	4–5	x5	5–6	5–6	w6a	6–7	6–7	7–8	7–8	7–9	8–9
10	4	4–5	4–5	5–6	5–6	5–6	6–7	6–7	z7–8	7–8	7–9
11	3-4	4	4–5	4–5	5–6	5–6	5–6	6–7	6–7	6–7	7e
12	3	3	3g	4	4	w5	5	5–6	x6	6–7	6–7
13	3	3	3	3	4	4	4–5	5	5–6	5–6	6–7
14	2	3	3	3	3	4	4	4–5	5	5–6	5–6
15	2	2	s3	3	3	3	4	4	4a	5	5
16	2	2	2	2–3	3	3	3	4	4	4	4–5
17	1	2	2	2	2–3	3	3	3	4	4	4
18	1	1	2	2	2	2d	3	3	3	3–4	4
19	1	1	1	2	2	2	2	3	3	3	3–4
20	1	1	1	1	2	2	2	2	3	3	3
21	0	1	1	1	1	2	2	2	2	3	3
22		0	1	1	1	1	2	2	2	2	3
23			0	1	1	1	1	2	2	2	2
24				0	1	1	1	1	2	2	2
25					0	1	1	1	1	2	2
26						0	1	1	1	1	1h
27							0	1	1	1	1
28								0	1	1	1
29									0	1	1
30										0	1
31											0

ТАБЛИЦА 1 (Продължение)

таблица за $t[n,k]$. част 3

k\n	32	33	34	35	36	37	38	39	40	41	42
1	16	16	17	17	18	18	19	19	20	20	21
2	15	16	16	17	17	18	18	19	19	20	20
3	15	15	16	16	17	17	18	18	19	19	20
4	14	14	15	15	16	16	17	17	18	18	19
5	13	14	14	15	15	16	16	17	17	18	18
6	10–12	w11–12	11–13	11–13	12–14	12–14	v13–15	13–15	13–16	14–16	14–17
7	9–11	10–12	10–12	y11–13	11–13	11–14	12–14	12–15	y13–15	13–16	z14–16
8	9–11	9–11	y10–12	10–12	10–13	11–13	11–14	z12–14	12–15	12–15	y13–16
9	8–10	x9–10	9–11	9–11	y10–12	10–12	10–13	11–13	11–14	y12–14	12–15
10	w8–9	8–10	8–10	9–11	9–11	9–12	10–12	10–13	y11–13	11–14	11–14
11	7–8	7–8	8–9	8–9	z9–10	9–10	9–11	y10–11	10–12	10–12	11–13
12	x7	7–8	7–8	y8–9	8–9	8–10	9–10	9–11	9–11	10–12	10–12
13	6–7	6–7	7–8	7–8	7–9	8–9	8–10	z9–10	9–11	9–11	y10–12
14	6–7	6–7	6–7	7–8	7–8	7–8a	8–9	8–9	8–10	9–10	9–11
15	5–6	x6	6–7	6–7	y7–8	7–8	7–8	7–9	8–9	8–10	8–10
16	5	5–6	5–6	6–7	6–7	6–8	7–8	7–8	7–9	8–9	8–10
17	4–5	5	5–6	5–6	6a	6–7	6–7	7–8	7–8	7–8a	8–9
18	4	4–5	5	5a	5–6	6	6–7	6–7	u7–8	7–8	7–8
19	4	4	4–5	5	5	5–6	5–6	6–7	6–7	6–8	7–8
20	3–4	4	4	4–5	y5	5	5–6	5–6	6–7	6–7	6–7a
21	3	3–4	4	4	4–5	4–5	5	5–6	5–6	6a	6–7
22	3	3	3–4	4	4	4a	4–5	5	5–6	5–6	6
23	p3	3	3	3–4	4	4	4	4–5	5	5a	5–6
24	2	2–3	3	3	3–4	y4	4	4	4–5	5	5
25	2	2	2–3	3	3	3–4	3–4	4	4	4–5	5
26	2	2	2	2–3	3	3	3d	3–4	4	4	4–5
27	1	2	2	2	2–3	3	3	3	3–4	4	4
28	1	1	2	2	2	2–3	3	3	3	3–4	4
29	1	1	1	2	2	2	2–3	3	3	3	3–4
30	1	1	1	1	2	2	2	2–3	3	3	3
31	1	1	1	1	1	2	2	2	2–3	3	3
32	0	1	1	1	1	1	2	2	2	2d	3
33		0	1	1	1	1	1	2	2	2	2
34			0	1	1	1	1	1	2	2	2
35				0	1	1	1	1	1	2	2
36					0	1	1	1	1	1	2
37						0	1	1	1	1	1
38							0	1	1	1	1
39								0	1	1	1
40									0	1	1
41										0	1
42											0

ТАБЛИЦА 1 (Продължение)

таблица за $t[n,k]$. част 4

k\n	43	44	45	46	47	48	49	50	51	52	53
1	21	22	22	23	23	24	24	25	25	26	26
2	21	21	22	22	23	23	24	24	25	25	26
3	20	21	21	22	22	23	23	24	24	25	25
4	19	20	20	21	21	22	22	23	23	24	24
5	19	19	20	20	21	21	22	22	23	23	24
6	14–17	15–18	15–18	16–19	16–19	17–20	17–20	y18–21	18–21	z19–22	19–22
7	14–17	14–17	y15–18	15–18	v16–19	16–19	16–20	17–20	17–21	17–21	18–22
8	13–16	y14–17	14–17	14–18	y15–18	15–19	y16–19	16–20	16–20	17–21	17–21
9	12–15	13–16	13–16	y14–17	14–17	14–18	15–18	15–19	y16–19	16–20	16–20
10	12–15	12–15	12–16	13–16	13–17	y14–17	14–18	14–18	15–19	15–19	y16–20
11	11–13	11–14	12–14	12–15	y13–15	13–16	13–16	14–17	14–17	y15–18	15–18
12	10–13	11–13	11–14	u12–14	12–15	12–15	13–16	13–16	13–17	14–17	14–18
13	10–12	10–13	y11–13	11–14	11–14	12–15	12–15	y13–16	13–16	13–17	y14–17
14	9–11	10–12	10–12	10–13	11–13	11–14	y12–14	12–15	12–15	y13–16	13–16
15	8–11	9–11	y10–12	10–12	10–13	y11–13	11–14	11–14	12–15	12–15	12–16
16	8–10	9–10a	9–11	9–11	10–12	10–12	10–12a	11–13	11–13	z12–14	12–14
17	8–9	8–10	y9–10	9–11	9–11	10–12	10–12	10–12	11–13	11–13	11–14
18	7–9	8–9	8–10	8–10	9–11	9–11	9–12	10–12	10–12	10–13	11–13
19	7–8	7–9	8–9	8–10	8–10	9–11	9–11	9–11a	10–12	10–12	10–13
20	7–8	7–8	7–9	8–9	8–9a	8–10	y9–10	9–11	9–11	y10–12	10–12
21	6–7	7–8	7–8	7–9	z8–9	8–9	8–10	8–10	9–11	9–11	9–12
22	6–7	6–7	6–8	7–8	7–9	7–9	8–9	8–10	8–10	9–10	9–10a
23	y6	6	6a	6–7	7	7–8	7–8	8–9	8–9	8–10	9–10
24	5–6	5–6	6	6	6–7	7	7–8	7–8	y8–9	8–9	8–10
25	5	5–6	5–6	6	6	6–7	7	7–8	7–8	7–9	8–9
26	4–5	5	5–6	5–6	6	6	6–7	y7	7a	7–8	7–8
27	4–5	4–5	5	5–6	5–6	6	6	6–7	6–7	7	7–8
28	4	4–5	4–5	5	5–6	5–6	y6	6	6–7	6–7	7
29	4	4	4–5	4–5	5	**5**a	5–6	5–6	6	6–7	6–7
30	3–4	4	4	4–5	4–5	5	5	5–6	5–6	6	6–7
31	3	3–4	4	4	4–5	4–5	5	5	5–6	5–6	6
32	3	3	3–4	4	4	4–5	4–5	5	5	5–6	5–6
33	3	3	3	3–4	3–4	4	4c	4–5	4–5	5	5–6
34	2	3	3	3	3–4	3–4	4	4	4–5	4–5	5
35	2	2	p3	3	3	3–4	3–4	4	4	4–5	4–5
36	2	2	2	u3	3	3	3–4	3–4	4	4	4–5
37	2	2	2	2	2–3	3	3	3–4	3–4	4	4
38	1	2	2	2	2	2–3	3	3	3–4	3–4	4
39	1	1	2	2	2	2	2–3	3	3	3–4	3–4
40	1	1	1	2	2	2	2	2–3	3	3	3–4
41	1	1	1	1	2	2	2	2	2–3	3	3
42	1	1	1	1	1	2	2	2	2	2–3	3
43	0	1	1	1	1	1	2	2	2	2	2–3
44		0	1	1	1	1	1	2	2	2	2
45			0	1	1	1	1	1	2	2	2
46				0	1	1	1	1	1	2	2
47					0	1	1	1	1	1	2
48						0	1	1	1	1	1
49							0	1	1	1	1
50								0	1	1	1
51									0	1	1
52										0	1
53											0

ТАБЛИЦА 1 (Продължение)

таблица за $t[n,k]$. част 5

k\n	54	55	56	57	58	59	60	61	62	63	64
1	27	27	28	28	29	29	30	30	31	31	32
2	26	27	27	28	28	29	29	30	30	31	31
3	26	26	27	27	28	28	29	29	30	30	31
4	25	25	26	26	27	27	28	28	29	29	30
5	24	25	25	26	26	27	27	28	28	29	29
6	19–23	20–23	20–24	y21–24	21–25	z22–25	22–26	**23**–26	23–27	**24**–27	**24**–28
7	18–22	19–23	19–23	19–24	20–24	z21–25	21–25	21–26	22–26	22–27	22–27
8	y18–22	18–22	18–23	19–23	19–24	v20–24	20–25	20–25	21–26	21–26	21–27
9	17–21	17–21	y18–22	18–22	18–23	19–23	19–24	y20–24	20–25	20–25	21–26
10	16–20	16–21	17–21	17–22	y18–22	18–23	18–23	19–24	19–24	y20–25	20–25
11	15–19	y16–19	16–20	16–20	17–21	17–21	y18–22	18–22	18–23	19–23	19–24
12	y15–18	15–19	15–19	16–20	16–20	y17–21	17–21	17–22	y18–22	18–23	18–23
13	14–18	14–18	15–19	15–19	15–20	16–20	16–21	y17–21	17–22	17–22	18–23
14	13–17	14–17	14–18	14–18	15–19	15–19	y16–20	16–20	16–21	17–21	17–22
15	13–16	13–17	y14–17	14–18	14–18	y15–19	15–19	15–20	16–20	16–21	16–21
16	12–15	y13–15	13–16	13–16	14–17	14–17	14–18	15–18	15–19	z16–19	16–20
17	12–14	12–15	12–15	13–16	13–16	13–17	14–17	14–18	y15–18	15–19	15–19
18	11–14	z12–14	12–15	12–15	y13–16	13–16	13–17	y14–17	14–18	14–18	15–19
19	11–13	11–13a	11–14	12–14	12–15	12–15	13–16	13–16	13–17	14–17	14–18
20	10–13	y11–13	11–13	11–14	11–14	12–15	12–15	y13–16	13–16	13–17	14–17
21	10–12	10–13	10–13	11–13	11–14	11–14	12–14	12–14a	12–15	13–15	13–16
22	9–11	10–11	10–12	10–12	11–13	11–13	11–14	12–14	12–14	12–15	13–15
23	9–10	9–11	z10–11	10–12	10–12	z11–13	11–13	11–14	z12–14	12–14	12–15
24	z9–10	9–10	9–11	9–11	10–12	10–12	10–13	11–13	11–14	11–14	12–14
25	8–10	8–10	9–10	9–11	9–11	10–11a	10–12	10–12	11–13	11–13	11–14
26	8–9	8–9	8–10	9–10	9–11	9–11	y10–11	10–12	10–12	z11–13	11–13
27	7–8	8–9	8–9	8–10	y9–10	9–11	9–11	9–11	10–12	10–12	10–13
28	7–8	7–8	y8–9	8–9	8–9a	8–10	9–10	9–11	9–11	10–11a	10–12
29	7	7–8	7–8	7–8a	8–9	8–9	8–10	9–10	9–11	9–11	10–11
30	6–7	7	7–8	7–8	7–8	8–9	8–9	8–10	9–10	9–11	9–11
31	6–7	6–7	y7	7–8	7–8	7–8	8–9	8–9	8–10	y9–10	9–10a
32	6	6–7	6–7	6–7	7–8	7–8	7–8	8–9	8–9	8–9a	8–10
33	5–6	6	6–7	6–7	6–7	7a	7–8	7–8	u8–9	8–9	8–9
34	5–6	5–6	y6	6–7	6–7	6–7	7	7–8	7–8	7–8a	8–9
35	5	5–6	5–6	5–6	6–7	6–7	6–7	7	7–8	7–8	7–8
36	4–5	5	5–6	5–6	5–6	6–7	6–7	6–7	6–7	708	7–8
37	4–5	4–5	5	5–6	5–6	5–6	6–7	6–7	6–7	6–7	7–8
38	4	4–5	4–5	5	5–6	5–6	5–6	6–7	6–7	6–7	6–7
39	4	4	4–5	4–5	5	5c	5–6	5–6	**6**a	6–7	6–7
40	3–4	4	4	4–5	4–5	5	5	5–6	5–6	6	6–7
41	3–4	3–4	4	4	4–5	4–5	5	5	5–6	5–6	6
42	3	**3**a	3–4	4	4	4–5	4–5	4–5	5	5–6	5–6
43	3	3	3	3–4	4	4	4–5	4–5	4–5	5	5–6
44	2–3	3	3	3	3–4	3–4	4	4–5	4–5	4–5	5
45	2	2–3	3	3	3	3–4	3–4	4	4–5	4–5	4–5
46	2	2	2–3	3	3	3	3–4	3–4	4	4–5	4–5
47	2	2	2	2–3	3	3	3	3–4	3–4	4	4–5
48	2	2	2	2	2b	3	3	3	3–4	3–4	4
49	1	2	2	2	2	2	3	3	3	3c	3–4
50	1	1	2	2	2	2	2	3	3	3	3
51	1	1	1	2	2	2	2	2	3	3	3
52	1	1	1	1	2	2	2	2	2	3	3
53	1	1	1	1	1	2	2	2	2	2	2–3
54	0	1	1	1	1	1	2	2	2	2	2
55		0	1	1	1	1	1	2	2	2	2
56			0	1	1	1	1	1	2	2	2
57				0	1	1	1	1	1	1h	2
58					0	1	1	1	1	1	1
59						0	1	1	1	1	1
60							0	1	1	1	1
61								0	1	1	1
62									0	1	1
63										0	1
64											0

Глава 2

Минимален радиус на покритие на самодопълнителни кодове

2.1 Самодопълнителни линейни кодове

Двоичният линеен код C се нарича *самодопълнителен*, ако съдържа единичния вектор $(1, 1, \ldots, 1)$. В този случай за всяка дума от кода $c \in C$, двоичното ѝ допълнение $\overline{c}$ също принадлежи на C. Това равномерно разпределение на кодовите думи в пространството F_2^n дава основание на Коен и др. [5] да поставят въпроса дали минималният радиус на покритие $t[n, k]$ винаги се достига и от самодопълнителни кодове. През 1988г. Ст. Додунеков, Кр. Манев и Вл. Тончев [7] отговарят отрицателно на този въпрос—те доказват, че радиусът на покритие на самодопълнителните $[14, 6]$ кодове е поне 4, въпреки че $t[14, 6] = 3$. Остава открит въпросът кога $t[n, k]$ се достига от самодопълнителни кодове.

В тази глава получаваме точните стойности за минималния радиус на покритие за самодопълнителни кодове с размерност $k \leq 6$ и построяваме таблица със стойностите на този радиус при $n \leq 64$.

2.2 Основни граници за минималния радиус на покритие на самодопълнителни кодове

Да означим с $t^s[n, k]$ най-малкия възможен радиус на самодопълнителен $[n, k]$ код, т.е.

$$t^s[n, k] = \min_C R(C), \tag{2.1}$$

където C пробягва множеството от всички самодопълнителни $[n, k]$ кодове.

Лема 2.1

$$t^s[n, k] \geq t[n, k]. \tag{2.2}$$

Доказателство Самодопълнителните кодове са подмножество на всички двоични линейни кодове. Твърдението следва от дефинициите (1.7) и (2.1).

От (2.2) следва, че всички долни граници от Глава 1 важат и за самодопълнителни кодове.

Изключването на координата от самодопълнителен код ни дава самодопълнителен код, както и кодовете, получени чрез външна директна сума или скъсена директна сума от самодопълнителни кодове са отново самодопълнителни. Така неравенствата (1.8), (1.9) и (1.10) ни дават

$$\begin{aligned} t^s[n,k] &\leq t^s[n+1,k], &(2.3)\\ t^s[n,k] &\leq t^s[n-1,k-1], &(2.4)\\ t^s[n+2,k] &\leq t^s[n,k]+1. &(2.5)\end{aligned}$$

Теорема 2.1 *За* $k \leq 5$ *и всяко* n *е в сила*

$$t^s[n,k] = t[n,k]. \tag{2.6}$$

Доказателство Нека T_n е $[n,1]$ кодът $\{\underbrace{000\ldots0}_{n},\underbrace{111\ldots1}_{n}\}$. Очевидно T_n е самодопълнителен и нормален (тъй като $k=1$, виж Твърдение 1.2).

Минималният радиус на покритие $t[n,k]$ се достига от следните самодопълнителни кодове [9]:

$k = 1:$ T_n;

$k = 2:$ $T_{n-1} \oplus T_1$;

$k = 3:$ $T_{n-2} \oplus T_1 \oplus T_1$;

$k = 4:$ За $n = 5$—$T_2 \oplus T_1 \oplus T_1 \oplus T_1$, а за $n > 5$ прилагаме Твърдение 1.9 към $T_3 \oplus T_1 \oplus T_1 \oplus T_1$ при четно n или към $[7,4]1$ кода на Хеминг при нечетно n;

$k = 5:$ Външна директна сума на T_1 и оптимален $[n-1,4]$ код.

Теорема 2.1 ни дава точните стойности на $t^s[n,k]$ за $k \leq 5$:

$$\begin{aligned} t^s[n,1] &= \left[\frac{n}{2}\right] \quad \text{за } n \geq 1, &(2.7)\\ t^s[n,2] &= \left[\frac{n-1}{2}\right] \quad \text{за } n \geq 2, &(2.8)\\ t^s[n,3] &= \left[\frac{n-2}{2}\right] \quad \text{за } n \geq 3, &(2.9)\end{aligned}$$

$$t^s[n,4] = \left[\frac{n-4}{2}\right] \quad \text{за } n \neq 5 \qquad \text{и} \quad t^s[5,4] = 1, \tag{2.10}$$

$$t^s[n,5] = \left[\frac{n-5}{2}\right] \quad \text{за } n \neq 6 \qquad \text{и} \quad t^s[6,5] = 1. \tag{2.11}$$

Лема 2.2 *Ако двоичният линеен $[n,k]R$ код C съдържа две еднакви колони, то $R \geq t[n-2,k]+1$. За самодопълнителен код C с повтарящи се колони е в сила $R \geq t^s[n-2,k]+1$.*

Доказателство Ако C съдържа нулева колона (в този случай C не е самодопълнителен), то според Твърдение 1.6, $R \geq t[n-1,k]+1 \geq t[n-2,k]+1$. В противен случай можем да изберем пораждаща матрица във вида

$$\begin{bmatrix} 1 & 1 & \\ 0 & 0 & \\ \vdots & \vdots & G' \\ 0 & 0 & \end{bmatrix}.$$

Матрицата G' поражда $[n-2,k']$ код C' $(k' \leq k)$. Ако C е самодопълнителен, C' също е самодопълнителен. Съществува вектор $u' \in F_2^{n-2}$, такъв че $\mathrm{dist}(u',x) \geq t[n-2,k']$ за всяко $x \in C'$. Нека $u = (10|u')$. Тогава $\mathrm{dist}(u,y) \geq 1 + t[n-2,k']$ за всяко $y \in C$, т.е. $R \geq 1 + t[n-2,k']$. От неравенствата (1.8) и (1.9) имаме $t[n,k] \leq t[n,k-1]$, откъдето $t[n-2,k'] \geq t[n-2,k]$. Окончателно $R \geq t[n-2,k]+1$.

Ако C е самодопълнителен, вместо $t[n,k]$ разглеждаме $t^s[n,k]$.

Лема 2.3 *Ако $n > 2^{k-1}$, то самодопълнителните $[n,k]R$ кодовете C имат повтарящи се колони в пораждащите си матрици и*

$$t^s[n,k] \geq t^s[n-2,k]+1. \tag{2.12}$$

Доказателство Да изберем пораждаща матрица G в систематичен вид. Единственият начин да получим единичния вектор $(111\dots1)$ като линейна комбинация на редове на G е да съберем всичките k реда. Следователно всички стълбове на G трябва да имат нечетно тегло. Броят на различните вектори над F_2 с дължина k и нечетно тегло е 2^{k-1}, така че ако G има повече колони, поне две ще са еднакви. В такъв случай твърдението следва от Лема 2.2.

Лема 2.4 *Радиусът на покритие на всеки самодопълнителен $[n,k,1]$ код C е поне $t^s[n-1,k-1]$.*

Доказателство Можем да изберем пораждаща матрица за C във вида

$$G = \begin{bmatrix} 100 & \cdots & 0 \\ 0 & & \\ 0 & G_1 & \\ \vdots & & \\ 0 & & \end{bmatrix},$$

където G_1 поражда $[n-1, k-1, d \geq 1]$ код C_1. Нека $u \in F_2^{n-1}$ е вектор, за който $\mathrm{dist}(u, x) \geq t^s[n-1, k-1]$ за всяко $x \in C_1$. Тогава $\mathrm{dist}((0|u), y) \geq t^s[n-1, k-1]$ за всяко $y \in C$, откъдето $R(C) \geq t^s[n-1, k-1]$.

Лема 2.5 *Радиусът на покритие на всеки самодопълнителен $[n, k, 2]$ код C е поне $t^s[n-1, k-1]$.*

Доказателство В този случай можем да изберем пораждаща матрица за C във вида

$$G = \begin{bmatrix} 110 & \cdots & 0 \\ 0 & & \\ 0 & G_2 & \\ \vdots & & \\ 0 & & \end{bmatrix},$$

където G_2 поражда $[n-1, k-1, d \geq 2]$ код C_2. Нека отново $u \in F_2^{n-1}$ е вектор, за който $\mathrm{dist}(u, x) \geq t^s[n-1, k-1]$ за всяко $x \in C_2$. Да означим с v първия ред на матрицата G. Тогава

$$C = (0|C_2) \cup (v + (0|C_2)),$$

където $(0|C_2) = \{(0|x) : x \in C_2\}$. Ако $c \in (0|C_2)$, то $\mathrm{dist}((0|u), c) \geq t^s[n-1, k-1]$. Ако пък $c \in (v + (0|C_2))$, то $c = v + (0|w)$ за някое $w \in C_2$ и

$$\begin{aligned} \mathrm{dist}(c, (0|u)) &= \mathrm{wt}(v + (0|w) + (0|u)) \\ &= \mathrm{wt}(v) + \mathrm{wt}((0|w) + (0|u)) - 2\,\mathrm{wt}(v * ((0|w) + (0|u))) \\ &\geq t^s[n-1, k-1]. \end{aligned}$$

Следователно $R(C) \geq t^s[n-1, k-1]$.

2.3 Самодопълнителни кодове с размерност шест

При $n = 6, \ldots, 13$ и $n = 15$ радиусите на покритие на самодопълнителните $[n, 6]$ кодове, конструирани по правилото (2.4), съвпадат с известните долни граници от Таблица 1. Другите дължини, за които е известна точната стойност на $t^s[n, 6]$, са:

$n = 14:$ $[14,6]3$ кодът, включен в Таблица 1, не е самодопълнителен. Ст. Додунеков, Кр. Манев и Вл. Тончев [7] доказват, че $t^s[14,6] = 4$.

$n = 19:$ Включеният в Таблица 1 $[19,6]5$ код е самодопълнителен (виж пораждащата му матрица в [9]), така че $t^s[19,6] = 5$.

$n = 18, 21, 23:$ Кодовете, включени в Таблица 1, се получават от $[19,6]5$ по правило (2.3) или (2.5) и са самодопълнителни.

За всички останали дължини n долните и горните граници за $t^s[n,6]$ не съвпадат.

2.3.1 Метод на търсене

Методът ни на търсене на самодопълнителни $[n,6]$ кодове с малък радиус на покритие е подобен на използвания в [7]. Тъй като еквивалентните кодове имат еднакъв радиус на покритие, без ограничения можем да разместваме редовете и стълбовете в пораждащите матрици.

Разглеждаме самодопълнителен $[n,6,d]$ код C. Ако C има минимално разстояние $d \leq 2$, то от Твърдения 2.4 и 2.5 имаме $R(C) \geq t^s[n-1,k-1]$, така че такъв код не може да подобри вече известните горни граници, получени чрез правилото (2.4). Също така, Твърдение 2.2 ни позволява да разглеждаме само кодове с неповтарящи се колони. Затова считаме, че $d \geq 3$ и C няма повтарящи се колони. Нека пораждащата матрица на C е записана в систематичен вид,

$$G = [I_6 N]. \tag{2.13}$$

Тъй като единичният вектор $(1,1,\ldots,1)$ принадлежи на C, той трябва да се получава като сума на всичките редове на G. Следователно теглата на всички колони в G трябва да са нечетни, т.е. 3 или 5 (колона с тегло 1 би съвпадала с някоя от колоните на I_6).

Можем да считаме, че първия ред на G има тегло d. Тогава G има вида

$$G = \left[\begin{array}{cc} & \overbrace{11\cdots1}^{d-1}\overbrace{00\cdots0}^{n-d-5} \\ I_6 & \\ & M \end{array} \right], \tag{2.14}$$

където M е $5 \times (n-6)$ матрица, чиито първи $d-1$ стълба имат четно тегло (2 или 4), а последните $n-d-5$ стълба—нечетно тегло (3 или 5).

Различните възможни стълбове над F_2 с дължина 5 и тегло 2 са 10, с тегло 3—10, с тегло 4—5 и с тегло 5—1. Тъй като ни интересуват само класовете еквивалентни кодове, подреждането на стълбовете е без значение. Без ограничение можем да разместваме и редовете на пораждащата матрица (след това с разместване само на първите шест стълба отново ще я приведем в систематичен вид), което ни позволява да разглеждаме с точност до пермутации на колони и стълбове една (но не повече!) от групите колони с определено тегло, при условие че разглеждаме всички комбинации на колони от останалите групи.

Да означим с n_i броят колони с тегло i. С точност до пермутации на редове и стълбове имаме следните следните възможности за n_3-те колони с тегло 3:

$n_3 = 1:$ Една възможност:

$$\begin{array}{c} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{array}$$

$n_3 = 2:$ Две възможности:

$$\begin{array}{cc} 00 & 01 \\ 01 & 01 \\ 10 & 10 \\ 11 & 10 \\ 11 & 11 \end{array}$$

$n_3 = 3:$ Четири възможности:

$$\begin{array}{cccc} 001 & 000 & 001 & 001 \\ 010 & 011 & 010 & 011 \\ 100 & 101 & 101 & 101 \\ 111 & 110 & 110 & 110 \\ 111 & 111 & 111 & 110 \end{array}$$

$n_3 = 4:$ Шест възможности:

$$\begin{array}{cccccc} 0010 & 0011 & 0000 & 0100 & 0011 & 0011 \\ 0101 & 0101 & 0111 & 0011 & 0101 & 0101 \\ 1001 & 1010 & 1011 & 1011 & 1001 & 1010 \\ 1110 & 1100 & 1101 & 1101 & 1110 & 1101 \\ 1111 & 1111 & 1110 & 1110 & 1110 & 1110 \end{array}$$

$n_3 = 5:$ Шест възможности [7]:

$$\begin{array}{cccccc} 11111 & 01111 & 00111 & 00111 & 00111 & 01111 \\ 00011 & 10011 & 11011 & 11011 & 11001 & 10011 \\ 01100 & 01101 & 11101 & 01101 & 01110 & 11100 \\ 10101 & 10110 & 01010 & 11110 & 10011 & 10101 \\ 11010 & 11000 & 10100 & 10000 & 11100 & 01010 \end{array}$$

$n_3 = 6, \ldots, 10:$ Толкова възможности, колкото и за $10 - n_3$ колони. Колоните се получават, като от всичко възможните 10 колони се изключат посочените по-горе $(10 - n_3)$ колони.

С точност до пермутация на колони и стълбове, възможностите за n_2-те колони с тегло 2 са:

$n_2 = 1:$ Една възможност;

$n_2 = 2:$ Две възможности;

$n_2 = 3:$ Четири възможности;

$n_2 = 4:$ Шест възможности;

$n_2 = 5:$ Шест възможности;

$n_2 = 6, \ldots, 10:$ Толкова възможности, колкото и за $(10 - n_2)$ колони.

Конкретните колони се получават, като в съответните възможности за n_3 се разменят местата на нулите и единиците.

Ще опишем по-подробно първия разгледан случай—$[16, 6]$. В останалите случаи се работи по същия начин, те ще бъдат описани накратко в §2.3.2. Където има разлики, те са изрично отбелязани.

За минималния радиус на покритие на самодопълнителните $[16, 6]$ кодове знаем $t^s[16, 6] = 4$–5. Долната граница е от Таблица 1, а горната се получава с правило (2.4). Търсим код с $R = 4$. Както отбелязахме по-горе, разглеждаме кодове с $d \geq 3$, а от [1] виждаме, че $d \leq 6$ за произволни $[16, 6]$ кодове. За различните стойности на d имаме:

$d = 3:$ Първите две колони на M са с четно тегло (2 или 4), а последните осем са с нечетно (3 или 5). Вземаме колоните с тегло 3 с точност до пермутации на редове и колони, а с останалите тегла—само с точност до пермутация на колони. За първите две колони на M имаме общо $\binom{10+5}{2} = 105$ възможности, а за последните осем—6 възможности (2 възможности за 8 колони с тегло 3 и 4 възможности за 7 колони с тегло 3 и една с тегло 5). Компютърната проверка показа, че всички тези 630 кода имат $R \geq 5$.

$d = 4:$ Тук имаме $\binom{15}{3} = 455$ възможности за 3-те колони с тегла 2 или 4 и 10 възможности за 7-те колони с тегла 3 или 5 (4 възможности за 7 колони с тегло 3 и 6 възможности за 6 колони с тегло 3 и една с тегло 5). Компютърната проверка отново показва, че всичките 4550 кода имат $R \geq 5$.

$d = 5:$ Тук имаме $\binom{15}{4} = 1365$ възможности за 4-те колони с тегла 2 или 4 и 12 възможности за 6-те колони с тегла 3 или 5 (6 за 6 колони с тегло 3 и 6 за 5 колони с тегло 3 и една с тегло 5). Тук бяха намерени кодове с $R = 4$, първият открит има пораждаща матрица

$$\begin{bmatrix} 100000 & 1111 & 000000 \\ 010000 & 1111 & 011111 \\ 001000 & 1111 & 100011 \\ 000100 & 0110 & 101101 \\ 000010 & 0101 & 110110 \\ 000001 & 0011 & 011000 \end{bmatrix}. \tag{2.15}$$

Този код е нормален, тъй като $d = 5$ (виж Твърдение 1.2).

$d = 6:$ Тук имаме $\binom{15}{5} = 3003$ възможности за 5-те колони с тегла 2 или 4 и 12 възможности за 5-те колони с тегла 3 или 5 (6 за 5 колони с тегло 3 и 6 за 4 колони с тегло 3 и една с тегло 5). Тук също има кодове с $R = 4$.

2.3.2 Изчисления и резултати

По описания в §2.3.1 метод са конструирани всички кодове, необходими за определяне точните стойности на $t^s[n, 6]$ за всяко n. За изчисляване на радиусите на покритие са разработени допълнителни процедури към пакета LINCOR [16]. Приложен е листинг на използваните програми. Изчисленията са извършени на компютри IBM PC 486DX и DEC 3100.

Ето кодовете, чиито радиуси на покритие са изчислени: (горните граници за d са взети от [1], а долните при $n \geq 20$ идват от факта, че матрицата M не може да съдържа повече от 11 колони с тегла 3 или 5 и следователно $d \geq n - 16$).

- $n = 17:$ Известни граници: $t^s[17, 6] = 4 - 5$.

  $d = 3, 4, 5:$ Ако изключим седмата координата, ще получим вече разгледан $[16, 6, d-1]$ код с радиус на покритие поне 5. Следователно (от Твърдение 1.6) всички тези кодове имат $R \geq 5$.

  $d = 6:$ Матрицата M съдържа 5 колони с тегла 2 или 4(3003 възможности) и 6 колони с тегла 3 или 5 (12 възможности).

  $d = 7:$ Матрицата M съдържа 6 колони с тегла 2 или 4(5005 възможности) и 5 колони с тегла 3 или 5 (12 възможности).

  Всички тези кодове имат $R \geq 5$.

- $n = 20:$ Известни граници: $t^s[20, 6] = 5 - 6$.

$d = 4:$ Матрицата M съдържа 3 колони с тегла 2 или 4(455 възможности) и 11 колони с тегла 3 или 5 (1 възможност).

$d = 5:$ Матрицата M съдържа 4 колони с тегла 2 или 4(1365 възможности) и 10 колони с тегла 3 или 5 (2 възможности).

$d = 6:$ Матрицата M съдържа 5 колони с тегла 2 или 4(3003 възможности) и 9 колони с тегла 3 или 5 (3 възможности).

$d = 7:$ Матрицата M съдържа 6 колони с тегла 2 или 4(5005 възможности) и 8 колони с тегла 3 или 5 (6 възможности).

$d = 8:$ Матрицата M съдържа 7 колони с тегла 2 или 4(6435 възможности) и 7 колони с тегла 3 или 5 (10 възможности).

Всички тези кодове имат $R \geq 6$.

- $n = 22:$ Известни граници: $t^s[22, 6] = 6 - 7$.

$d = 6:$ Матрицата M съдържа 5 колони с тегла 2 или 4(3003 възможности) и 11 колони с тегла 3 или 5 (1 възможност).

$d = 7:$ Матрицата M съдържа 6 колони с тегла 2 или 4(5005 възможности) и 10 колони с тегла 3 или 5 (2 възможности).

$d = 8:$ Матрицата M съдържа 7 колони с тегла 2 или 4(6435 възможности) и 9 колони с тегла 3 или 5 (3 възможности).

$d = 9:$ Матрицата M съдържа 8 колони с тегла 2 или 4(6435 възможности) и 8 колони с тегла 3 или 5 (6 възможности).

Всички тези кодове имат $R \geq 7$.

- $n = 24:$ Известни граници: $t^s[24, 6] = 7 - 8$.

$d = 8:$ Матрицата M съдържа 7 колони с тегла 2 или 4(6435 възможности) и 11 колони с тегла 3 или 5 (1 възможност).

$d = 9:$ Матрицата M съдържа 8 колони с тегла 2 или 4(6435 възможности) и 10 колони с тегла 3 или 5 (2 възможности).

$d = 10:$ Матрицата M съдържа 9 колони с тегла 2 или 4(5005 възможности) и 9 колони с тегла 3 или 5 (3 възможности).

Всички тези кодове имат $R \geq 8$.

- $n = 26:$ Известни граници: $t^s[26, 6] = 8 - 9$.

$d = 10:$ Матрицата M съдържа 9 колони с тегла 2 или 4(147 възможности—тъй като всички възможни колони с тегло 3 участват, колоните с тегло 2 са взети с точност до пермутации на редове и стълбове) и 11 колони с тегла 3 или 5 (1 възможност).

$d = 11$: Матрицата M съдържа 10 колони с тегла 2 или 4(3003 възможности) и 10 колони с тегла 3 или 5 (2 възможности).

$d = 12$: Матрицата M съдържа 11 колони с тегла 2 или 4(1365 възможности) и 9 колони с тегла 3 или 5 (3 възможности).

Всички тези кодове имат $R \geq 9$.

- $n = 28$: Известни граници: $t^s[28, 6] = 9 - 10$.

$d = 12$: Матрицата M съдържа 11 колони с тегла 2 или 4(61 възможности—тъй като всички възможни колони с тегло 3 участват, колоните с тегло 2 са взети с точност до пермутации на редове и стълбове) и 11 колони с тегла 3 или 5 (1 възможност).

Всички тези кодове имат $R \geq 10$.

- $n = 30$: Известни граници: $t^s[30, 6] = 9 - 11$.

$d = 14$: Матрицата M съдържа 13 колони с тегла 2 или 4(8 възможности—тъй като всички възможни колони с тегло 3 участват, колоните с тегло 2 са взети с точност до пермутации на редове и стълбове, а когато участват и всички възможни колони с тегло 2, колоните с тегло 4 са взети с точност до пермутации на редове и колони) и 11 колони с тегла 3 или 5 (1 възможност).

Всички тези кодове имат $R \geq 11$.

Тези пресмятания ни позволяват да докажем следната

Теорема 2.2 *Точните стойности на $t^s[n, 6]$ са:*

$$t^s[7,6] = 1; \tag{2.16}$$

$$t^s[n,6] = \left\lceil \frac{n-6}{2} \right\rceil \quad \text{за } 8 \leq n \leq 15 \quad \text{и} \quad n = 17; \tag{2.17}$$

$$t^s[16,6] = 4; \tag{2.18}$$

$$t^s[n,6] = \left\lceil \frac{n-8}{2} \right\rceil \quad \text{за } n \geq 18. \tag{2.19}$$

Оптимални $[n, 6]$ кодове при $n \geq 18$ се получават чрез прилагане на Твърдение 1.9 към $[19, 6]$ кода, посочен в [9], ако n е четно и чрез изключване на произволна координата от оптимален $[n + 1, 6]$ код, ако n е нечетно.

Доказателство Стойностите на $t^s[n, 6]$ при $7 \leq n \leq 15$ и $n = 18$, 19, 21 и 23 са известни от по-рано. За конструиране на оптимални кодове с тези дължини виж началото на §2.3.

$[16,6]$ кодът (2.15) достига долната граница от Таблица 1 и следователно е оптимален.

При четни n между 20 и 32 разсъждението е следното: Ако $[n,6]$ кодът съдържа повтарящи се колони, то радиусът му на покритие е поне $t^s[n-2,6]+1$ и не може да намали тази известна горна граница. Ако пък кодът не съдържа повтарящи се колони и $n \leq 30$, то компютърната проверка показва, че радиусът му на покритие отново е най-малко $t^s[n-2,6]+1$ (за $n=32$ има единствен самодопълнителен $[32,6]$ код—$RM(1,5)$, и неговият радиус на покритие е 12). Тъй като всички използвани кодове са нормални, от неравенство (2.5) следва, че $t^s[n,6] = t^s[n-2,6]+1$. При нечетни n, неравенствата (2.5) и $t^s[n,k] \geq t^s[k-1,k]$ също показват, че $t^s[n,6] = t^s[n-2,6]+1$.

Когато $n > 32$, Лема 2.3 и неравенство (2.5) са в сила едновременно и следователно $t^s[n,6] = t^s[n-2,6]+1$.

2.4 Таблица за $t^s[n,k]$ при $n \leq 64$

В края на тази глава обобщаваме всички резултати за минималния радиус на покритие на самодопълнителни кодове в таблица за $t^s[n,k]$ при $n \leq 64$. За $k=1$ до 6 са известни точните стойности на $t^s[n,k]$ за всяко n. За $k \geq 7$, всички долни граници са взети от Таблица 1.

Всички горни граници при $k \geq 7$ са получени с явни конструкции. Неотбелязаните с буква стойности се получават от някое от неравенствата (2.3), (2.4) или (2.5). Последното неравенство може да се използва, тъй като всички кодове, включени в таблицата, са нормални.

Маркираните горни граници отговарят на стойности, които не могат да бъдат получени от някое от правилата (2.3), (2.4) или (2.5). Означенията са същите, както в Таблица 1 (виж §1.5), със следните забележки:

a: Отпадат кодовете $[36,17]6$, $[42,20]7$, $[44,16]10$, $[48,29]5$, $[50,19]11$, $[55,42]3$, $[58,28]9$, $[62,39]6$ и $[64,31]10$, тъй като при конструирането им са използвани кодовете $[14,6]3$, $[28,18]2$ и $[41,32]2$ (виж по-надолу). За да запълним получените празнини от отпадането на тези и някои други кодове, използваме скъсената директна сума за получаването на следните кодове:

$[19,10]3 = [7,4]1\dot{\oplus}[13,7]2$,
$[38,17]7 = [23,12]3\dot{\oplus}[16,6]4$,
$[41,29]3 = [27,19]2\dot{\oplus}[15,11]1$,
$[46,16]11 = [31,11]7\dot{\oplus}[16,6]4$,
$[49,30]5 = [27,19]2\dot{\oplus}[23,12]3$,
$[56,43]3 = [42,33]2\dot{\oplus}[15,11]1$,
$[60,28]10 = [45,23]6\dot{\oplus}[16,6]4$,
$[63,40]6 = [49,30]5\dot{\oplus}[15,11]1$.

b: Кодът $[58,48]2$ не е самодопълнителен и отпада. Поради отпадането на кодовете, отбелязани с d в Таблица 1, включваме $[27,19]2$ и $[42,33]2$—кодове, конструирани от Бруалди, Плес и Уилсън в [2]. Тези два кода са самодопълнителни и нормални.

c: Цикличният код C е самодопълнителен, ако 0 не му е корен. Изключването на координата от самодопълнителен код дава отново самодопълнителен код, но скъсяването на кода дава самодопълнителен код само ако $d = 1$. Цикличният код $C^{63} = [63,49]3$ с дължина 63 и корени 1, 5 и 21 е самодопълнителен, но $C^{51}_{ss} = [49,33]4$ и $C^{60}_{p} = [59,39]5$, включени в Таблица 1, не са и отпадат. На тяхно място включваме следните кодове, отново получени от Дафърти и Янва в [8]:

- $C^{51} = [51,35,3]4$ цикличен код с дължина 51 и корени 1 и 5;
- $C^{63}_{*} = [63,43,6]5$ цикличен код с дължина 63 и корени 1, 5, 21 и 31.

d: Не ни е известно дали кодовете $[18,9]3$, $[26,18]2$, $[38,26]3$ и $[41,32]2$ са самодопълнителни и затова не сме ги включили в Таблица 2.

e: $[31,11,11]7$ BCH кодът и $[19,6]5$ кодовете [9] са самодопълнителни, но $[14,6]3$ не е. Последният код е изключен от таблицата.

g: $[23,12]3$ кодът на Голей и скъсеният $[19,12]2$ код на Голей, получен от първия чрез изключване на произволни четири координати, са самодопълнителни.

h: $[2^r-1, 2^r-1-r]1$ кодовете на Хеминг са самодопълнителни.

f: Това означение не е използвано в Таблица 1. Тук с него са отбелязани $[16,6]4$ кодът (2.15), получен в §2.3.1, и $[59,49]2$ кодът, конструиран подолу.

Твърдение 2.1 *[2] Ако H е $m \times n$ проверочна матрица на двоичен код с радиус на покритие 2 и за някое $2 \le t \le m$ първите t реда на H съдържат всичките 2^t-1 ненулеви вектор-стълба с дължина t поне по веднъж, то $(m+1)\times(n+2^{m-t})$ матрицата*

$$\left[\begin{array}{c|c} 000\cdots0 & 111\cdots1 \\ \hline H & \begin{array}{c} 0 \\ \hline M \end{array} \end{array}\right] \tag{2.20}$$

е проверочна матрица на код с радиус на покритие 2, където M е $(m-t)\times 2^{m-t}$ матрица, чиито колони са всички двоични $(m-t)$-торки.

Лема 2.6 *Ако приложим конструкцията от Твърдение 2.1 над самодопълнителен код, то новополученият код също е самодопълнителен.*

Доказателство Един код е самодопълнителен тогава и само тогава, когато всички редове на проверочната му матрица имат четно тегло. Редовете на M имат четно тегло—2^{m-t-1}, така че ако и редовете на H са с четно тегло, новополучената матрица ще е проверочна за самодопълнителен код.

Според [2],

$$H = \begin{bmatrix} 101101101101000000000000000 \\ 011011011011000000000000000 \\ 101110011000101000000000000 \\ 011101110000011000000000000 \\ 101011110000000000101101101 \\ 011110101000000000011011011 \\ 000000000000000101101110011 \\ 000000000000000011011101110 \end{bmatrix} \tag{2.21}$$

е проверочна матрица на $[27, 19]2$ код. Този код е самодопълнителен (теглата на всички редове на H са четни). Първите 4 реда на H съдържат всяка двоична четворка поне веднъж (същото важи и за последните 4 реда), така че можем да приложим конструкцията (2.20). Получаваме 9×43 матрица H_1, която е проверочна за $[43, 34]2$ код. Първият и последните 4 реда на H_1 съдържат всяка двоична петорка поне веднъж. Прилагаме конструкцията (2.20) още веднъж, тя ни дава 10×59 матрица H_2, проверочна за $[59, 49]2$ код. Според Лема 2.6, така полученият код е самодопълнителен.

Подчертаните стойности в Таблица 2 представляват различията в сравнение с Таблица 1.

ТАБЛИЦА 2

таблица за $t^s[n,k]$.   част 1

k\n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10
2		0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9
3			0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9
4				0	1	1	1h	2	2	3	3	4	4	5	5	6	6	7	7	8
5					0	1	1	1	2	2	3	3	4	4	5	5	6	6	7	7
6						0	1	1	1	2	2	3	3	$\underline{4}$	4	**4**f	**5**	5	5e	**6**
7							0	1	1	1	2	2	2a	3	3	4	4	4–5	4–5	5
8								0	1	1	1	2	2	2	3	3	3–4	4	4–5	4–5
9									0	1	1	1	2	2	2	3	3	3–$\underline{4}$	3–4	4–$\underline{5}$
10										0	1	1	1	2	2	2	3	3	3a	3–4
11											0	1	1	1	1h	2	2	2–3	3	3
12												0	1	1	1	1	2	2	2g	3
13													0	1	1	1	1	2	2	2
14														0	1	1	1	1	2	2
15															0	1	1	1	1	2
16																0	1	1	1	1
17																	0	1	1	1
18																		0	1	1
19																			0	1
20																				0

таблица за $t^s[n,k]$.   част 2

k\n	21	22	23	24	25	26	27	28	29	30	31
1	10	11	11	12	12	13	13	14	14	15	15
2	10	10	11	11	12	12	13	13	14	14	15
3	9	10	10	11	11	12	12	13	13	14	14
4	8	9	9	10	10	11	11	12	12	13	13
5	8	8	9	9	10	10	11	11	12	12	13
6	6	**7**	7	**8**	**8**	**9**	**9**	**10**	**10**	**11**	**11**
7	5–6	6	6–7	6–7	7–8	7–8	7–9	8–9	8–10	9–10	9–11
8	5	5–6	5–6	6–7	6–7	7–8	7–8	7–9	8–9	8–10	8–10
9	4–5	5	5–6	5–6	6a	6–7	6–7	7–8	7–8	7–9	8–9
10	4	4–5	4–5	5–6	5–6	5–6	6–7	6–7	7–8	7–8	7–9
11	3-4	4	4–5	4–5	5–6	5–6	5–6	6–7	6–7	6–7	7e
12	3	3	3g	4	4	5	5	5–6	6	6–7	6–7
13	3	3	3	3	4	4	4–5	5	5–6	5–6	6–7
14	2	3	3	3	3	4	4	4–5	5	5–6	5–6
15	2	2	3	3	3	3	4	4	4a	5	5
16	2	2	2	2–3	3	3	3	4	4	4	4–5
17	1	2	2	2	2–3	3	3	3	4	4	4
18	1	1	2	2	2	2–$\underline{3}$	3	3	3	3–4	4
19	1	1	1	2	2	2	2b	3	3	3	3–4
20	1	1	1	1	2	2	2	2	3	3	3
21	0	1	1	1	1	2	2	2	2	3	3
22		0	1	1	1	1	2	2	2	2	3
23			0	1	1	1	1	2	2	2	2
24				0	1	1	1	1	2	2	2
25					0	1	1	1	1	2	2
26						0	1	1	1	1	1h
27							0	1	1	1	1
28								0	1	1	1
29									0	1	1
30										0	1
31											0

ТАБЛИЦА 2 (Продължение)

таблица за $t^s[n,k]$. част 3

k\n	32	33	34	35	36	37	38	39	40	41	42
1	16	16	17	17	18	18	19	19	20	20	21
2	15	16	16	17	17	18	18	19	19	20	20
3	15	15	16	16	17	17	18	18	19	19	20
4	14	14	15	15	16	16	17	17	18	18	19
5	13	14	14	15	15	16	16	17	17	18	18
6	**12**	**12**	**13**	**13**	**14**	**14**	**15**	**15**	**16**	**16**	**17**
7	9–11	10–12	10–12	11–13	11–13	11–14	12–14	12–15	13–15	13–16	14–16
8	9–11	9–11	10–12	10–12	10–13	11–13	11–14	12–14	12–15	12–15	13–16
9	8–10	9–10	9–11	9–11	10–12	10–12	10–13	11–13	11–14	12–14	12–15
10	8–9	8–10	8–10	9–11	9–11	9–12	10–12	10–13	11–13	11–14	11–14
11	7–8	7–8	8–9	8–9	9–10	9–10	9–11	10–11	10–12	10–12	11–13
12	7	7–8	7–8	8–9	8–9	8–10	9–10	9–11	9–11	10–12	10–12
13	6–7	6–7	7–8	7–8	7–9	8–9	8–10	9–10	9–11	9–11	10–12
14	6–7	6–7	6–7	7–8	7–8	7–8a	8–9	8–9	8–10	9–10	9–11
15	5–6	6	6–7	6–7	7–8	7–8	7–8	7–9	8–9	8–10	8–10
16	5	5–6	5–6	6–7	6–7	6–8	7–8	7–8	7–9	8–9	8–10
17	4–5	5	5–6	5–6	6–$\underline{7}$	6–7	6–7a	7–8	7–8	7–8a	8–9
18	4	4–5	5	5a	5–6	6	6–7	6–7	7–8	7–8	7–8
19	4	4	4–5	5	5	5–6	5–6	6–7	6–7	6–8	7–8
20	3–4	4	4	4–5	5	5	5–6	5–6	6–7	6–7	6–$\underline{8}$
21	3	3–4	4	4	4–5	4–5	5	5–6	5–6	6a	6–7
22	3	3	3–4	4	4	4a	4–5	5	5–6	5–6	6
23	3	3	3	3–4	4	4	4	4–5	5	5a	5–6
24	2	2–3	3	3	3–4	4	4	4	4–5	5	5
25	2	2	2–3	3	3	3–4	3–4	4	4	4–5	5
26	2	2	2	2–3	3	3	3–$\underline{4}$	3–4	4	4	4–5
27	1	2	2	2	2–3	3	3	3–$\underline{4}$	3–4	4	4
28	1	1	2	2	2	2–3	3	3	3–$\underline{4}$	3–4	4
29	1	1	1	2	2	2	2–3	3	3	3a	3–4
30	1	1	1	1	2	2	2	2–3	3	3	3
31	1	1	1	1	1	2	2	2	2–3	3	3
32	0	1	1	1	1	1	2	2	2	2–$\underline{3}$	3
33		0	1	1	1	1	1	2	2	2	2b
34			0	1	1	1	1	1	2	2	2
35				0	1	1	1	1	1	2	2
36					0	1	1	1	1	1	2
37						0	1	1	1	1	1
38							0	1	1	1	1
39								0	1	1	1
40									0	1	1
41										0	1
42											0

ТАБЛИЦА 2 (Продължение)

таблица за $t^s[n,k]$. част 4

k\n	43	44	45	46	47	48	49	50	51	52	53
1	21	22	22	23	23	24	24	25	25	26	26
2	21	21	22	22	23	23	24	24	25	25	26
3	20	21	21	22	22	23	23	24	24	25	25
4	19	20	20	21	21	22	22	23	23	24	24
5	19	19	20	20	21	21	22	22	23	23	24
6	**17**	**18**	**18**	**19**	**19**	**20**	**20**	**21**	**21**	**22**	**22**
7	14–17	14–17	15–18	15–18	16–19	16–19	16–20	17–20	17–21	17–21	18–22
8	13–16	14–17	14–17	14–18	15–18	15–19	16–19	16–20	16–20	17–21	17–21
9	12–15	13–16	13–16	14–17	14–17	14–18	15–18	15–19	16–19	16–20	16–20
10	12–15	12–15	12–16	13–16	13–17	14–17	14–18	14–18	15–19	15–19	16–20
11	11–13	11–14	12–14	12–15	13–15	13–16	13–16	14–17	14–17	15–18	15–18
12	10–13	11–13	11–14	12–14	12–15	12–15	13–16	13–16	13–17	14–17	14–18
13	10–12	10–13	11–13	11–14	11–14	12–15	12–15	13–16	13–16	13–17	14–17
14	9–11	10–12	10–12	10–13	11–13	11–14	12–14	12–15	12–15	13–16	13–16
15	8–11	9–11	10–12	10–12	10–13	11–13	11–14	11–14	12–15	12–15	12–16
16	8–10	9–$\underline{11}$	9–11	9–11a	10–12	10–12	10–12a	11–13	11–13	12–14	12–14
17	8–9	8–10	9–10	9–11	9–11	10–12	10–12	10–12	11–13	11–13	11–14
18	7–9	8–9	8–10	8–10	9–11	9–11	9–12	10–12	10–12	10–13	11–13
19	7–8	7–9	8–9	8–10	8–10	9–11	9–11	9–$\underline{12}$	10–12	10–12	10–13
20	7–8	7–8	7–9	8–9	8–9a	8–10	9–10	9–11	9–11	10–12	10–12
21	6–7	7–8	7–8	7–9	8–9	8–9	8–10	8–10	9–11	9–11	9–12
22	6–7	6–7	6–8	7–8	7–9	7–9	8–9	8–10	8–10	9–10	9–10a
23	6	6	6a	6–7	7	7–8	7–8	8–9	8–9	8–10	9–10
24	5–6	5–6	6	6	6–7	7	7–8	7–8	8–9	8–9	8–10
25	5	5–6	5–6	6	6	6–7	7	7–8	7–8	7–9	8–9
26	4–5	5	5–6	5–6	6	6	6–7	7	7a	7–8	7–8
27	4–5	4–5	5	5–6	5–6	6	6	6–7	6–7	7	7–8
28	4	4–5	4–5	5	5–6	5–6	6	6	6–7	6–7	7
29	4	4	4–5	4–5	5	5–$\underline{6}$	5–6	5–6	6	6–7	6–7
30	3–4	4	4	4–5	4–5	5	5a	5–6	5–6	6	6–7
31	3	3–4	4	4	4–5	4–5	5	5	5–6	5–6	6
32	3	3	3–4	4	4	4–5	4–5	5	5	5–6	5–6
33	3	3	3	3–4	3–4	4	4–$\underline{5}$	4–5	4–5	5	5–6
34	2	3	3	3	3–4	3–4	4	4–$\underline{5}$	4–5	4–5	5
35	2	2	3	3	3	3–4	3–4	4	4c	4–5	4–5
36	2	2	2	3	3	3	3–4	3–4	4	4	4–5
37	2	2	2	2	2–3	3	3	3–4	3–4	4	4
38	1	2	2	2	2	2–3	3	3	3–4	3–4	4
39	1	1	2	2	2	2	2–3	3	3	3–4	3–4
40	1	1	1	2	2	2	2	2–3	3	3	3–4
41	1	1	1	1	2	2	2	2	2–3	3	3
42	1	1	1	1	1	2	2	2	2	2–3	3
43	0	1	1	1	1	1	2	2	2	2	2–3
44		0	1	1	1	1	1	2	2	2	2
45			0	1	1	1	1	1	2	2	2
46				0	1	1	1	1	1	2	2
47					0	1	1	1	1	1	2
48						0	1	1	1	1	1
49							0	1	1	1	1
50								0	1	1	1
51									0	1	1
52										0	1
53											0

ТАБЛИЦА 2 (Продължение)

таблица за $t^s[n,k]$. част 5

k\n	54	55	56	57	58	59	60	61	62	63	64
1	27	27	28	28	29	29	30	30	31	31	32
2	26	27	27	28	28	29	29	30	30	31	31
3	26	26	27	27	28	28	29	29	30	30	31
4	25	25	26	26	27	27	28	28	29	29	30
5	24	25	25	26	26	27	27	28	28	29	29
6	**23**	**23**	**24**	**24**	**25**	**25**	**26**	**26**	**27**	**27**	**28**
7	18–22	19–23	19–23	19–24	20–24	21–25	21–25	21–26	22–26	22–27	22–27
8	18–22	18–22	18–23	19–23	19–24	20–24	20–25	20–25	21–26	21–26	21–27
9	17–21	17–21	18–22	18–22	18–23	19–23	19–24	20–24	20–25	20–25	21–26
10	16–20	16–21	17–21	17–22	18–22	18–23	18–23	19–24	19–24	20–25	20–25
11	15–19	16–19	16–20	16–20	17–21	17–21	18–22	18–22	18–23	19–23	19–24
12	15–18	15–19	15–19	16–20	16–20	17–21	17–21	17–22	18–22	18–23	18–23
13	14–18	14–18	15–19	15–19	15–20	16–20	16–21	17–21	17–22	17–22	18–23
14	13–17	14–17	14–18	14–18	15–19	15–19	16–20	16–20	16–21	17–21	17–22
15	13–16	13–17	14–17	14–18	14–18	15–19	15–19	15–20	16–20	16–21	16–21
16	12–15	13–15	13–16	13–16	14–17	14–17	14–18	15–18	15–19	16–19	16–20
17	12–14	12–15	12–15	13–16	13–16	13–17	14–17	14–18	15–18	15–19	15–19
18	11–14	12–14	12–15	12–15	13–16	13–16	13–17	14–17	14–18	14–18	15–19
19	11–13	11–13a	11–14	12–14	12–15	12–15	13–16	13–16	13–17	14–17	14–18
20	10–13	11–13	11–13	11–14	11–14	12–15	12–15	13–16	13–16	13–17	14–17
21	10–12	10–13	10–13	11–13	11–14	11–14	12–14	12–14a	12–15	13–15	13–16
22	9–11	10–11	10–12	10–12	11–13	11–13	11–14	12–14	12–14	12–15	13–15
23	9–10	9–11	10–11	10–12	10–12	11–13	11–13	11–14	12–14	12–14	12–15
24	9–10	9–10	9–11	9–11	10–12	10–12	10–13	11–13	11–14	11–14	12–14
25	8–10	8–10	9–10	9–11	9–11	10–11a	10–12	10–12	11–13	11–13	11–14
26	8–9	8–9	8–10	9–10	9–11	9–11	10–11	10–12	10–12	11–13	11–13
27	7–8	8–9	8–9	8–10	9–10	9–11	9–11	9–11	10–12	10–12	10–13
28	7–8	7–8	8–9	8–9	8–$\underline{10}$	8–10	9–10a	9–11	9–11	10–11a	10–12
29	7	7–8	7–8	7–8a	8–9	8–9	8–10	9–10	9–11	9–11	10–11
30	6–7	7	7–8	7–8	7–8	8–9	8–9	8–10	9–10	9–11	9–11
31	6–7	6–7	7	7–8	7–8	7–8	8–9	8–9	8–10	9–10	9–$\underline{11}$
32	6	6–7	6–7	6–7	7–8	7–8	7–8	8–9	8–9	8–9a	8–10
33	5–6	6	6–7	6–7	6–7	7a	7–8	7–8	8–9	8–9	8–9
34	5–6	5–6	6	6–7	6–7	6–7	7	7–8	7–8	7–8a	8–9
35	5	5–6	5–6	5–6	6–7	6–7	6–7	7	7–8	7–8	7–8
36	4–5	5	5–6	5–6	5–6	6–7	6–7	6–7	6–7	708	7–8
37	4–5	4–5	5	5–6	5–6	5–6	6–7	6–7	6–7	6–7	7–8
38	4	4–5	4–5	5	5–6	5–6	5–6	6–7	6–7	6–7	6–7
39	4	4	4–5	4–5	5	5–$\underline{6}$	5–6	5–6	6–$\underline{7}$	6–7	6–7
40	3–4	4	4	4–5	4–5	5	5–$\underline{6}$	5–6	5–6	6a	6–7
41	3–4	3–4	4	4	4–5	4–5	5	5–$\underline{6}$	5–6	5–6	6
42	3	3–$\underline{4}$	3–4	4	4	4–5	4–5	4–5	5–$\underline{6}$	5–6	5–6
43	3	3	3a	3–4	4	4	4–5	4–5	4–5	5c	5–6
44	2–3	3	3	3	3–4	3–4	4	4–5	4–5	4–5	5
45	2	2–3	3	3	3	3–4	3–4	4	4–5	4–5	4–5
46	2	2	2–3	3	3	3	3–4	3–4	4	4–5	4–5
47	2	2	2	2–3	3	3	3	3–4	3–4	4	4–5
48	2	2	2	2	2–$\underline{3}$	3	3	3	3–4	3–4	4
49	1	2	2	2	2	**2**f	3	3	3	3c	3–4
50	1	1	2	2	2	2	2	3	3	3	3
51	1	1	1	2	2	2	2	2	3	3	3
52	1	1	1	1	2	2	2	2	2	3	3
53	1	1	1	1	1	2	2	2	2	2	2–3
54	0	1	1	1	1	1	2	2	2	2	2
55		0	1	1	1	1	1	2	2	2	2
56			0	1	1	1	1	1	2	2	2
57				0	1	1	1	1	1	1h	2
58					0	1	1	1	1	1	1
59						0	1	1	1	1	1
60							0	1	1	1	1
61								0	1	1	1
62									0	1	1
63										0	1
64											0

Глава 3

Спектър на лидерите на съседни класове за кодове с повтарящи се координати

Да означим с L_i броя на съседните класове, чийто лидер има тегло i (за дефиницията на лидер на съседен клас виж §1.3). Задачата за намиране разпределението на $\{L_i\}$ все още не е решена за никоя фамилия кодове [15]. Освен теоретично значение, тази задача има и практическо приложение—ако знаем това разпределение, можем да определим вероятността за допускане на грешка при декодиране по максимално правдоподобие. Наистина, ако p е вероятността за грешка по канала ($0 \leq p \leq 1/2$), то [15] вероятността за грешка при декодирането е

$$P = 1 - \sum_{i=0}^{n} L_i p^i (1-p)^{n-i}. \tag{3.1}$$

Задачата за спектъра на лидерите на съседни класове е тясно свързана и с радиуса на покритие R, защото R е максималната стойност на i, за която $L_i \neq 0$. Радиусът на покритие на кодове с повтарящи се координати е изследван от Слоен [20] и Килби и Слоен [14].

В [17] сме разгледали спектъра на лидерите на съседни класове за самодопълнителни $[n,k]$ кодове при $k \leq 3$. Тук доразвиваме използваните там идеи и получаваме резултати за двоични линейни кодове от произволни размерности.

3.1 Произволни двоични линейни кодове

Нека C е $[n,k]$ код. Ако C има пораждаща матрица, в която всички колони са различни, казваме, че C има *различни координати*. Оттук следва $n \leq 2^k$. Описаният тук метод е насочен към кодове с повтарящи се координати. Всеки такъв код може да бъде получен от код C^* с различни координати, вземайки $n_i \geq 0$ копия от i-тата координата на C^* ($n = \sum n_i$). Така полученият код C ще наричаме *раздута* версия на C^*.

Важна роля играе *симплексният* $[2^k-1,k]$ код S_k, който има $k\times(2^k-1)$ пораждаща матрица, чиито колони са всички ненулеви двоични k-торки. Всеки код C, несъдържащ нулева колона, може да се разглежда като раздута версия на S_k. Ако C съдържа и нулеви колони, то той е раздута версия на разширения симплексен код $\hat{S}_k$ с пораждаща матрица, състояща се от всички възможни двоични колони с дължина k. Ще считаме, че колоните в пораждащите матрици на S_k и $\hat{S}_k$ са подредени в нарастващ ред, така например пораждащата матрица на $\hat{S}_3$ е

$$G(\hat{S}_3)=\begin{bmatrix}0&0&0&0&1&1&1&1\\0&0&1&1&0&0&1&1\\0&1&0&1&0&1&0&1\end{bmatrix}. \tag{3.2}$$

Нека $[n,k]$ кодът C е получен чрез раздуване на $\hat{S}_k$ и $n=\sum_{l=0}^{2^k-1}n_l$, където $n_l\geq 0$ е броя копия от l-тата координата на $\hat{S}_k$. Интересуваме се от спектъра на лидерите на съседни класове на C.

Лема 3.1 *Векторът $x\in F_2^n$ е лидер на съседен клас за C тогава и само тогава, когато за всяко $c\in C$ е изпълнено*

$$2\,\mathrm{wt}(x*c)\leq \mathrm{wt}(c). \tag{3.3}$$

Доказателство Според дефиницията, x е лидер на съседния клас $x+C$ тогава и само тогава, когато

$$\mathrm{wt}(x+c)\geq \mathrm{wt}(x) \qquad \forall c\in C.$$

Но $\mathrm{wt}(x+c)=\mathrm{wt}(x)+\mathrm{wt}(c)-2\,\mathrm{wt}(x*c)$, следователно $\mathrm{wt}(x)+\mathrm{wt}(c)-2\,\mathrm{wt}(x*c)\geq \mathrm{wt}(x)$ и $2\,\mathrm{wt}(x*c)\leq \mathrm{wt}(c)$.

Лема 3.2 *Нека векторът x е лидер на съседен клас за C и равенството*

$$2\,\mathrm{wt}(x*c)=\mathrm{wt}(c) \tag{3.4}$$

се достига за N различни вектора $c\in C$. Тогава съседният клас $x+C$ съдържа точно N вектора с тегло $\mathrm{wt}(x)$.

Доказателство От доказателството на Лема 3.1 се вижда, че равенството $2\,\mathrm{wt}(x*c)=\mathrm{wt}(c)$ се достига точно тогава, когато $\mathrm{wt}(x+c)=\mathrm{wt}(x)$. Това дава точно N вектора с тегло $\mathrm{wt}(x)$.

Забележка $N\geq 1$, тъй като равенство (3.4) е изпълнено при $c=0$.

Нека $x\in F_2^n$. Разглеждаме координатите на x на групички с дължини съответно n_0, n_1, …, n_{2^k-1}, т.е. $x=(x_0,x_1,\ldots,x_{2^k-1})$, където $x_l\in F_2^{n_l}$ за $l=0$, 1, …, 2^k-1, и нека $i_l=\mathrm{wt}(x_l)$. Да означим $\bar{n}=(n_0,n_1,\ldots,n_{2^k-1})$, $\bar{\imath}=(i_0,i_1,\ldots,i_{2^k-1})$ и $i=i_0+i_1+\cdots+i_{2^k-1}$.

Лема 3.3 *Векторът x е лидер на съседен клас за C тогава и само тогава, когато $\bar{\imath}$ удовлетворява системата линейни неравенства*

$$2\hat{S}_k\,\bar{\imath}^T \leq \hat{S}_k\,\bar{n}^T. \tag{3.5}$$

Доказателство Следва директно от Лема 3.1.

Забележка Тъй като първият стълб на S_k е нулев, тази система съвпада с

$$2S_k\,(i_1,\ldots,i_{2^k-1})^T \leq S_k\,(n_1,\ldots,n_{2^k-1})^T. \tag{3.6}$$

Теорема 3.1

$$L_i = \sum_{i=i_0+i_1+\cdots+i_{2^k-1}} \kappa_{\bar{n},\bar{\imath}} \prod_{l=0}^{2^k-1} \binom{n_l}{i_l}, \tag{3.7}$$

където

$$\kappa_{\bar{n},\bar{\imath}} = \begin{cases} 0, & \text{ако } \bar{\imath} \text{ не удовлетворява системата (3.5);} \\ \dfrac{1}{N}, & \text{ако я удовлетворява и } N \text{ е броя} \\ & \quad\text{достигнати равенства.} \end{cases} \tag{3.8}$$

Доказателство На всяко $\bar{\imath}$ съответстват $\binom{n_0}{i_0}\binom{n_1}{i_1}\cdots\binom{n_{2^k-1}}{i_{2^k-1}}$ вектора $x \in F_2^n$. Ако $\bar{\imath}$ не удовлетворява системата (3.5), то според Лема 3.3 съответстващите вектори x не са лидери на съседни класове. Ако пък $\bar{\imath}$ удовлетворява системата и се достигат N равенства, то според Лема 3.2 в съседните класове, съдържащи съответните x, има точно по N вектора с тегло i. Следователно броят на тези съседни класове е N пъти по-малък от броя вектори, съответстващи на $\bar{\imath}$.

3.2 Самодопълнителни кодове

Всичко, изложено в §3.1, важи и за самодопълнителни кодове. Броят на различните възможни колони обаче не е 2^k-1, а 2^{k-1} (Виж Лема 2.3). Въпреки че при пресмятанията можем да използваме резултата от Теорема 3.1, по-удобно е да я преформулираме за самодопълнителни кодове.

Нека S'_k е $2^{k-1} \times 2^k$ матрица, чиито колони са 2^{k-1}-те възможни различни колони на k-мерен самодопълнителен код (такава матрица е кодът на Рид-Малер от първи ред $R(1,k-1)$). Номерираме колоните на тази матрица от 1 до 2^{k-1}. Нека C е $[n = n_1 + \cdots + n_2^{k-1}, k]$ самодопълнителен код, който съдържа n_l копия от l-тата колона на S'_k, $l = 1,\ 2,\ \ldots,\ 2^{k-1}$. Нека векторът $x \in F_2^n$ е представен във вида $x = (x_1,\ldots,x_{2^{k-1}})$, където $x_l \in F_2^l$, и нека $i_l = \mathrm{wt}(x_l)$, $i = i_1 + \cdots + i_{2^{k-1}}$. Означаваме $\bar{n} = (n_1,\ldots,n_{2^{k-1}})$, $\bar{\imath} = (i_1,\ldots,i_{2^{k-1}})$. Тогава, аналогично на Лема 3.3 и Теорема 3.1, имаме:

Лема 3.4 *Векторът x е лидер на съседен клас за C тогава и само тогава, когато $\bar{\imath}$ удовлетворява системата линейни неравенства*

$$2S'_k\,\bar{\imath}^T \leq S'_k\,\bar{n}^T. \tag{3.9}$$

Теорема 3.2

$$L_i = \sum_{i=i_1+\cdots+i_{2^{k-1}}} \chi_{\bar{n},\bar{\imath}} \prod_{l=1}^{2^{k-1}} \binom{n_l}{i_l}, \tag{3.10}$$

където

$$\chi_{\bar{n},\bar{\imath}} = \begin{cases} 0, & \text{ако } \bar{\imath} \text{ не удовлетворява системата (3.9);} \\[2ex] \dfrac{1}{N}, & \text{ако я удовлетворява и } N \text{ е броя} \\ & \qquad \text{достигнати равенства.} \end{cases} \tag{3.11}$$

Пример Да разгледаме $[39,4]$ кодът C:

$$C = \begin{pmatrix}
111111111111111111111111111111111111111 \\
111111100000000011111001111111111000000 \\
111111111111111100000001000000000000000 \\
111111100000000000000111000000000111111 \\
111111111111111111111110000000000000000 \\
111111100000000011111000000000000111111 \\
111111111111111100000001111111111111111 \\
111111100000000000000110111111111000000 \\
000000000000000000000000000000000000000 \\
000000011111111100000110000000000111111 \\
000000000000000011111110111111111111111 \\
000000011111111111111000111111111000000 \\
000000000000000000000001111111111111111 \\
000000011111111100000111111111111000000 \\
000000000000000011111110000000000000000 \\
000000011111111111111001000000000111111
\end{pmatrix}.$$

Той съдържа 7 копия от първата възможна колона, 9 копия от втората, 5 от третата, 2 от четвъртата, 1 от петата, 9 от седмата и 6 от осмата. От Теорема 3.2 получаваме: (приложена е програмата, изчисляваща L_i).

$$\begin{array}{lll}
L_0 = 1, & L_7 = 378230, & L_{13} = 45208408, \\
L_1 = 21, & L_8 = 1105276, & L_{14} = 64970408, \\
L_2 = 216, & L_9 = 2894989, & L_{15} = 70216344, \\
L_3 = 1472, & L_{10} = 6889128, & L_{16} = 488376000, \\
L_4 = 7579, & L_{11} = 14549324, & L_{17} = 176736000, \\
L_5 = 31943, & L_{12} = 27092986, & L_{18} = 20160000. \\
L_6 = 116352, & &
\end{array}$$

3.3 Оценки за сложността на пресмятане на $\{L_i\}$

Известно е, че задачата за пресмятане на радиуси на покритие е NP-сложна (в действителност дори $\prod_2^n$-пълна [18]). Както вече споменахме, радиусът на покритие е равен на максималната стойност на i, за която $L_i \neq 0$, така че изчисляването на разпределението на $\{L_i\}$ е поне толкова трудно, колкото и пресмятането на радиуса на покритие. Тук даваме оценка на описания в §3.1 алгоритъм в сравнение със стандартно използвания.

1. Стандартният алгоритъм използва дефиницията за лидер на съседен клас. При него трябва да се създадат всичките 2^{n-k} съседни класа, за всеки от тях да се намери вектора с минимално тегло ($O(2^k)$ операции), като междувременно се използват и по $O(n)$ операции за пресмятане на теглото на всеки вектор. Общо сложността по време е $O(n2^n)$.

   Изискванията за памет също са големи—необходим е масив с 2^n елемента. Това го прави неприложим за големи n, не може да се използва дори за разгледания пример.

2. При описания в §3.1 алгоритъм трябва да проверим дали е изпълнена системата (3.6) за всяко от $(1+n_1)(1+n_2)\dots(1+n_{2^k-1})$-те стойности на i. Горна граница за този брой е $\left(1+\frac{n}{2^k-1}\right)^{2^k-1}$. За всяка стойност на i трябва да проверим най-много 2^k неравенства (а на практика много по-малко), при проверката на едно неравенство са необходими $O(2^k)$ операции. Общо сложността по време е $O\left(2^{2k}\left(1+\frac{n}{2^k-1}\right)^{2^k-1}\right)$. Алгоритъмът е полиномиален по n и е много по-добър при фиксирано k и голямо n (т.е. при кодове с повтарящи се координати).

   Изискванията за памет също са много по-малки—основното е масив с $2^k \times 2^k$ елемента за съхраняване на матрицата на системата.

Библиография

[1] A. E. Brouwer and T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory* **IT-39** (1993), 662–677.

[2] R. A.Brualdi, V. S. Pless, and R. M. Wilson, " Short codes with a given covering radius," *IEEE Trans. Inform. Theory* **IT-35** (1989), 99–109.

[3] R. A. Brualdi and V. S. Pless, "On the length of codes with a given covering radius," *IMA Vol. Math. Appl.* **20** (1990), 9–15.

[4] A. R. Calderbank and N. J. A. Sloane, "Inequalities for covering codes," *IEEE Trans. Inform. Theory* **IT-34** (1988), 1276–1280.

[5] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, "Covering radius—survey and recent results," *IEEE Trans. Inform. Theory* **IT-31** (1985), 328–343.

[6] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inform. Theory* **IT-32** (1986), 680–694.

[7] S. M. Dodunekov, K. N. Manev, and V. D. Tonchev, "On the covering radius of binary $[14, 6]$ codes containing the all-one vector," *IEEE Trans. Inform. Theory* **IT-34** (1988), 591–593.

[8] R. Dougherty and H. Janwa, "Covering radius computations for binary cyclic codes," *Math. Comp.* **57** (1991), no. 195, 415–434.

[9] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory* **IT-31** (1985), 385–401.

[10] I. S. Honkala, "Modified bounds for covering codes," *IEEE Trans. Inform. Theory* **IT-37** (1991), 351–365.

[11] X.-D. Hou, "New lower bounds for covering codes," *IEEE Trans. Inform. Theory* **IT-36** (1990), 895–899.

[12] X.-D. Hou, "An improved sphere covering bound for the codes with $n = 3R + 2$," *IEEE Trans. Inform. Theory* **IT-36** (1990), 1476–1478.

[13] H. Janwa and H. F. Mattson, Jr., "On the normality of binary linear codes," *IEEE Trans. Inform. Theory* (to appear).

[14] K. E. Kilby and N. J. A. Sloane, "On the covering radius problem for codes: (i) bounds on normalized covering radius, (ii) codes of low dimension; normal and abnormal codes," *SIAM J. Algebraic Discrete Methods* **8** (1987), 604–627.

[15] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes,* North-Holland, Amsterdam, 1977.

[16] K. N. Manev, "LINCOR—A system for linear codes researches," in *Mathematics and Education in Mathematics, Proc. 16th Spring Conf. of the Union of Bulgarian Mathematicians,* Sunny Beach (1987), 500–503.

[17] K. N. Manev and N. B. Mateev, "On the weight distribution of the leaders of cosets for some linear binary codes," *Proc. Third Int. Workshop on Algebraic and Combinatorial Coding Theory, Voneshta Voda* (1992), 126–129.

[18] A. McLoughlin, "The complexity of computing the covering radius of a code," *IEEE Trans. Inform. Theory* **IT-30** (1984), 800–804.

[19] J. Simonis, "The minimal covering radius $t[15, 6]$ of a six-dimensional binary linear code of length 15 is equal to 4," *IEEE Trans. Inform. Theory* **IT-34** (1988), 1344–1345.

[20] N. J. A. Sloane, "A new approach to the covering radius of codes," *J. Combin. Theory Ser. A* **42** (1986), 61–86.

[21] J. H. van Lint, "Recent results on covering problems," *Lect. Notes Comput. Sci.* **357** (1989), 7–21.

[22] G. J. M. van Wee, "Improved sphere bounds on the covering radius of codes," *IEEE Trans. Inform. Theory* **IT-34** (1988), 237–245.

[23] G. J. M. van Wee, "More binary covering codes are normal," *IEEE Trans. Inform. Theory* **IT-36** (1990), 1466–1470.

[24] Z. Zhang and C. Lo, "Lower bounds on $t[n, k]$ from linear inequalities," *IEEE Trans. Inform. Theory* **IT-38** (1992), 194–197.

[25] Z. Zhang and C. Lo, "Linear inequalities for covering codes. II. Triple covering inequqlities," *IEEE Trans. Inform. Theory* **IT-38** (1992), 1648–1662.

[26] С. Х. Буюклиева, "Минимален радиус на покритие на $[16, 7]$ кодовете," Дипломна Работа, Софийски Университет (1988).