БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ЕМИЛ МИЛАНОВ КОЛЕВ

ОПТИМАЛНИ КОДОВЕ И ЗАДАЧИ ЗА ТЪРСЕНЕ

Д И С Е Р Т А Ц И Я

за придобиване на научната степен
„доктор на математическите науки“
по научна специалност
01.01.02 – Алгебра и теория на числата

БАН, София, 2014 г.

Съдържание

У В О Д

Настоящият труд е посветен на изследвания, свързани с:

- намиране на точни стойности за мощността на оптимални двоични кодове със зададена дължина и минимално разстояние и определяне на броя на нееквивалентните оптимални кодове със съответните параметри;
- намиране на точни стойности и получаване на граници за мощността на оптимални покриващи кодове;
- намиране на точни стойности за мощността на покрития на $\mathbb{F}_3^n$ със сфери и определяне броя на нееквивалентните оптимални покрития;
- задачи за неадаптивно търсене на неизвестен елемент с множества с равни тегла;
- една двумерна задача за адаптивно търсене.

Нека $\mathbb{F}_q$ е поле с q елемента, а $\mathbb{F}_q^n$ е n-мерното векторно пространство над $\mathbb{F}_q$. Под *разстояние по Хеминг* между два вектора $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ и $\mathbf{y} = (y_2, y_2, \ldots, y_n)$ от $\mathbb{F}_q^n$ разбираме броя на координатите, в които те се различават, т.е.

$$d(\mathbf{x}, \mathbf{y}) = |\{i \mid x_i \neq y_i\}|.$$

Всяко подмножество C на n-мерното векторно пространство $\mathbb{F}_q^n$ наричаме q-ичен код. Минимално разстояние d на код C се дефинира като най-малкото от разстоянията между две различни кодови думи. С $(n, M, d)_q$ означаваме код над $\mathbb{F}_q$ с дължина n, минимално разстояние d и мощност M. Във връзка с коригиращите възможности на един код основната задача на теорията на кодирането е при зададени n, q и d да се намери най-голямото M, за което съществува $(n, M, d)_q$ код. Тази най-голяма стойност се бележи с $A_q(n, d)$.

Определянето на точната стойност на функцията $A_q(n,d)$ е трудна изследователска задача [56]. За доказване на неравенството $A_q(n,d) \geq M$ трябва да се конструира $(n,M,d)_q$ код, а за доказване на неравенството $A_q(n,d) < M$ трябва да се покаже, че не съществува $(n,M,d)_q$ код. В първите години на развитие на теорията на кодирането, когато използването на компютърни пресмятания е ограничено, за намиране на граници за тази функция се използват чисто комбинаторни подходи.

Особен интерес предизвиква намирането на $A(n,3) = A_2(n,3)$, като във всеки момент усилията на изследователите основно са насочени към първия открит случай, т.е. най-малката стойност на n, за която стойността на $A(n,3)$ не е определена.

При изследване на функцията $A(n,3)$ особено важни се оказват следните свойства.

$$A(n+1,d) \leq 2A(n,d) \quad \text{и} \quad A(n,2d-1) = A(n+1,2d).$$

Когато знаем точната стойност на $A(n,d)$, неравенството дава горна граница за $A(n+1,d)$. Равенството показва, че задачата за определяне на функцията $A(n,d)$ за четни d е еквивалентна на задачата за определяне на тази функция за нечетни d.

Намирането на точните стойности на $A(n,3)$ за $n \leq 7$ не представлява особена трудност и е свързано със съществуването на $(7,16,3)$ двоичен код на Хеминг. Известно е, че $A(3,3) = 2$, $A(4,3) = 2$, $A(5,3) = 4$, $A(6,3) = 8$ и $A(7,3) = 16$. Да отбележим, че всички оптимални кодове, доказващи тези стойности се получават чрез скъсяване на $(7,16,3)$ кода на Хеминг.

Стойностите $A(8,3) = 20$ и $A(9,3) = 40$ са намерени в статиите [2] и [3] съответно през 1978 г. и 1980 г. По този начин първият открит случай остава намирането на $A(10,3)$, като поради $A(n+1,d) \leq 2A(n,d)$, имаме $A(10,3) \leq 80$.

През 1965 г. Julin [27] използва Щайнеровата система $S(5,6,12)$ (която е единствена), добавя 6 вектора с тегло 2 и 6 вектора с тегло 10 и получава $(12,144,4)$ двоичен код. Поради $A(11,3)=A(12,4)$, намираме $A(11,3)=144$. Сега от $A(11,3)\leq 2A(10,3)$ следва неравенството $A(10,3)\geq 72$.

През 1980 г. Best в [3] доказва $A(10,3)\leq 79$, след което през 1994 г. Litsyn и Vardy в [55] показват, че $A(10,3)\leq 78$. През 1995 г. Klein, Litsyn и Vardy в [34] намират границата $A(10,3)\leq 76$ и през 1998 г. Колев в [35] доказва, че $A(10,3)\leq 74$.

Във втора глава ще докажем, че $A(10,3)=72$, откъдето ще следва и равенството $A(11,3)=144$. Освен това ще докажем, че съществуват 562 нееквивалентни $(10,72,3)$ кода и 7398 нееквивалентни $(11,144,3)$ кода [61].

Друга важна характеристика на един код C е неговият *радиус на покритие*. Това е най-малкото естествено число R със следното свойство: за всеки вектор $\mathbf{x}$ съществува кодова дума $\mathbf{y}\in C$, за която $d(\mathbf{x},\mathbf{y})\leq R$. С други думи, кълбетата с радиус R и центрове кодовите думи, покриват $\mathbb{F}_q^n$. С $(n,M)_qR$ означаваме q-ичен код с дължина n, мощност M и радиус на покритие R.

Основната задача при задачи за покритие е при дадени n, q и R да намерим минималната мощност на q-ичен код с дължина n и радиус на покритие R. Тази най-малка стойност се бележи с $K_q(n,R)$. Както и при определяне на точните стойности на $A_q(n,d)$, намирането на $K_q(n,R)$ за малки стойности на n не представлява особена трудност. За да докажем равенството $K_q(n,R)=M$ е необходимо да конструираме $(n,M)_qR$ код и да докажем несъществуването на $(n,M-1)_qR$ код.

Възможно е да се разгледат и *смесени покриващи кодове*. Това са кодове, при които различните координати са от различни полета. С

$$(q_1,q_2,\ldots,q_m;n_1,n_2,\ldots,n_m;M)R$$

означаваме код с n_i координати от $\mathbb{F}_{q_i}$ за $i=1,2,\ldots,m$, мощност M и радиус на покритие R. В този случай съответната най-малка стойност се дефинира

като

$$K_{q_1,q_2,\ldots,q_m}(n_1,n_2,\ldots,n_m;R)=\min\{M \mid \exists\ (q_1,\ldots,q_m;n_1,\ldots,n_m;M)R \text{ код}\}.$$

Задачата за определяне на минималната мощност на смесени кодове с двоични и троични координати има пряка връзка с играта ТОТО 1 на спортния тотализатор. Да допуснем, че при игра на ТОТО 1 знаем със сигурност как ще завършат част от срещите, за други b срещи знаем, че даден резултат е невъзможен и за някои t срещи не можем да предвидим нищо. Искаме да направим минимален възможен брой предположения (или колонки) така, че да си гарантираме познаването на $13-R$ срещи за $R=1,2,3$ (тъй като печалби при ТОТО 1 се изплащат при познати поне 10 срещи). Използвайки кодовите думи на $(3,2;t,b)R$ код, можем да конструираме система за ТОТО 1, при която да си осигурим $13-R$ познати резултата. Приети са означенията $K(n,R)=K_2(n,R)$, $\sigma_n=K_3(n,1)$, $K(t,b,R)=K_{3,2}(t,b,R)$ [19].

На изследването на функциите $K_q(n,R)$ и $K_{q_1,q_2,\ldots,q_m}(n_1,n_2,\ldots,n_m;R)$ са посветени значителен брой статии: [4], [8], [9], [10], [11], [12], [18], [19], [20], [21], [22], [23], [24], [31], [54], [56], [58], [59], [60], [67], [68], [69], [70], [75], [76], [77], [78], [79], [80], [81].

За намиране на горни граници за функцията $K_q(n,R)$ (съответно $K_{q_1,q_2,\ldots,q_m}(n_1,n_2,\ldots,n_m;R)$) трябва да конструираме „добър“ покриващ код, т.е. код с минимален възможен брой кодови думи. Използват се различни методи за конструиране:

1. Директни конструкции – използват се известни покриващи кодове за конструиране на нови такива [19], [65].

2. Матричен метод – търси се матрица с определени свойства, с чиято помощ се дефинира покриващ код [4], [29].

3. Комбинаторни конструкции – в зависимост от конкретните параметри на търсения код се намира подходяща конструкция [66].

Несъществуването на покриващ код с дадени параметри се доказва с използването на комбинаторни аргументи. В [7], [8], [10], [11], [17], [19], [20], [21], [77] са представени различни методи за получаване на двоични покриващи кодове, както и методи за получаване на добри долни граници.

Основните компютърни методи за получаване на долни граници за покриващи кодове са simulated annealing и tabu search [58], [60], [80].

Една универсална долна граница се дава от $K_2(n,1) \geq \dfrac{2^n}{n+1}$, която при четни n може да бъде подобрена до $K_2(n,1) \geq \dfrac{2^n}{n}$.

В Глава 3 са получени следните резултати за покриващи кодове:

1. Доказана е границата $K_2(9,1) \geq 57$;

2. Намерени са точните стойности

$$K_{3,2}(1,5,1) = 16,\ K_{3,2}(2,4,1) = 20,$$

$$K_{3,2}(4,2,1) = 36,\ K_{3,2}(5,0,2) = 8,\ K_{3,2}(4,1,2) = 6.$$

3. Намерени са точните стойности

$$K_{3,2}(2,2R+1,R) = 6, \quad K_{3,2}(2,2R-1,R) = 4,$$

$$K_{3,2}(2,2R,R) = 6, \qquad K(3,2R-2,R) = 5.$$

В Глава 3 е разгледана и задачата за покриване на $\mathbb{F}_3^n$ със сфери с радиус n, [5], [64], [71]. Постановката на задачата е следната: За дадено естествено число n да се намери минималният възможен брой сфери с радиус n, които покриват $\mathbb{F}_3^n$.

Кодът C над $\mathbb{F}_3$ с дължина n се нарича *покритие* на $\mathbb{F}_3^n$, ако за всеки вектор $\mathbf{x}$ от $\mathbb{F}_3^n$ съществува кодова дума $\mathbf{y}$ такава, че $d(\mathbf{x},\mathbf{y}) = n$. Означаваме минималния брой елементи на покритие на $\mathbb{F}_3^n$ с $T(n)$. В [5] е представена таблицата, даваща известните резултати.

n	T(n)	7	29
1	2	8	44
2	3	9	66–68
3	5	10	99–104
4	8	11	149–172
5	12	12	224–264
6	18	13	336–408

В същата статия е доказано, че покритието на $\mathbb{F}_3^7$ с 29 сфери е единствено с точност до еквивалентност. Поставена е задачата за определяне дали покритието на $\mathbb{F}_3^8$ с 44 сфери е единствено. В [48] е доказано, че съществуват две нееквивалентни покрития на $\mathbb{F}_3^8$. Освен това в [51] се намира и точната стойност $T(9) = 68$, което води до подобряване на известните граници за $T(n)$ при $10 \leq n \leq 13$, както следва $T(10) \geq 102$, $T(11) \geq 153$, $T(12) \geq 230$ и $T(13) \geq 345$.

В Глава 4 са разгледани две задачи за търсене. Първата задача е за неадаптивно търсене на неизвестен елемент с множества с равни тегла. Втората задача е за двумерно адаптивно търсене.

Нека x е неизвестен елемент от дадено теглово множество A с 2^n елемента, като можем да приемем, че $A = \{1, 2, 3, \ldots, 2^n\}$. Това означава, че на всеки елемент от A е съпоставено реално число, наречено тегло на този елемент. Имаме право да задаваме въпроси от вида: принадлежи ли x на дадено подмножество B на A, при положение, че теглото на множеството B (т.е. сбора от теглата на елементите на B) е равно на дадено естествено число S.

При класическата задача за търсене, когато за множествата-въпроси нямаме никакви ограничения, за решаване на съответната задача за търсене са ни необходими поне $\log_2 |A| = n$ въпроса.

Естественото число S се нарича *добро*, ако съответната задача за търсене е решима, т.е. неизвестния елемент x може да бъде намерен с неадаптивно търсене. Това означава, че съществува някакъв брой от множества-въпроси, с помощта на които се намира x. За различни добри стойности на S броят на множествата-въпроси за намиране на x е различен. Естественото число S се нарича *подходящо*, ако неизвестния елемент x може да бъде намерен с минималния възможен брой въпроси.

В Глава 4 са представени резултати, получени в [14], [15], [42], [43], [44], [45], [46], [47], [50], [53]. За теглова функция $\mathrm{w}(i) = i$ основните резултати са получени в [42], [43] и са както следва.

1. Естественото число S е добро тогава и само тогава, когато

$$S \in [2^n - 1, 2^{2n-1} - 2^{n-1} + 1].$$

2. Ако $n \neq 2^k$, то числото S е подходящо тогава и само тогава, когато

$$S \in \left[2^{2n-2} + 2^{n-2} - \frac{\binom{2n-1}{n-1}}{2}; 2^{2n-2} + 2^{n-2} + \frac{\binom{2n-1}{n-1}}{2}\right].$$

3. За $n = 2^k$, $k \geq 2$ числото S е подходящо тогава и само тогава, когато

$$S \in \left[2^{2n-2} + 2^{n-2} - \frac{1}{2}\left(\binom{2n-1}{n-1} - 1\right); 2^{2n-2} + 2^{n-2} + \frac{1}{2}\left(\binom{2n-1}{n-1} - 1\right)\right].$$

За теглова функция $\mathrm{w}(i) = \left[\frac{i-1}{2^{n-1}}\right] + 1$ в [45] е доказано, че при нечетни n числото S е подходящо тогава и само тогава, когато

$$S \in \left[3.2^{n-2} - \binom{n-2}{t}, 3.2^{n-2} + \binom{n-2}{t}\right].$$

За теглова функция $\mathrm{w}(i) = \left[\frac{i-1}{2^{n-2}}\right] + 1$ в [46] е намерен интервал от подходящи числа.

Разгледана е задачата за търсене на два елемента [47]. Доказано е следното твърдение:

При неадаптивно търсене на два елемента без грешни отговори, числото S е добро тогава и само тогава, когато

$$S \in \left[2^n - 1, 2^{2n-1} - 2^{n-1} + 1\right].$$

Когато в отговорите се допуска един грешен, решаването на съответната задача за търсене е свързано със съществуването на двоичен код с минимално разстояние 3 и с определени свойства [44]. Намерени са граници за добрите числа в някои частни случаи, както и връзка между циклични кодове с нечетна дължина и намирането на долна и горна граници за добрите числа.

Втората задача, разгледана в Глава 4, е една задача за двумерно търсене, предложена от Katona [30]. Множеството

$$\mathcal{A}(m,n) = \{(i,j) \mid i.j \in \mathbf{Z}, 1 \leq i \leq m, 1 \leq j \leq n\}$$

се нарича правоъгълник с размерност $m \times n$. Когато $m = n$ казваме, че е даден квадрат с размерност n.

За два елемента $\mathbf{a} = (a_1, a_2) \in \mathcal{A}(m,n)$ и $\mathbf{b} = (b_1, b_2) \in \mathcal{A}(m,n)$ записваме $\mathbf{a} \leq \mathbf{b}$ тогава и само тогава, когато $a_1 \leq b_1$ и $a_2 \leq b_2$. Както в класическата задача за търсене, нека е избран елемент $\mathbf{x} \in \mathcal{A}(m,n)$, който не ни е известен.

Искаме да намерим неизвестния елемент с минималния брой въпроси от вида: Вярно ли е, че $\mathbf{x} \leq \mathbf{a}$?

Задаването на въпрос е еквивалентно на посочването на елемент на $\mathcal{A}(m,n)$. Разглеждаме неадаптивно търсене, което означава, че всеки въпрос се задава след като е получен отговора на предишния.

В Глава 4 е доказано [53], че за всяко m от вида $m = \dfrac{2^{si} - 1}{2^s - 1}$ и всяко n правоъгълникът $\mathcal{A}(m,n)$ е разрешим. Решени са задачи, поставени в [72], като са намерени най-малкият неразрешим правоъгълник $\mathcal{A}(11,93)$ и най-малкият неразрешим квадрат $\mathcal{A}(181,181)$.

Апробация на резултатите

В дисертацията са включени резултати, получени в периода 1993 г. – 2013 г. Резултатите, представени в публикации [P3], [P5], [P6], [P9], [P10], [P11], [P12], [P15], [P16], [P17], [P18], [P19] и [P20] са получени самостоятелно. Останалите резултати са получени в съавторство, както следва:

Ланджев	[P1], [P2]
Hill	[P7]
Байчева	[P4], [P21], [P22]
Байчева, Östergård	[P8]
Дичев	[P13], [P14]

Част от резултатите са публикувани в научни списания, както следва:

Lecture Notes in Computer Science	[P1]
Applied Algebra, Algebraic Algorithms and Error-Corr. Codes	[P3]
Discrete Mathematics	[P7]
IEEE Trans on Information Theory	[P8]
CR Acad. Bulg. Sci.	[P5], [P20]
Central European Journal of Mathematics	[P12]
Utilitas Mathematica	[P22]
Serdica Mathematical Journal	[P2], [P11]

Част от резултатите са докладвани на международни научни конференции, както следва:

International Workshop on Algebraic and Combinatorial Coding Theory: [P6], [P10], [P13], [P16], [P17], [P19];

International Workshop Optimal Codes and Related Topics: [P4], [P15], [P18], [P21];

International congress MASSEE: [P13];

Swedish-Bulgarian Government IT Security Conference Information Security in the 21th Century: Global Convergence: [P9];

British Combinatorial Conference, 1997, Milton Keyns, UK: [P7];

Eleventh Intern. Symposium AAECC, Paris 1995: [P3];

First French-Israeli Workshop on Algebraic Coding: [P1].

Отделни резултати от дисертацията са докладвани пред Националния семинар по теория на кодирането, както и на семинари в Институт по математика, Унгарска Академия на Науките, Salford University, University of East Anglia, Norwich, University of Bilbao.

Авторска справка

По мнение на автора, основните приноси на дисертационния труд са:

- Определяне на точните стойности $A(10,3) = 72$ и $A(11,3) = 144$, и намиране на всички нееквивалентни 562 кода с параметри $(10, 72, 3)$ и всички нееквивалентни 7398 кода с параметри $(11, 144, 3)$.

- Намиране на граници и точни стойности за оптимални покриващи кодове, както следва: $K_2(9,1) \geq 57$, $K_{3,2}(1,5,1) = 16$, $K_{3,2}(2,4,1) = 20$, $K_{3,2}(4,2,1) = 36$, $K_{3,2}(5,0,2) = 8$, $K_{3,2}(4,1,2) = 6$, $K_{3,2}(2,2R+1,R) = 6$, $K_{3,2}(2,2R-1,R) = 4$ и $K_{3,2}(2,2R,R) = 6$.

- Определяне на броя на оптималните нееквивалентни покрития със сфери на $\mathbb{F}_3^8$ и намиране на точната стойност $T(9) = 68$ – минималния брой сфери с радиус 9, които покриват $\mathbb{F}_3^9$.

- Намиране на необходими и достатъчни условия едно число да е добро или подходящо при неадаптивно търсене на неизвестен елемент в тегловно множество без грешни отговори.

- Намиране на необходими и достатъчни условия едно число да е добро при неадаптивно търсене в тегловно множество на два неизвестни елемента без грешни отговори.

- Намиране на граници за подходящите числа при неадаптивно търсене в тегловно множество с най-много един грешен отговор. Показване на връзка между цикличните кодове и конструиране на подходящи матрици.

- Доказване, че за всяко m от вида $m = \dfrac{2^{si}-1}{2^s-1}$ и всяко n правоъгълникът $\mathcal{A}(m,n)$ е разрешим. Намиране на най-малкият неразрешим правоъгълник $\mathcal{A}(11,93)$ и най-малкият неразрешим квадрат $\mathcal{A}(181,181)$.

Глава 1

Основни понятия и предварителни резултати

В тази глава ще въведем основните понятия и дефиниции, необходими за представяне на резултатите. Пълна и изчерпателна информация за теорията на кодове, коригиращи грешки и възникващите от нея задачи, може да се намери в [25] и [56].

С $\mathbb{F}_q$ ще означаваме крайно поле с q елемента. Нека $\mathbb{F}_q^n$ е n-мерното векторно пространство над $\mathbb{F}_q$.

Дефиниция 1.0.1. Под *разстояние по Хеминг* $d(\mathbf{x}, \mathbf{y})$ между два вектора $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ и $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ от $\mathbb{F}_q^n$ разбираме броя на координатите, в които те се различават, т.е.

$$d(\mathbf{x}, \mathbf{y}) = |\{i \mid x_i \neq y_i\}|.$$

Броят на ненулевите координати на вектор $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ се нарича *тегло* на вектора $\mathbf{x}$ и се бележи с $wt(\mathbf{x})$.

Разстоянието по Хеминг задава метрика в $\mathbb{F}_q^n$, тъй като са изпълнени следните свойства:

1. $d(\mathbf{x}, \mathbf{y}) = 0 \iff \mathbf{x} = \mathbf{y}$;

2. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;

3. $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{y}, \mathbf{z})$.

Директно се проверява, че за всеки два вектора $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ и $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ е изпълнено равенството:

$$d(\mathbf{x}, \mathbf{y}) = wt(x) + wt(y) - 2.wt(x \star y),$$

където $\mathbf{x} \star \mathbf{y} = (x_1y_1, x_2y_2, \ldots, x_ny_n)$,

Дефиниция 1.0.2. *Скаларно произведение* на векторите $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ и $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ се дефинира като

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

Дефиниция 1.0.3. Всяко подмножество C на n-мерното векторно пространство $\mathbb{F}_q^n$ се нарича q-ичен код с дължина n. Елементите на C се наричат кодови думи, а техният брой – мощност на кода. Когато множеството C представлява линейно подпространство на $\mathbb{F}_q^n$, кодът се нарича *линеен*. Размерността на C като линейно подпространство е *размерност на кода. Пораждаща матрица* на един линеен код е матрица, чийто редове представляват базис на кода като линейно пространство.

Дефиниция 1.0.4. *Минимално разстояние* на код C се дефинира като най-малкото от разстоянията между две различни кодови думи:

$$d(C) = \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

С $(n, M, d)_q$ се бележи код с дължина n над полето $\mathbb{F}_q$, с мощност M и минимално разстояние d. С $[n, k, d]_q$ се бележи линеен код над $\mathbb{F}_q$ с дължина n, размерност k и минимално разстояние d. Ясно е, че един $[n, k, d]_q$ код има $M = q^k$ кодови думи.

За даден линеен код C с $C^{\perp}$ бележим кода, съставен от всички вектори, които са ортогонални (т.е. скаларното им произведение е равно на нула) на всяка кодова дума от C. Всяка пораждаща матрица за кода $C^{\perp}$ се нарича *проверочна матрица* за C. Всяка пораждаща матрица на $[n, k, d]$ има размери $k \times n$, докато всяка проверочна матрица е с размери $(n-k) \times n$.

Дефиниция 1.0.5. За всяко цяло число $r \geq 0$ и вектор $\mathbf{x} \in \mathbb{F}_q^n$ с $\mathcal{B}(\mathbf{x}, r)$ означаваме множеството от всички вектори, на разстояние не надминаващо r от $\mathbf{x}$:

$$\mathcal{B}(\mathbf{x}, r) = \{\mathbf{y} \in \mathbb{F}_q^n \mid d(\mathbf{x}, \mathbf{y}) \leq r\}.$$

Множеството $\mathcal{B}(\mathbf{x}, r)$ се нарича *кълбо с център* $\mathbf{x}$ *и радиус* r.

При използване на кодове за предаване или съхранение на информация, минималното разстояние на даден код е свързано с възможностите на кода да открива или поправя грешки [25], [56]. В сила е следното твърдение:

Лема 1.0.1. Код с минимално разстояние d открива до $d-1$ и поправя до $\left[\frac{d-1}{2}\right]$ грешки.

Код с по-малка дължина позволява по-бързо предаване на информацията. От друга страна, кодове с по-голяма мощност позволяват предаване на по-голям брой различни съобщения.

Ето защо един добър код би трябвало да има малка дължина n (за по-бързо предаване на кодовите думи), голямо M (за предаване на по-голям брой различни съобщения) и голямо d (за да поправя повече грешки).

Ясно е, че горните изисквания са в противоречие. Поради това в теорията на кодирането се поставя въпроса за дадени стойности на n, d и q да се намери най-голямото M, за което съществува $(n, M, d)_q$ код. Тази най-голяма стойност на M се означава с $A_q(n, d)$.

Основната задача в теорията на кодирането е намирането на точните стойности на функцията $A_q(n, d)$.

Дефиниция 1.0.6. *Радиус на покритие* на код C се нарича най-малкото естествено число R, за което кълбетата с радиус R и центрове кодовите думи покриват цялото пространство $\mathbb{F}_q^n$.

Нека C е код с минимално разстояние d и радиус на покритие R. При произволна пермутация на координатите на C и произволна пермутация на символите във всяка координата, минималното разстояние за новия код C' не се променя. Лема 1.0.1 показва, че от гледна точка на коригиращите възможности на кода, двата кода имат едни и същи свойства.

Дефиниция 1.0.7. Два кода над $\mathbb{F}_q$ се наричат *еквивалентни*, ако единият може да бъде получен от другия чрез последователно прилагане на следните еквивалентни трансформации:

(1) пермутация на координатите;

(2) пермутация на символите, във всяка от координатите.

При търсене на кодове, имащи определени свойства, се описват всички такива кодове с точност до еквивалентност.

За даден код с дължина n да означим с A_i, $i = 0, 2, \ldots, n$ броя на кодовите думи с тегло i. Особено важна характеристика на един код е множеството $\{A_i\}_{i=0}^n$, което се нарича *тегловно разпределение* на кода. Тегловното разпределение не е инвариантa при прилагане на еквивалентни трансформации.

За всяко $i = d, d+1, \ldots, n$ да означим с B_i броя на ненаредените двойки от различни кодови думи, разстоянието между които е равно на i. Директно се проверява, че еквивалентните трансформации запазват разстоянието между векторите, което означава, че множеството $\{B_i\}_{i=d}^n$ е инвариантно при прилагане на еквивалентните трансформации.

Кодовете на Хеминг са важна фамилия от линейни кодове с минимално разстояние 3. Те могат да бъдат дефинирани над всяко крайно поле, но за целите на настоящото изложение, ще се ограничим с двоичните и троичните кодове на Хеминг.

Дефиниция 1.0.8. За произволно естествено число r нека H е матрицата, чиито стълбове са всички ненулеви непропорционални двоични (съответно троични) вектори с дължина r. Линейният код C с проверочна матрица H се нарича *двоичен (съответно троичен) код на Хеминг*.

Тъй като броят на ненулевите непропорционални двоични вектори с дължина r е $2^r - 1$, то матрицата H е с размери $r \times (2^r - 1)$. Следователно двоичният код на Хеминг има параметри $[n = 2^r - 1, k = n - r, 3]$ и има $2^{2^r - r - 1}$ кодови думи. Аналогично получаваме, че троичният код на Хеминг има параметри $\left[n = \dfrac{3^r - 1}{2}, k = n - r, 3\right]$ и следователно има 3^{n-r} кодови думи.

Кодовете на Хеминг притежават и друго важно свойство. Те имат минимално разстояние 3, което означава, че сферите с центрове кодовите думи и радиус 1 не се пресичат. Освен това те имат радиус на покритие 1, което означава, че всеки вектор се съдържа в някоя сфера с център кодова дума и радиус 1. Такива кодове се наричат *съвършени*. В общия случай, за q-ичен съвършен код с параметри $(n, M, d = 2t + 1)$ е изпълнено равенството

$$M\left[1 + (q-1)n + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t}\right] = q^n.$$

Да разгледаме n мерното векторно пространство $\mathbb{F}_q^n$.

Дефиниция 1.0.9. С $P_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s}$ означаваме множеството от всички вектори, имащи i_t в позиция p_t за $t = 1, 2, \ldots, s$. Множеството $P_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s}$ се нарича *равнина*.

Броят на кодовите думи в дадена равнина е важна характеристика на един код и често се използва при основните комбинаторни подходи. Нека $\mathcal{C}$ е двоичен (n, M, d) код.

Дефиниция 1.0.10. Дефинираме множеството $C_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s}$ като всички кодови думи с дължина $n-s$, получени от кодовите думи от $P_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s}$ чрез изтриване

на координати $p_1, p_2, \ldots, p_s$. Елементите на $C_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s}$ се наричат *опашки в равнината* $P_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s}$. С $c_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s}$ означаваме броя на елементите на множеството $C_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s}$, т.е.

$$c_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s} = \mid C_{i_1 i_2 \ldots i_s}^{p_1 p_2 \ldots p_s} \mid.$$

За опростяване на записването, когато изпускаме горните индекси във всяка от горните дефиниции ще считаме, че разглеждаме първите s координати. Например, с $P_{i_1 i_2 \ldots i_s}$ означава множеството $P_{i_1 i_2 \ldots i_s}^{12 \ldots s}$, а с C_0 означаваме множеството от всички вектори, получени от кодовите думи с първа координата 0, след изтриване на тази координата.

Глава 2

Оптимални двоични кодове с минимално разстояние 3

В тази глава са представени резултатите, получени в [1], [35], [61]. Основният резултат е определянето на точните стойности $A(10,3) = 72$ и $A(11,3) = 144$, както и намирането на всички 562 нееквивалентни $(10, 72, 3)$ кода и всички 7398 нееквивалентни $(11, 144, 3)$ кода. За целта са класифицирани кодове с по-малка дължина, след което съответните кодове са разширявани и тествани за еквивалентност.

Да припомним, че основната задача на теорията на кодирането е намиране на максималната мощност на код над поле с q елемента, със зададени дължина n и минимално разстояние d. Това означава, че търсим стойността на функцията $A_q(n,d)$, където:

$$A_q(n,d) = \max\{M \mid \text{съществува } (n,M,d)\ q\text{–ичен код }\}.$$

След намиране на стойността на $A_q(n,d)$ се поставя задачата за описание на всички оптимални кодове, т.е. за намирането на всички нееквивалентни $(n,M,d)_q$ кодове, за които $M = A_q(n,d)$. Да означим с $B_q(n,d)$ броя на нееквивалентните q-ични кодове с дължина n, минимално разстояние d и $A_q(n,d)$

кодови думи.

В тази глава ще разгледаме задачата за намиране на максималната мощност на двоични кодове с дължини $n \leq 10$ и минимално разстояние $d = 3$, както и за намирането на всички нееквивалентни оптимални кодове. Понеже всички разглеждани кодове са двоични, за опростяване на записването, ще използваме означенията $A(n,d) = A_2(n,d)$ и $B(n,d) = B_2(n,d)$.

Ще докажем, че за $A(n,3)$, $B(n,3)$ и $B(n+1,4)$, за $n \leq 11$ са в сила стойностите от дадената таблица.

n	3	4	5	6	7	8	9	10	11
$A(n,3) = A(n+1,4)$	2	2	4	8	16	20	40	72	144
$B(n,3)$	1	2	1	1	1	5	1	562	7398
$B(n+1,4)$	1	2	1	1	1	3	1	96	1041

2.1 История на задачата

Изучаването на функцията $A(n,d)$ предизвиква значителен интерес, особено в първите години на развитие на теорията на кодирането. На тази задача са посветени значителен брой изследвания, като във всеки момент особен интерес предизвиква най-малката стойност на n, за която съответната стойност на $A(n,d)$ не е определена [25], [56].

Всяко, макар и малко, подобрение на съществуващите граници се оказва стъпка към постигане на крайната цел – определяне на точната стойност на $A(n,d)$ за съответното n. За целта се търсят горни и долни граници, като тяхното подобряване евентуално води до намиране и на точната стойност.

Долните граници за $A(n,d)$ са винаги конструктивни, т.е. съществуването на (n,M,d) код означава, че $A(n,d) \geq M$. За намирането на подходящи кодове (такива с голяма мощност) се използват различни подходи. При „малки“ стойности на n построяването на оптимален код може да се извърши с

помощта на комбинаторни съображения. Оказва се, че с увеличаването на n, трудността на задачата нараства експоненциално, т.е. получаването на кодове с голяма мощност с използването на чисто комбинаторни разсъждения рядко води до намирането на оптимални кодове.

За намиране на горни граници за $A(n,d)$ се използват комбинаторни методи. За доказване, че $A(n,d) < M$ трябва да се докаже, че не съществува (n,M,d) код. Основната трудност е свързването на „локалната“ характеристика минимално разстояние d с „глобалната“ характеристика брой на кодовите думи M.

Стандартният комбинаторен подход за доказване на несъществуване на (n,M,d) код включва подходящо разделяне на кодовите думи на този код на групи в зависимост от някоя от следните характеристики.

1. Брой на кодовите думи, които имат дадена стойност в една или повече фиксирани координати.

2. Брой на кодовите думи с определено тегло.

3. Брой на кодовите думи, които се съдържат в дадено фиксирано множество (например обединение на няколко сфери).

Ако чрез разглеждане на броя на кодовите думи в различните множества и връзките между тях се достигне до противоречие, то е изпълнено неравенството $A(n,d) < M$.

След започване на масовото използване на компютрите за решаването на задачи от теория на кодирането, комбинаторните подходи за намиране на оптимални кодове се съчетават с компютърни пресмятания. Особено важно в това направление става намирането на ефективни алгоритми за търсене.

Както ще се убедим в тази глава, намирането на $A(n,3)$ за малки стойности на n (например до $n \leq 7$) не представлява особена трудност. В [2] е намерена точната стойност $A(8,3) = 20$. По-късно в [3] е построен $(10,40,4)$ двоичен

код на Best, което доказва равенството $A(9,3) = 40$. От Лема 2.1.2 следва границата $A(10,3) \leq 80$. В статията [75] на Wax се твърди, че $A(10,3) \leq 78$, но както по-късно се показва в [2], това доказателство е грешно. Границата за $A(10,3)$ е подобрявана няколко пъти: през 1980 г. Best в [3] доказва $A(10,3) \leq 79$, след това през 1994 Litsyn и Vardy в [55] показват, че $A(10,3) \leq 78$, през 1995 г. Klein, Litsyn и Vardy в [34] намират границата $A(10,3) \leq 76$ и през 1998 г. Колев в [35] доказва, че $A(10,3) \leq 74$.

Подробна информация за развитието на проблема може да се намери в [56]. Подобрения на някои от границите са публикувани в [6], [9] и [28].

Ще докажем някои основни твърдения, които са необходими за получаване на резултатите от тази глава.

Една универсална горна граница за $A(n,3)$ се дава от следната лема. Тази граница е известна като *граница на сферичната опаковка.*

Лема 2.1.1. В сила е неравенството:

$$A(n,3) \leq \frac{2^n}{n+1}.$$

Доказателство. Нека C е $(n, M, 3)$ оптимален код, т.е. $M = A(n,3)$. Да припомним, че множеството

$$\mathcal{B}(\mathbf{x}, 1) = \{\mathbf{y} \in F_2^n \mid d(\mathbf{x}, \mathbf{y}) \leq 1\}$$

се нарича кълбо с център $\mathbf{x}$ и радиус 1. Първо ще докажем, че две кълбета с центрове кодови думи и радиус 1 не се пресичат. За целта да допуснем противното, т.е. кълбетата $\mathcal{B}(\mathbf{x}, 1)$ и $\mathcal{B}(\mathbf{y}, 1)$ за $\mathbf{x}, \mathbf{y} \in C$ имат общ елемент $\mathbf{z}$. Тогава $d(\mathbf{x}, \mathbf{z}) \leq 1$, $d(\mathbf{z}, \mathbf{y}) \leq 1$ и от неравенството на триъгълника имаме

$$d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y}) \leq 2,$$

което е противоречие с минималното разстояние на кода.

Тъй като в кълбо с радиус 1 се съдържат $n+1$ вектора, то във всички кълбета с центрове кодовите думи и радиус 1 се съдържат $M(n+1)$ вектора. Понеже тези кълбета не се пресичат, получаваме

$$M(n+1) \leq 2^n,$$

откъдето следва търсеното неравенство. □

Ако за даден $(n, M, 3)$ код е изпълнено $M = \dfrac{2^n}{n+1}$, то кодът се нарича съвършен. За такъв код кълбетата с центрове в кодовите думи и радиус 1 не се пресичат и покриват цялото пространство. Неравенството от Лема 2.1.1 се използва за получаване на горна граница за функцията $A(n, 3)$, въпреки че (с изключение на случаите, когато съществува съвършен код) тази граница обикновено е далече от точната стойност.

Лема 2.1.2. В сила е неравенството $A(n+1, d) \leq 2A(n, d)$.

Доказателство. Да разгледаме оптимален двоичен $(n+1, M, d)$ код C, т.е. $M = A(n+1, d)$. Тогава множеството C_0 от всички кодови думи с първа координата 0 без тази координата представлява (n, c_0, d) код. Аналогично множеството C_1 от всички кодови думи с първа координата 1 без тази координата представлява (n, c_1, d) код. Тъй като $c_i \leq A(n, d)$ за $i = 0, 1$, получаваме

$$A(n+1, d) = c_0 + c_1 \leq 2A(n, d).$$

С това лемата е доказана. □

Лема 2.1.2 показва, че когато е известна точната стойност на $A(n, d)$ (или имаме „добра“ горна граница за тази стойност) можем да намерим и горна граница за $A(n+1, d)$. Тази граница обикновено е по-добра от границата, представена в Лема 2.1.1

Свойството, представено в следващата лема показва, че задачата за намиране на $A(n+1, 2d)$ е еквивалентна със задачата за намиране на $A(n, 2d-1)$.

Лема 2.1.3. В сила е равенството $A(n, 2d-1) = A(n+1, 2d)$.

Доказателство. Да разгледаме оптимален $(n, M, 2d-1)$ код C. Това означава, че е изпълнено равенството $M = A(n, 2d-1)$. Да прибавим към всяка кодова дума една координата така, че сборът от всички координати на новополучения вектор да е четно число. Това означава, че кодовата дума $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ се трансформира в

$$\overline{\mathbf{x}} = (x_1, x_2, \ldots, x_n, x_{n+1}),$$

където сборът $x_1 + x_2 + \cdots + x_n + x_{n+1}$ е четно число, т.е. е равна на 0 в полето $\mathbb{F}_2$. Да забележим, че поради

$$d(\overline{\mathbf{x}}, \overline{\mathbf{y}}) = wt(\overline{\mathbf{x}}) + wt(\overline{\mathbf{y}}) - 2.wt(\overline{\mathbf{x}} \star \overline{\mathbf{y}}),$$

където $\overline{\mathbf{x}} \star \overline{\mathbf{y}} = (x_1y_1, x_2y_2, \ldots, x_ny_n, x_{n+1}y_{n+1})$, разстоянието между две разширени кодови думи $\overline{\mathbf{x}}$ и $\overline{\mathbf{y}}$ е четно число.

При тази трансформация кодът C се преобразува в код $\overline{C}$ с дължина $n+1$, мощност M и четно минимално разстояние, т.е. получаваме $(n+1, M, 2d)$ код. Тъй като по дефиниция $M \leq A(n+1, 2d)$, получаваме неравенството

$$A(n, 2d-1) \leq A(n+1, 2d).$$

Обратно, да разгледаме оптимален $(n+1, N, 2d)$ код. За него е изпълнено равенството $N = A(n+1, 2d)$. Ако $\mathbf{x}$ и $\mathbf{y}$ са две кодови думи на разстояние $2d$, след изтриване на една от координатите, в които $\mathbf{x}$ и $\mathbf{y}$ се различават, получаваме $(n, N, 2d-1)$ код. Тъй като по дефиниция $N \leq A(n, 2d-1)$, получаваме $A(n, 2d-1) \geq A(n, 2d)$.

Следователно $A(n, 2d-1) = A(n+1, 2d)$. □

От горната лема следва, че определяйки точната стойност на $A(n, 3)$ определяме и точната стойност на $A(n+1, 4)$ и обратното. Въпреки еквивалентността на двете задачи, понякога е по-удобно да разглеждаме едната от

тях. Това е така, тъй като съответният оптимален код притежава по-добра структура и съответно е по-достъпен за намиране и изследване. Например, кодът на Best [3] има параметри $(10, 40, 4)$. Кодовите думи се получават от цикличните премествания на четирите вектора

$$1010000001, 0000110100, 0001010111, 0111111010.$$

Тогава единственият $(9, 40, 3)$ код се получава чрез еднократно скъсяване на кода на Best.

Последователно ще намерим стойностите на $A(n, 3)$, $A(n + 1, 4)$, $B(n, 3)$ и $B(n + 1, 4)$ за $3 \leq n \leq 11$.

Да допуснем, че за някое n имаме $B(n, 3) = 1$, т.е съществува единствен $(n, M, 3)$ код C за $M = A(n, 3)$. Да разгледаме граф G_C с върхове кодовите думи на C. Два върха $\mathbf{x}, \mathbf{y} \in G_C$ са свързани с ребро тогава и само тогава, когато $d(\mathbf{x}, \mathbf{y}) = 3$. Тъй като при $d(\mathbf{x}, \mathbf{y}) = 3$ общият брой на единиците в $\mathbf{x}$ и $\mathbf{y}$ е нечетен, то в G_C няма цикли с нечетна дължина, т.е. G_C е двуделен граф. Да наречем G_C индуциран от C двуделен граф.

Сега да разгледаме оптимален $(n + 1, M, 4)$ код C_1. Тъй като $B(n, 3) = 1$ можем да считаме, че скъсяването на C_1 по последната координата води до получаване на единствения $(n, M, 3)$ код C.

Следователно кодът C_1 се получава от C чрез разширяване с една координата. При това ако за две кодови думи $\mathbf{x}$ и $\mathbf{y}$ от C имаме $d(\mathbf{x}, \mathbf{y}) = 3$, то те трябва да бъдат разширени с 0 и 1. Оттук следва, че ако G_C е свързан, то разширяването на C се извършва по единствен начин и тогава $B(n+1, 4) = 1$.

2.2 Определяне на $A(n,3)$, $B(n,3)$ и $B(n+1,4)$ за $3 \leq n \leq 9$

В тази част ще намерим стойностите на $A(n,3) = A(n+1,4)$, $B(n,3)$ и $B(n+1,4)$ за $n \leq 9$. Да отбележим, че при намирането на стойностите на $A(n,3)$, $B(n,3)$ и $B(n+1,4)$ за $n = 10, 11$ в следващата част, същите резултати ще бъдат получени отново чрез използване на компютър. Разликата е, че включените в тази част доказателства основно използват комбинаторни подходи и разсъждения. Това позволява по-добро изучаване и познаване на структурата на съответните оптимални кодове.

Първо ще определим стойностите на $A(n,3)$, $B(n,3)$ и $B(n+1,4)$ за $3 \leq n \leq 7$.

Очевидно имаме $A(3,3) = 2$, $B(3,3) = 1$ и $B(4,4) = 1$ (единственият $(3,2,3)$ код е $\{000, 111\}$, а единственият $(4,2,4)$ код е $\{0000, 1111\}$).

Доказателството на равенствата $A(4,3) = 2$ и $B(4,3) = 2$ (двата кода са $\{0000, 0111\}$ и $\{0000, 1111\}$) е тривиално. Освен това $B(5,4) = 2$, като двата нееквивалентни кода са $\{00000, 11111\}$ и $\{00000, 01111\}$.

Основна роля в по-нататъшното изложение играе двоичния код на Хеминг с дължина 7, 16 кодови думи и минимално разстояние 3. Проверочната матрица на този код е:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Кодовите му думи са:

$$\{0000000, 0001111, 1001100, 1000011, 0100101, 0101010, 0010110, 0011001,$$

$$1111111, 1110000, 0110011, 0111100, 1011010, 1010101, 1101001, 1100110\},$$

а тегловното му разпределение е $A_0 = 1$, $A_3 = 7$, $A_4 = 7$ и $A_7 = 1$.

Директно се проверява, че за този код неравенството от границата на сферичната опаковка $M(n+1) = 2^n$ става равенство. Това означава, че сферите с центрове кодовите думи и радиус 1 не се пресичат и покриват цялото пространство $\mathbb{F}_2^7$. Такъв код се нарича *съвършен*. Това означава, че $A(7,3) = 16$ и понеже $(7,16,3)$ кода на Хеминг е единствен с точност до еквивалентност, имаме $B(7,3) = 1$. Тъй като индуцирания двуделен граф за кода на Хеминг е свързан, то $B(8,4) = 1$, като единственият $(8,16,4)$ код се получава от $(7,16,3)$ кода на Хеминг чрез разширяване с проверка по четност.

Като използваме Лема 2.1.2 получаваме

$$16 = A(7,3) \leq 2A(6,3) \leq 4A(5,3) \leq 8A(4,3) = 16.$$

Следователно навсякъде в горната верига от неравенства трябва да имаме равенства, което означава, че

$$A(6,3) = 8, \quad A(5,3) = 4.$$

Остана да определим стойностите на $B(6,3)$ (съответно $B(7,4)$) и $B(5,3)$ (съответно $B(6,4)$).

Лема 2.2.1. Изпълнени са равенствата $B(5,3) = 1$ и $B(6,3) = 1$.

Доказателство. Нека C е $(5,4,3)$ код. Ще докажем, че той е единствен с точност до изоморфизъм. Тъй като според Лема 2.1.3 имаме $A(5,4) = A(4,3) = 2$, то съществуват кодови думи $\mathbf{x}, \mathbf{y} \in C$, за които $d(\mathbf{x},\mathbf{y}) = 3$. Без ограничение можем да считаме, че това са $\mathbf{x} = 00000$ и $\mathbf{y} = 00111$. Ако някоя от останалите две думи от кода има нула в някоя от първите две координати, лесно се вижда, че разстоянието до $\mathbf{x}$ или $\mathbf{y}$ е по-малко от 3. Сега е ясно, че без ограничение другите две думи са 11110 и 11001. Следователно $B(5,3) = 1$

и единственият с точност до еквивалентност $(5, 4, 3)$ код е

$$\mathcal{C} = \{00000, 00111, 11001, 11110\}.$$

Нека C е $(6, 8, 3)$ код и да разгледаме множествата от опашки C_0 и C_1. Тези две множества представляват съответно кодове с параметри $(5, c_0, 3)$ и $(5, c_1, 3)$, където $c_0 + c_1 = 8$. От това равенство и от $A(5, 3) = 4$, имаме $c_0 = c_1 = 4$, като всеки от кодовете C_0 и C_1 е еквивалентен на $\mathcal{C}$. Без ограничение можем да считаме, че C_0 съвпада с $\mathcal{C}$. Стандартни разсъждения за C_1 показват, че съществува единствен $(6, 8, 3)$ код и това е:

$$\{000000, 001111, 010101, 011010, 100110, 101001, 110011, 111100\}.$$

Следователно $B(5, 3) = 1$ и $B(6, 3) = 1$. □

От Лема 2.2.1 и от свързаността на съответните индуцирани двуделни графи следва, че $B(7, 4) = B(6, 4) = 1$.

За по-кратко записване на векторите ще представяме всеки двоичен вектор $(x_1, x_2, \ldots, x_n)$ чрез естественото число

$$x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_{n-1} 2 + x_n.$$

Например, единствените $(5, 4, 3)$ и $(6, 8, 3)$ кодове, получени в Лема 2.2.1 се записват съответно като $\{0, 7, 25, 30\}$ и $\{0, 15, 21, 26, 38, 41, 51, 60\}$.

Сега ще определим стойностите на $A(8, 3)$, $B(8, 3)$ и $B(9, 4)$. За това ще са ни необходими няколко предварителни резултата.

Лема 2.2.2. Дадено е множество $\mathcal{A}$ от вектори с дължина $n-1$ и с мощност p. Ако множеството $F_2^{n-1} \setminus \cup_{x \in \mathcal{A}} \mathcal{B}(\mathbf{x}, 1)$ може да се покрие с q сфери с радиус 1, то $(n, M, 3)$ код C, за който $C_0 \equiv \mathcal{A}$ има най-много $p + q$ кодови думи, т.е. $M \leq p + q$.

Доказателство. Да разгледаме код C, за който $C_0 \equiv \mathcal{A}$. Понеже C е $(n, M, 3)$ код, то всяка опашка от C_1 принадлежи на $F_2^{n-1} \setminus \cup_{\mathbf{x} \in C_0} \mathcal{B}(\mathbf{x}, 1)$. Тъй като това множество може да се покрие с q сфери с радиус 1 и два вектора от C_1 не принадлежат на една и съща сфера, то $c_1 \leq q$. Следователно $|C| = c_0 + c_1 \leq p + q$. □

Лема 2.2.2 показва как, при определена структура на множеството от опашки C_0, можем да получим горна граница за мощността на кода.

Сега ще намерим всички $(6, M, 3)$ кодове за $M = 6, 7, 8$.

Лема 2.2.3. С точност до еквивалентност

а) съществува единствен $(6, 8, 3)$ код:

$$D_1 = \{0, 15, 21, 26, 38, 41, 51, 60\};$$

б) съществува единствен $(6, 7, 3)$ код:

$$D_2 = \{0, 15, 21, 26, 41, 51, 60\};$$

в) съществуват четири $(6, 6, 3)$ кода:

$$D_3 = \{0, 7, 25, 42, 52, 63\},\ D_4 = \{0, 7, 25, 43, 53, 62\},$$

$$D_5 = \{0, 15, 21, 41, 51, 60\},\ D_6 = \{0, 15, 22, 37, 42, 60\}.$$

Доказателство. а) Единствеността на $(6, 8, 3)$ кода следва от доказаното в Лема 2.2.1.

б) Нека C е $(6, 7, 3)$ код. Тъй като $c_0 + c_1 = 7$, $A(5, 3) = 4$ и $B(5, 3) = 1$, без ограничение приемаме, че C_0 е единствения $(5, 4, 3)$ код. Стандартни разсъждения показват, че кодът C_1 може да бъде избран по единствен начин. Полученият код е:

$$D_2 = \{0, 15, 21, 26, 41, 51, 60\}.$$

в) Нека C е $(6,6,3)$ код. Имаме $c_0 + c_1 = 6$ и без ограничение можем да приеме, че $c_0 \geq c_1$. Тъй като $A(5,3) = 4$ са възможни два случая: $c_0 = 4$ и $c_0 = 3$.

Когато $c_0 = 4$ от единствеността на $(5,4,3)$ кода следва, че без ограничение можем да считаме, че C_0 е еквивалентен на единствения $(5,3,3)$ код, без ограничение приемаме, че

$$C_0 = \{0, 7, 25, 30\}.$$

Стандартни разсъждения за C_1 показват, че той може да бъде избран по 4 начина, като резултатът е получаване на кодовете D_3, D_4, D_5 и D_6. □

От Лема 2.1.2 и от равенството $A(7,3) = 16$ получаваме неравенството $A(8,3) \leq 2A(7,3) = 32$. Оказва се, че тази граница е далече от точната стойност на $A(8,3)$.

Лема 2.2.4. Изпълнено е равенството $A(8,3) = 20$.

Доказателство. Да означим с H двоичния $(7,16,3)$ код на Хеминг. Да допуснем, че съществува $(8,21,3)$ код C. Тъй като $c_{00} + c_{01} + c_{10} + c_{11} = 21$ без ограничение $c_{00} \geq 6$. Това означава, че C_{00} е еквивалентен на някои от кодовете $D_1, D_2, \ldots, D_6$. Лесно се проверява, че всеки от тези кодове съдържа подмножество с $c_{00} - 1$ елемента, което е подмножество на кода на Хеминг. Да отбележим, че всяко множество, в което разстоянията между различните му елементи са 3, 4 или 7 е подмножество на H_0

Тогава в C_{01} има $8 - c_{00} + 1$ сфери (с центрове, допълващи множеството от $c_{00} - 1$ елемента до H_0) и още 8 вектора. Тогава най-много $9 - c_{00} + 1$ не са от H_0 и значи $c_0 + c_{00} - 10$ са от H. Тогава в C_1 има най-много

$$16 - (c_0 + c_{00} - 10) = 26 - c_0 - c_{00}$$

вектора. Следователно $c_0 + c_1 \leq 26 - c_{00}$ и понеже $c_{00} \geq 6$, то $|C| \leq 20$. □

Доказахме, че оптимален двоичен код с дължина 8 и минимално разстояние 3 има 20 кодови думи. Ще докажем, че съществуват пет нееквивалентни $(8, 20, 3)$ двоични кодове. За целта първо ще намерим всички нееквивалентни $(6, 5, 3)$ кода.

Лема 2.2.5. Съществуват четири нееквивалентни $(6, 5, 3)$ кода:

$$G_1 = \{0, 7, 25, 42, 63\},\ G_2 = \{0, 7, 25, 43, 62\},$$

$$G_3 = \{0, 15, 21, 51, 60\},\ G_4 = \{0, 15, 22, 37, 42\};$$

Доказателството на Лема 2.2.5 е аналогично на доказателството на Лема 2.2.3.

Нека $\mathcal{C}$ е $(8, 20, 3)$ двоичен код. Без ограничение можем да считаме, че $c_0 \geq c_1$.

Да допуснем, че съществува подмножество на C_0 с мощност $c_0 - 3$, което е еквивалентно на подмножество на кода на Хеминг. Тъй като кодът на Хеминг е съвършен, съществуват $16 - (c_0 - 3)$ вектора, които покриват $F_2^7 \setminus \cup_{\mathbf{x} \in C_0} \mathcal{B}(x, 1)$. От Лема 2.2.2 получаваме, че $\mathcal{C}$ има най-много

$$c_0 + 16 - (c_0 - 3) = 19$$

кодови думи, което е противоречие. □

Лема 2.2.6. Неравенството $c_{ij}^{pq} \leq 6$ е изпълнено за всички $i, j \in F_2$ и $p, q \in \{1, 2, \ldots, 8\}$.

Доказателство. Без ограничение можем да допуснем, че $i = j = 0$, $p = 1, q = 2$ и $c_{00} > 6$. Тъй като всеки $(6, M, 3)$ код има мощност помалка от 9, получаваме, че C_{00} е еквивалентно на D_1 или D_2. Елементите на C_{01} са измежду $F_2^6 \setminus \cup_{\mathbf{x} \in C_{00}} \{\mathcal{B}(\mathbf{x}, 1)\}$. В случая $C_{00} \equiv D_2$ това множество е $\mathcal{B}(38, 1) \cup \{3, 12, 22, 25, 37, 42, 48, 63\}$ (и следователно поне $c_{10} - 1$ вектора в C_{10} са от $\{3, 12, 22, 25, 37, 42, 48, 63\}$), а в случая $C_{00} \equiv D_1$ то е

$\{3, 12, 22, 25, 37, 42, 48, 63\}$ (и следователно всички вектори в C_{10} са от $\{3, 12, 22, 25, 37, 42, 48, 63\}$). И в двата случая лесно се намира подмножество на C_0 с мощност $c_0 - 1$, което е подмножество на кода на Хеминг, което е противоречие. Следователно $c_{ij}^{pq} \leq 6$. □

Теорема 2.2.1. Съществуват 5 нееквивалентни $(8, 20, 3)$ двоични кода.

Доказателство. Нека C е $(8, 20, 3)$ двоичен код. Без ограничение на общността можем да предполагаме, че $c_0 \geq c_1$ и $c_{00} \geq c_{01}$. Следователно $c_{00} \geq 5$, което означава, че множеството C_{00} е еквивалентно на един от кодовете от Лема 2.2.3. Чрез търсене с помощта на компютър намираме всички множества C_{01}, за които няма подмножество на C_0 с мощност $c_0 - 3$, което е еквивалентно на подмножество на кода на Хеминг. Намираме 30 множества с мощност 10, 4 множества с мощност 11 и 2 множества с мощност 12:

Множества с мощност 12

0 124 7 123 25 30 42 53 77 82 97 102 0 124 13 50 23 46 57 70 81 90 101 107

Множества с мощност 11

0 124 7 123 25 30 42 53 77 82 97 0 124 7 123 25 30 42 53 77 82 102
0 124 13 50 23 46 57 70 90 101 107 0 124 13 50 23 46 70 81 90 101 107

Множества с мощност 10

0 124 7 57 26 46 73 86 101 115	0 124 7 57 26 46 73 95 98 101
0 124 7 57 26 46 75 85 97 114	0 124 7 57 26 46 77 81 86 107
0 124 7 57 26 46 77 81 98 119	0 124 7 123 25 30 42 53 77 82
0 124 7 123 25 42 53 77 82 97	0 124 7 123 25 42 53 77 82 102
0 124 7 123 25 42 53 77 86 97	0 124 7 123 25 42 53 78 82 97
0 124 7 123 25 45 54 78 85 97	0 124 7 123 25 45 54 78 85 98
0 124 13 50 23 43 70 81 90 101	0 124 13 50 23 43 78 91 103 113
0 124 13 50 23 46 57 70 91 97	0 124 13 50 23 46 57 90 101 107
0 124 13 50 23 46 70 89 101 107	0 124 13 50 23 46 70 90 101 107
0 124 13 50 23 46 74 81 101 123	0 124 13 50 23 46 81 90 101 107
0 124 13 50 23 46 81 90 103 105	0 124 13 50 23 70 81 90 101 107
0 124 13 50 30 53 70 83 97 111	0 124 13 50 30 53 70 89 97 106
0 124 13 50 63 70 81 90 101 107	0 124 13 51 22 42 67 78 89 101
0 124 13 51 22 46 85 90 103 105	0 124 13 54 19 43 74 95 103 113
0 126 7 56 27 45 73 84 98 113	0 126 14 51 29 52 71 88 98 105

Отново с търсене с компютър намираме останалите $20 - c_0$ вектора от C_1, за да образуваме $(8, 20, 3)$ код. След проверка за еквивалентност на така получените кодове, намираме 5 нееквивалентни кода:

$$\Psi_1 = \{0, 124, 7, 57, 26, 46, 73, 95, 98, 101, 139, 140, 149, 161, 182, 198, 208, 232, 239, 243\}$$

$$\Psi_2 = \{0, 124, 7, 57, 26, 46, 73, 95, 98, 101, 141, 150, 163, 168, 181, 196, 202, 211, 239, 240\}$$

$$\Psi_3 = \{0, 124, 7, 57, 26, 46, 75, 85, 97, 114, 141, 147, 162, 180, 191, 196, 217, 222, 231, 232\}$$

$$\Psi_4 = \{0, 124, 7, 123, 25, 30, 42, 53, 77, 82, 97, 139, 148, 166, 173, 179, 184, 200, 209, 223\}$$

$$\Psi_5 = \{0, 124, 7, 123, 25, 30, 42, 53, 77, 82, 97, 139, 148, 173, 179, 184, 200, 209, 223, 230\}$$

□

За определянето на $B(9, 4)$ разширяваме всеки от горните кодове чрез проверка по четност, след което проверяваме така получените кодове за еквивалентност. Оказва се, че от получените 5 кода само три са нееквивалентни. Следователно $B(9, 4) = 3$.

През 1980 г. Best [3] конструира $(10, 40, 4)$ двоичен код, като в [55] е доказано, че този код е единствен. Този код се получава от четирите вектора 1010000001, 1100101100, 0001010111, 0111111010 и техните циклични премествания.

След скъсяване на кода на Best се получава $(9, 40, 3)$ код. От друга страна, от Лема 2.1.2 следва, че

$$A(9, 3) \leq 2A(8, 3) = 40.$$

Следователно $A(9, 3) = 40$. Тъй като кодът на Best е цикличен и единствен [55], то $B(9, 3) = 1$.

2.3 Определяне на $A(n, 3)$, $B(n, 3)$ и $B(n+1, 4)$ за $10 \leq n \leq 11$

В [35] е представено комбинаторно доказателство на неравенството $A_2(10, 3) \leq 74$. Тъй като по-късно в [61] е намерена точната стойност на $A_2(10, 3)$, ще представим само схематично доказателство на неравенството $A_2(10, 3) \leq 74$.

Следната лема представя някои свойства на $(9, M, 3)$ двоични кодове за $38 \leq M \leq 40$.

Лема 2.3.1. а) Съществува единствен $(9, 40, 3)$ двоичен код.

б) Ако C е $(9, 39, 3)$ двоичен код, то C е подмножество на скъсения $(9, 40, 3)$ код на Best.

в) Ако C е $(9, 38, 3)$ двоичен код, то съществуват кодови думи $\mathbf{x}$ и $\mathbf{y}$ за които $C\backslash\{\mathbf{x}, \mathbf{y}\}$ е подмножество на скъсения $(9, 40, 3)$ код на Best.

Лема 2.3.2. Ако C е двоичен $(n, M, 3)$ код и радиусът на покритие на C_0 е $R > 2$, то съществува двоичен $(n, M, 3)$ код ζ, за който $|\zeta_0| = c_0 + 1$.

Лема 2.3.3. Ако C е $(10, M, 3)$ код, за който $c_0 = 38$, то съществува $(10, M-2, 3)$ код ζ, за който $|\zeta_0| = 40$.

Лема 2.3.4. Не съществува двоичен $(10, 73, 3,)$ код C, за който $c_0 = 40$.

Теорема 2.3.1. В сила е неравенството $A_2(10, 3) \leq 74$.

Доказателство. Ако C е $(10, 75, 3)$ код, то без ограничение можем да считаме, че $c_0 \geq 38$. От Лема 2.3.3 съществува $(10, 73, 3)$ код ζ, за който $|\zeta_0| = 40$. Съществуването на такъв код е противоречие с Лема 2.3.4. Следователно $A_2(10, 3) \leq 74$. □

Ще представим резултатите, получени в [61]. Ще определим точните стойности на $A(n, 3)$, $A(n, 4)$, $B(n, 3)$ и $B(n, 4)$ за $10 \leq n \leq 11$.

Основната идея при конструирането на един $(n, M, 3)$ код C е следната. Да допуснем, че сме намерили всички $(n-1, N, 3)$ кодове, за които $N \leq A(n-1, 3)$. Знаем, че C_0 и C_1 са съответно $(n-1, c_0, 3)$ и $(n-1, c_1, 3)$ кодове, където $c_0 + c_1 = M$. Без ограничение можем да приемем, че $c_0 \geq c_1$. Това означава, че за намирането на кода C е достатъчно да разгледаме всички $(n-1, N, 3)$ кодове, за които $N \geq \lceil \frac{M}{2} \rceil$ и да ги допълним до $(n, M, 3)$ код чрез добавяне на кодови думи от вида $\mathbf{1x}$.

Следната теорема намалява значително пресмятанията при получаване на резултата. Тя показва, че при разглеждане на всички възможни кодове C_0 е достатъчно да се ограничим с онези, които не могат да бъдат разширявани с добавяне на нова кодова дума.

Теорема 2.3.2. Нека C е $(n, M, 3)$ двоичен код. Ако $(n-1, c_0, 3)$ кодът C_0 може да бъде разширен до $(n-1, c_0 + b, 3)$ код, то съществува $(n, M, 3)$ код C', за който $c'_0 = c_0 + b$.

Доказателство. Ще покажем, че прибавянето на опашка $\mathbf{x}$ към C_0 води до изтриване на най-много една опашка от C_1. Да допуснем, че съществуват два

вектора $\mathbf{y}$ и $\mathbf{z}$ от C_1, за които $d(\mathbf{0x}, \mathbf{1y}) \leq 2$ и $d(\mathbf{0x}, \mathbf{1z}) \leq 2$. Тогава $d(\mathbf{x}, \mathbf{y}) \leq 1$ и $d(\mathbf{x}, \mathbf{z}) \leq 1$ и от неравенството на триъгълника имаме $d(\mathbf{y}, \mathbf{z}) \leq 2$, което е противоречие с минималното разстояние на кода. Прилагайки горната процедура b пъти, получаваме твърдението на теоремата. □

Ще опишем индуктивен алгоритъм за намиране (или доказване на несъществуване) на всички $(n, M, 3)$ кодове. Да означим търсеният код с C. За всяко N, за което $N \geq \lceil \frac{M}{2} \rceil$ определяме с точност до еквивалентност всички $(n-1, N, 3)$ кодове, за които не е изпълнено условието от Теорема 2.3.2, т.е. те не могат да бъдат разширени до $(n-1, N+1, 3)$ код. Нека C_0 е един такъв код. За C_0 първо определяме възможните кодови думи в кода C_1.

Тъй като минималното разстояние на търсения код C е 3, то за разстоянието между всяка кодова дума $\mathbf{x}$ от C_1 и всяка кодова дума $\mathbf{y}$ от C_0 трябва да е изпълнено $d(\mathbf{x}, \mathbf{y}) \geq 2$. Следователно възможните кодови думи на C_1 са всички вектори с дължина $n-1$, които са на разстояние поне 2 от кода C_0. От така получените вектори трябва да конструираме код C_1 с минимално разстояние 3 и $M - N$ кодови думи. Подреждаме лексикографски така намерените вектори, след което избираме последователно възможните кодовите думи. На всяка стъпка изтриваме онези от възможните вектори, които са на разстояние по-малко от 3 от някой от вече избраните вектори. Когато намерим необходимия брой вектори, търсеният код е конструиран и трябва да бъде проверен за еквивалентност с вече намерените. Получените резултати са представени в Таблица 1. Остава отворен въпроса за комбинаторно доказателство на равенството $A(10, 3) = 72$, както и за изучаване на свойствата на намерените 562 нееквивалентни кода.

n	M	$\#(n, M, 3)$	$\#(n+1, M, 4)$
4	2	2	2
5	3	1	
5	4	1	1
6	5	4	
6	6	4	
6	7	1	
6	8	1	1
7	9	191	
7	10	90	
7	11	27	
7	12	16	
7	13	4	
7	14	3	
7	15	1	
7	16	1	1
8	18	17547	
8	19	216	
8	20	5	3
9	36	19502	
9	37	732	
9	38	58	
9	39	3	
9	40	1	1
10	72	562	96
10	73	0	
11	144	7398	1041

Таблица 1.

Глава 3

Оптимални покриващи кодове

В тази глава са представени резултатите, получени в [36], [37], [38], [48], [49], [51] и [52].

В [36] и [38] са доказани съответно границите $K_2(9,1) \geq 56$ и $K_2(9,1) \geq 57$ за минималната мощност на двоичен код с дължина 9 и радиус на покритие 1. В [37] и [49] са намерени долни граници и някои точни стойности за $K_{3,2}(t,b)$ – минималната мощност на смесен код с t троични и b двоични координати и радиус на покритие 1. В частност е намерена точната стойност $K_{3,2}(4,2) = 36$.

3.1 Основни дефиниции и предварителни резултати

Нека C е q-ичен код с дължина n и мощност M. Да припомним, че радиус на покритие на кода C се нарича най-малкото естествено число R, за което кълбетата, с центрове кодовите думи и радиус R покриват цялото пространство F_q^n. Основна задача е при зададени n, q и R да се намери минималното M, за което съществува q-ичен код C с дължина n, мощност M и радиус на

покритие R. С $K_q(n, R)$ означаваме тази минимална стойност. За опростяване на означенията нека $K(n) = K_2(n, 1)$. Ще казваме, че код C е $(n, M)R$ код, ако C има дължина n, мощност M и радиус на покритие R.

Една тривиална долна граница за $K(n)$ се дава от следната Лема.

Лема 3.1.1. Изпълнено е равенството

$$K(n) \geq \frac{2^n}{n+1}.$$

Доказателство. Нека C е $(n, M)1$ код. Тъй като всяка кодова дума покрива точно $n + 1$ вектора (самият вектор и всички вектори на разстояние 1 от него), то $M(n + 1) \geq 2^n$. Следователно

$$K(n) \geq M \geq \frac{2^n}{n+1}.$$

□

Оказва се, че когато n е четно число, границата от Лема 3.1.1 може да бъде подобрена [76].

Лема 3.1.2. За четно число n е изпълнено неравенството $K(n) \geq \frac{2^n}{n}$.

Доказателство. Да разгледаме оптимален код C с дължина n, $M = K(n)$ кодови думи и радиус на покритие 1. Да означим с B множеството от всички вектори, които са покрити повече от един път. Ясно е, че

$$M(n + 1) \geq 2^n + |B|.$$

Ще покажем, че векторите от B покриват всички вектори, които не са кодови думи. За целта е достатъчно да докажем, че за произволен вектор $\mathbf{x} \notin C$ съществува $\mathbf{y} \in B$, за който $d(\mathbf{x}, \mathbf{y}) \leq 1$.

Без ограничение можем да считаме, че $\mathbf{x}$ е нулевият вектор и че съществува кодова дума с тегло 1. Ако съществува втора кодова дума с тегло 1, то

$\mathbf{x} \in B$ и $\mathbf{y} = \mathbf{x}$ е търсеният вектор. Ако такава кодова дума не съществува, то всички вектори с тегло 1 се покриват от кодови думи с тегло 2. Но всяка кодова дума с тегло 2 покрива точно два вектора с тегло 1, а не покритите вектори с тегло 1 са $n-1$, т.е. нечетно число. Следователно поне един вектор $\mathbf{y}$ с тегло 1 е покрит два пъти. Това е търсеният вектор.

Всеки вектор от B е покрит от поне две кодови думи и следователно самият той покрива най-много $n-1$ вектора, които не са кодови думи. От доказаното по-горе сега следва, че $|B|(n-1) \geq 2^n - M$, т.е.

$$|B| \geq \frac{2^n - M}{n-1}.$$

Следователно

$$M(n+1) \geq 2^n + |B| \geq 2^n + \frac{2^n - M}{n-1},$$

което е еквивалентно на $M \geq \frac{2^n}{n}$. □

Разглеждането на задачи за смесени кодове е естествено обобщение на съответните задачи за кодове над дадено поле. С особен интерес се отличават смесените кодове, в които имаме двоични и троични координати. Това е така поради пряката връзка на задачата за радиус на покритие на смесени кодове с играта ТОТО 1.

Класическата игра ТОТО 1 се описва по следния начин. Всеки участник дава предположение как ще завърши всяка една от дадени 13 срещи. Възможните предположения са: реми, победа за отбор А, или победа за отбор Б. При познаване на определен брой срещи участникът получава парична награда.

Да допуснем, че участник в ТОТО 1 иска да си осигури 12 познати резултата, без да има никакво предположение как ще завършат срещите. За целта може да се използва съвършения троичен $[13, 10, 3]$ код на Хеминг, който има 3^{10} кодови думи и радиус на покритие $R = 1$. На всяка кодова дума съответства колонка с 13 предположения, като 0 означава реми, 1 оз-

начава победа за единия отбор и 2 означава победа за другия отбор. Тъй като радиусът на покритие е 1, то при всеки възможен резултат от всички 13 срещи ще съществува колонка в която имаме поне 12 познати резултата.

Сега да предположим, че знаем със сигурност как ще завършат част от срещите, за други b срещи знаем, че даден резултат е невъзможен и за някои t срещи не можем да предвидим нищо. Искаме да попълним минимален възможен брой предположения така, че да си гарантираме познаването на 12 срещи.

Дефиниция 3.1.1. Нека $\mathcal{F}_{t,b} = \big\{(x_1, \ldots, x_t, x_{t+1}, \ldots, x_{t+b}) \mid x_i \in \mathbf{F}_3, i = 1, \ldots, t,\ x_j \in \mathbf{F}_2,\ j = t+1, \ldots, t+b\big\}$, където t, b са естествени числа. Множеството $\mathcal{F}_{t,b}$ е абелева група по отношение на координатно събиране. Ще наричаме елементите на това множество думи.

Аналогично на разстояние между вектори над дадено поле, може да се дефинира и разстояние между смесени вектори.

Дефиниция 3.1.2. Разстояние на Хеминг между две думи $\mathbf{x} = (x_1, x_2, \ldots, x_{t+b})$ и $\mathbf{y} = (y_1, y_2, \ldots, y_{t+b})$ от $\mathcal{F}_{t,b}$ се дефинира като броят на координатните позиции, в които двете думи се различават.

$$d(\mathbf{x}, \mathbf{y}) = \big|\big\{i \mid x_i \neq y_i, i \in \{1, 2, \ldots, t+b\}\big\}\big|.$$

Дефиниция 3.1.3. Под кълбо $\mathcal{B}_R(\mathbf{x})$ с център $\mathbf{x} \in \mathcal{F}_{t,b}$ и радиус R разбираме множеството

$$\mathcal{B}_R(\mathbf{x}) = \big\{\mathbf{y} \mid \mathbf{y} \in \mathcal{F}_{t,b}; d(\mathbf{x}, \mathbf{y}) \leq R\big\}.$$

Всяко непразно множество $\mathcal{C}$ на $\mathcal{F}_{t,b}$ се нарича *смесен код*, а елементите му се наричат кодови думи. Числото $n = t + b$ се нарича *дължина* на кода.

Нека $\mathcal{C}$ е код над $\mathcal{F}_{t,b}$. Както и в случая на кодове над поле се дефинира радиус на покритие на смесен код.

Дефиниция 3.1.4. *Радиус на покритие* $R(\mathcal{C})$ на код $\mathcal{C}$ се дефинира като най-малкото естествено число R, за което кълбетата, с центрове в кодовите думи и радиус R покриват цялото множество $\mathcal{F}_{t,b}$. С други думи за всяко $\mathbf{x} \in \mathcal{F}_{t,b}$ съществува кодова дума $\mathbf{c}$ от $\mathcal{C}$, за която $d(\mathbf{x}, \mathbf{c}) \leq R$.

Ако разгледаме смесен двоичен-троичен код с b двоични и t троични координати, разгледаната по-горе задача се формулира като:

Да се определи минималната мощност на смесен двоичен-троичен код с дължина $n = b + t \leq 13$ и даден радиус на покритие $R \leq 3$.

С $K(t, b, R)$ означаваме минималната мощност на код над $\mathcal{F}_{t,b}$ с радиус на покритие R.

Задачата за намиране на $K(t, b, R)$ за различни стойности на t, b и R е разглеждана в [19], [24], [31], [54], [59], [69], [78], [79]. Точните стойности за тези числа са известни само за малък брой стойности на n. В тази глава ще представим комбинаторен подход за намиране на долни граници за $K(t, b, R)$. В част от случаите тези долни граници се оказват достатъчни за намиране на съответните точни стойности.

Лема 3.1.3. В сила е следното неравенство:

$$K_{3,2}(t, b) \geq \frac{2^b 3^t}{b + 2t + 1}.$$

Доказателство. Нека C е смесен код с b двоични и t троични координати и радиус на покритие 1. Тъй като всяка кодова дума покрива точно $b+2t+1$ вектора, а всички кодови думи са $2^b 3^t$, то

$$|C|(b + 2t + 1) \geq 2^b 3^t,$$

откъдето следва исканото неравенство. □

3.2 Долна граница за $K_2(9,1)$

Долни граници за $K(n,R) = K_2(n,R)$ са получавани в [10], [11], [12], [22], [23], [65], [66], [67], [76]. Определянето на $K(9,1)$ има дълга история. Границата на сферичната опаковка дава $K(9,1) \geq 52$. В [36] е доказана границата $K(9,1) \geq 56$. Ще представим получената в [38] граница $K(9,1) \geq 57$. Точната стойност $K(9,1) = 62$ е намерена в [70] с търсене с компютър.

Да разгледаме равнината $P^{p_1p_2\dots p_s}_{i_1i_2\dots i_s}$ от степен s. Кодова дума от тази равнина покрива $n-s+1$ вектора в нея и по един вектор във всяка от равнините $P^{p_1p_2\dots p_s}_{j_1j_2\dots j_s}$, където $d(i_1i_2\dots i_s, j_1j_2\dots j_s) = 1$. Тъй като във всяка равнина имаме 2^{n-s} вектора, получаваме:

$$(n-s+1)c^{p_1p_2\dots p_s}_{i_1i_2\dots i_s} + \sum_{d(i_1\dots i_s, j_1\dots j_s)=1} c^{p_1\dots j_s}_{j_1\dots j_s} \geq 2^{n-s}$$

При $n = 9$ и $s = 3$ горното неравенство става

$$7c_{ijk} + \sum_{d(ijk,pqr)=1} c_{pqr} \geq 64 \tag{3.1}$$

Ясно е, че някои от сферите с центрове опашки от P_{ijk} (това е точно множеството C_{ijk}) могат да се пресичат. За произволно множество X от вектори с дължина 6 с L_X означаваме броя на покритите вектори от елементите на X. Имаме $L_{C_{ijk}} \leq 7c_{ijk}$ и

$$L_{C_{ijk}} + \sum_{d(ijk,pqr)} c_{pqr} \geq 64$$

От това неравенство е ясно, че ако знаем точната стойност на $L_{C_{ijk}}$, получаваме долна граница за броят на опашките в трите съседни на F_{ijk} равнини. Следователно е важно да знаем какви стойности може да приема $L_{C_{ijk}}$ в зависимост от броят на опашките в F_{ijk}. Ще опишем възможните множества A, съставени от 6 вектора, за които $39 \leq L_A \leq 42$.

Лема 3.2.1. Нека $A = \{v_1, v_2, \ldots, v_6\}$ е множество от двоични вектори с дължина 6. Нека L_A е броят на векторите покрити от $v_1, v_2, \ldots, v_6$. Тогава $L_A \leq 42$ и с точност до еквивалентност:

а) съществуват 4 множества A, за които $L_A = 42$;

б) не съществува множество A, за което $L_A = 41$;

в) съществуват 16 множества A, за които $L_A = 40$;

г) не съществува множество A, за които $L_A = 39$.

Доказателство. а) Тъй като $L_A = 42$, то сферите с центрове елементите на A с радиус 1 не се пресичат. Това означава, че $d(v_i, v_j) \geq 3$ за $1 \leq i < j \leq 6$. Ще докажем, че съществуват 4 такива множества:

$$C_1 = \{000000, 000111, 011001, 101010, 110100, 111111\};$$

$$C_2 = \{000000, 000111, 011001, 101011, 110101, 111110\};$$

$$C_3 = \{000000, 001111, 010101, 101001, 110011, 111100\};$$

$$C_4 = \{000000, 001111, 010110, 100101, 101010, 111100\}.$$

Нека

$$d = \max\{d(v_i, v_j) : 1 \leq i < j \leq 6\}.$$

Ясно е, че $d \geq 3$, като ако $d(v_1, v_i) = d(v_1, v_j) = 3$, то $d(v_i, v_j)$ е четно число и следователно $d \geq 4$. Трябва да разгледаме три случая: (i) $d = 6$; (ii) $d = 5$ и (iii) $d = 4$. Освен това множества, получени при различни стойности на d не могат да бъдат еквивалентни.

Без ограничение можем да считаме, че $v_1 = 000000$.

(i) Нека $d = 6$. Без ограничение приемаме, че $v_6 = 111111$. Тъй като $3 \leq d(v_1, v_i) = wt(v_i)$ и $3 \leq d(v_6, v_i) = 6 - wt(v_i)$ за $2 \leq i \leq 5$, следва, че $wt(v_i) = 3$ за $2 \leq i \leq 5$. Следователно $v_2 = 000111$. Да допуснем, че $111000 \in \{v_3, v_4, v_5\}$ (например $v_3 = 111000$). Директно се вижда, че (да

отбележим, че $wt(v_4) = 3$) или $d(v_2, v_4) < 3$ или $d(v_3, v_4) < 3$. Следователно $111000 \notin \{v_3, v_4, v_5\}$. Лесно се проверява, че с точност до еквивалентност $v_3 = 011001, v_4 = 101010$ и $v_5 = 110100$. В този случай $A = C_1$.

(ii) Нека $d = 5$. Без ограничение $v_6 = 111110$. Ако последната координата на някои от векторите $v_i, 2 \leq i \leq 5$ е 0, то или $d(v_1, v_i) < 3$ или $d(v_6, v_i) < 3$. Следователно последната координата на всеки от векторите $v_i, 2 \leq i \leq 5$ е 1. Очевидно е, че $3 \leq d(v_1, v_i) = wt(v_i)$ и $3 \leq d(v_6, v_i) = 7 - wt(v_i)$, откъдето $wt(v_i)$ за $2 \leq i \leq 5$ е 3 или 4. Тъй като прибавянето на вектора 111110 към $v_i, 1 \leq i \leq 6$ разменя местата на v_1 и v_6 и променя теглата на v_i, $2 \leq i \leq 5$ от 3 на 4 и обратно, можем да приеме, че $wt(v_2) = wt(v_3) = 3$ и $v_2 = 000111$. С точност до еквивалентност има две възможности за v_3 - 001011 и 011001. Първата дава $d(v_2, v_3) = 2$, противоречие, откъдето следва $v_3 = 011001$. Сега лесно се вижда, че с точност до еквивалентсост $v_4 = 101011$ и $v_5 = 110101$. В този случай $A = C_2$.

(iii) Нека $d = 4$. В този случай $d(v_i, v_j)$ е 3 или 4 за $1 \leq i < j \leq 6$. Следователно $wt(v_i) = 3$ или 4 за $2 \leq i \leq 6$ (да отбележим, че $wt(v_i) = d(v_1, v_i)$). Съществуват поне три равни тегла измежду $wt(v_i), 2 \leq i \leq 6$. Без ограничение $wt(v_2) = wt(v_3) = wt(v_4) = x$. Тъй като

$$d(v_i, v_j) = wt(v_i) + wt(v_j) - 2wt(v_i \star v_j), 2 \leq i < j \leq 4$$

е четно число, получаваме, че $d(v_2, v_3) = d(v_2, v_4) = d(v_3, v_4) = 4$.

Доказахме, че ако $d = 4$ съществуват три вектора (без ограничение v_1, v_2, v_3) за които $d(v_1, v_2) = d(v_1, v_3) = d(v_2, v_3) = 4$. Лесно се вижда, че с точност до еквивалентност $v_1 = 000000, v_2 = 111100$ и $v_3 = 001111$. Да допуснем, че един от векторите $v_i, 4 \leq i \leq 6$ (например v_4) има тегло 4. Директно се проверява, че без ограничение $v_4 = 110011$, $v_5 = 010101$ и $v_6 = 101001$. В този случай $A = C_3$.

Ако $wt(v_4) = wt(v_5) = wt(v_6) = 3$, както по-горе се доказва, че без ограничение $v_4 = 101010, v_5 = 100101$ и $v_6 = 010110$. В този случай $A = C_4$.

Множествата C_3 и C_4 не са еквивалентни, понеже в C_3 съществува 4 елементно подмножество

$$\{000000, 111100, 001111, 110011\},$$

с разстояние между всеки два елемента равно на 4, докато в C_4 такова множество не съществува.

За удобство ще записваме двоичните вектори $v_1, v_2, v_3, v_4, v_5, v_6$ като съответните естествени числа. Тогава:

$$C_1 = \{0, 7, 25, 42, 52, 63\}; C_2 = \{0, 7, 25, 43, 53, 62\};$$

$$C_3 = \{0, 15, 21, 41, 51, 60\}; C_4 = \{0, 15, 22, 37, 42, 60\}.$$

б) Ако $L_A < 42$, то съществуват две сфери с центрове в елементи на A, които имат общ елемент. Ако това са елементите $\mathbf{x}$ и $\mathbf{y}$, имаме $d(\mathbf{x}, \mathbf{y}) \leq 2$. Тогава двете сфери имат точно два общи елемента, което означава, че $L_A \leq 40$. Следователно не съществува множество с $L_A = 41$.

в) Когато $L_A = 40$ имаме само две кодови думи на разстояние 1 или 2. Директно се проверява, че сферите, с центрове в тези кодови думи имат точно два общи елемента.

Следователно в множеството A съществуват 5 елемента, разстоянията между всеки два от които са поне 3. Това означава, че A съдържа като подмножество някои от четирите кода от Лема 2.2.5

За всеки от тези кодове с директна проверка намираме вектор, който е на разстояние 1 или 2 от една от кодовите думи и на разстояние поне 3 от всяка от останалите. От така получените кодове по стандартен начин определяме нееквивалентните. Получените 16 множества са представени в долната таблица.

$B_1 = \{0, 1, 14, 23, 43, 50\}$	$B_2 = \{0, 1, 14, 23, 43, 52\}$	$B_3 = \{0, 1, 14, 23, 43, 60\}$
$B_4 = \{0, 1, 14, 23, 43, 61\}$	$B_5 = \{0, 1, 14, 27, 54, 61\}$	$B_6 = \{0, 3, 13, 22, 42, 49\}$
$B_7 = \{0, 3, 13, 22, 42, 53\}$	$B_8 = \{0, 3, 13, 22, 42, 60\}$	$B_9 = \{0, 3, 13, 22, 46, 53\}$
$B_{10} = \{0, 3, 13, 22, 46, 56\}$	$B_{11} = \{0, 3, 13, 22, 46, 57\}$	$B_{12} = \{0, 3, 13, 26, 52, 63\}$
$B_{13} = \{0, 3, 13, 30, 50, 57\}$	$B_{14} = \{0, 3, 13, 30, 52, 57\}$	$B_{15} = \{0, 3, 13, 30, 52, 59\}$
$B_{16} = \{0, 3, 28, 45, 54, 59\}$		

г) Ако $L_A = 39$, то в A трябва да има поне две двойки пресичащи се сфери. Понеже във всяка от тези двойки има по два вектора, всеки от които е покрит по два пъти, то $L_A \leq 38$, противоречие. □

Да допуснем, че съществува $(9, 56)1$ двоичен код C. Без ограничение $c_{000} = \min\{c_{ijk}\}$. Сега 3.1 дава

$$\begin{aligned} 7c_{000} + c_{001} + c_{010} + c_{100} &\geq 64 \\ c_{110} + c_{101} + c_{011} &\geq 3c_{000} \\ 7c_{110} + c_{100} + c_{010} + c_{111} &\geq 64 \\ 7c_{101} + c_{100} + c_{001} + c_{111} &\geq 64 \\ 7c_{011} + c_{001} + c_{010} + c_{111} &\geq 64 \\ 7c_{111} + c_{110} + c_{101} + c_{011} &\geq 64 \end{aligned}$$

Умножаваме първото неравенство с 8, второто с 2 и събираме с останалите 4 и получаваме

$$46c_{000} + 10|C| \geq 6c_{000} + 12.64.$$

Оттук $5c_{000} \geq 26$ и следователно $c_{000} \geq 6$.

Лема 3.2.2. Ако $c_{ijk} = 6$ то $\sum_{d(ijk,pqr)=1} c_{pqr} \leq 25$.

Доказателство. Без ограничение $c_{000} = 6$ и да допуснем, че

$$c_{100} + c_{010} + c_{001} \geq 26.$$

Тъй като $|C| = 56$ получаваме $c_{111} + c_{110} + c_{101} + c_{011} \leq 24$. Като използваме, че $c_{ijk} \geq 6$ намираме $c_{111} = c_{110} = c_{101} = c_{011} = 6$. Сега неравенство 3.1 не е вярно за $ijk = 111$. Това противоречие показва, че $c_{100} + c_{010} + c_{001} \leq 25$. □

Лема 3.2.3. Ако $c_{ijk} = 6$ и $\sum_{d(ijk,pqr)=1} c_{pqr} = \min_{c_{lmn}=6}\{\sum_{d(lmn,pqr)=1} c_{pqr}\}$, то

$$\sum_{d(ijk,pqr)=1} c_{pqr} \leq 24.$$

Доказателство. От Лема 3.2.2 следва, че е достатъчно да докажем, че

$$\sum_{d(ijk,pqr)=1} c_{pqr} \neq 25.$$

За целта да допуснем, че $\sum_{d(ijk,pqr)=1} c_{pqr} = 25$. Без ограничение $ijk = 000$. Сега $c_{111} + c_{110} + c_{101} + c_{011} = 25$. Ако $c_{111} = 6$, то 3.1 не е вярно за $ijk = 111$ и следователно $c_{111} = 7, c_{110} = c_{101} = c_{011} = 6$. Като използваме, че

$$25 = c_{100} + c_{010} + c_{001} = \min_{c_{ijk}=6}\{\sum_{d(ijk,pqr)=1} c_{pqr}\},$$

намираме

$$c_{100} + c_{010} + c_{111} \geq 25$$
$$c_{100} + c_{001} + c_{111} \geq 25$$
$$c_{010} + c_{001} + c_{111} \geq 25$$

Събираме горните неравенства и получаваме

$$2(c_{100} + c_{010} + c_{001}) + 3c_{111} \geq 75,$$

откъдето $71 \geq 75$, противоречие. Следователно $c_{100} + c_{010} + c_{001} \leq 24$. □

Теорема 3.2.1. Не съществува $(9, 56)1$ двоичен код.

Доказателство. Да допуснем, че съществува $(9, 56)1$ двоичен код C. Тъй като $|C| = 56$ и имаме 8 равнини от степен 3 трябва да разгледаме два случая:

Случай 1: Съществува $\{p, q, r\} \subset \{1, 2, \ldots, 9\}$ и $i, j, k \in \mathbb{F}_2$, за които $c_{ijk}^{pqr} = 6$.

Случай 2: В сила са равенствата $c_{ijk}^{pqr} = 7$ за произволни $\{p, q, r\} \subset \{1, 2, \ldots, 9\}$ и $i, j, k \in \mathbb{F}_2$.

Случай 1: Без ограничение $c_{000} = 6$ и

$$c_{001} + c_{010} + c_{100} = \min_{c_{ijk}=6} \{ \sum_{d(ijk,pqr)=1} c_{pqr} \}.$$

Да отбележим, че винаги когато $c_{ijk} = 6$, имаме $L_{C_{ijk}} \geq 39$. Лема 3.2.1 означава, че множеството C_{ijk} е еквивалентно на едно от $C_i, i = 1, 2, 3, 4$ или $B_i, i = 1, 2 \ldots, 16$. Също така Лема 3.2.1 дава $L_{C_{000}} \geq 40$.

Да допуснем, че $L_{C_{000}} = 40$. Тогава C_{000} е еквивалентно на B_i за някое $i = 1, 2, \ldots, 16$. Разглеждаме множеството Q_{B_i} (виж **Таблица 2**) от вектори с дължина 6, които не са покрити от B_i. Ясно е, че $|Q_{B_i}| = 24$ и всички вектори от това множество са опашки в P_{100}, P_{010} или P_{001}. От Лема 3.2.2 намираме, че $c_{100} + c_{010} + c_{001} = 24$ и следователно всички елементи на Q_{B_i} са опашки в P_{110}, P_{101} и P_{011}. Понеже $c_{111} + c_{110} + c_{101} + c_{011} = 26$ и при $c_{111} = 6$ в P_{111} остават непокрити вектори, имаме $c_{110} + c_{101} + c_{011} \leq 19$ и $c_{111} \leq 8$. Да разгледаме множествата $R_{B_i}^t$ (виж **Таблица 2**) от вектори, които не са в B_i и са покрити по t пъти от векторите в Q_{B_i}. Тъй като всеки вектор с дължина 6 е покрит 3 пъти (по веднъж във всяка равнина P_{100}, P_{010} и P_{001} следва, че всеки вектор от $R_{B_i}^0$ се появява поне два пъти като опашка в P_{110}, P_{101} или P_{011} и всеки вектор от $R_{B_i}^1$ и $R_{B_i}^2$ се появява поне веднъж като опашка в P_{110}, P_{101} и P_{011}. Следователно има поне $2|R_{B_i}^0| + |R_{B_i}^1| + |R_{B_i}^2|$ опашки в P_{110}, P_{101} и P_{011}. За всяко i освен 5,12,15 и 16 горната сума е повече от 19 (за i=2,3,4,7,8,10,11,13,14 сумата е 20; за i=1,6,9 сумата е 24), което е противоречие с $c_{110} + c_{101} + c_{011} \leq 19$. Да разгледаме случая $i = 5$ ($i = 12, 15$ се разглеждат аналогично). Известните опашки в P_{110}, P_{101} и P_{011} са

$$R_{B_5}^1 \cup R_{B_5}^2 = \{2, 3, 4, 6, 8, 9, 10, 11, 13, 17, 18, 25, 30, 31, 62, 63\}.$$

Да забележим, че само два от тези вектори имат 1 в първата си координата. Като преброим покритите вектори с първа координата 1 в тези равнини получаваме противоречие. Случаят $i = 16$ се отхвърля аналогично като заместваме „първа координата 1(0)“ с „вектори с нечетно (четно) тегло“. Да отбележим, че ако $c_{ijk} = 6$, то C_{ijk} е еквивалентно на C_i за някое $i = 1, 2, 3$ или 4. В частност няма разстояния по-малки от 3 в C_{ijk}.

Да допуснем, че $L_{C_{000}} = 42$. Ясно е, че $c_{100} + c_{010} + c_{001} = 22, 23$ или 24.

Нека $c_{100} + c_{010} + c_{001} = 24$. Лесно се вижда, че $c_{110} + c_{101} + c_{011} = 18$ или 19 и следователно поне 2 от $c_{110}, c_{101}, c_{011}$ (например c_{110} и c_{101}) са равни на 6 (да припомним, че в тези две равнини няма опашки на разстояние по-малко от 3). Освен това броят на опашките в съседните равнини на равнините P_{110} и P_{101} е по-голям от 24, т.е. $c_{100} + c_{010} + c_{111} \geq 24$ и $c_{100} + c_{001} + c_{111} \geq 24$. Някои от векторите от $R^1_{B_i}$ (виж **Таблица 1**) (които са покрити два пъти от двете неизвестни опашки) може да не са опашки в P_{110}, P_{101} или P_{011}. Ще разгледаме случая $i = 1$ (останалите случаи се разглеждат аналогично). В този случай

$$R^1_{C_1} = \{1, 2, 4, 8, 11, 16, 21, 31, 32, 38, 47, 55, 56, 59, 61, 62\}.$$

Да забележим, че всички вектори с тегла 1 и 5 са в $R^1_{C_1}$. Тъй като опашка в P_{100}, P_{010} или P_{001} не може да покрива едновременно вектор с тегло 1 и вектор с тегло 5 следва, че без ограничение всички вектори с тегло 1 (има 6 такива вектора) са опашки в P_{110}, P_{101} или P_{011}. Тъй като разстоянието между всеки два такива вектора е по-малко от 3, следва че поне 4 от тях са опашки P_{011}. Следователно $c_{011} \neq 6$, откъдето $c_{011} = 7$. От горните разсъжденrя можем да заключим, че:

$$c_{000} = 6, c_{100} + c_{010} + c_{001} = 24, c_{110} = 6, c_{101} = 6, c_{011} = 7, c_{111} = 7,$$

$$c_{100} + c_{010} + c_{111} \geq 24; c_{100} + c_{001} + c_{111} \geq 24.$$

Събираме последните две неравенства и получаваме $c_{100} \geq 10$, което води до $c_{010} + c_{001} \leq 14$. Да преброим покритите вектори в P_{011}. Директна проверка показва, че четирите известни опашки (тези с тегло 1) покриват 19 различни вектора. Трите неизвестни опашки покриват не повече от 21 вектора и $c_{111} + c_{010} + c_{001} \leq 7 + 14 = 21$. Общият брой покрити вектори е

$$19 + 21 + 21 = 61 < 64,$$

което е противоречие.

Нека $c_{100}+c_{010}+c_{001} = 23$. Тъй като имаме само една неизвестна опашка в P_{100}, P_{010} и P_{001}, получаваме, че всички вектори от $R^1_{C_i}$ са опашки в P_{110}, P_{101} или P_{011}. Преброяването на покритите вектори с последна координата 1(или 0) или броят на покритите вектори с четно (нечетно) тегло в P_{110}, P_{101}, P_{011} и P_{111} води до противоречие.

Нека $c_{100} + c_{010} + c_{001} = 22$. Когато $c_{111} \geq 7$ като преброим покритите вектори с последна координата 1(или 0) или броят на покритите вектори с четно (нечетно) тегло в P_{110}, P_{101}, P_{011} и P_{111}, отново достигаме до противоречие.

Ако $c_{111} = 6$, то $c_{110} + c_{101} + c_{011} = 22$. Ще разгледаме случаят $i = 1$ (случаите $i = 2, 3, 4$ се разглеждат аналогично). Да забележим, че всички вектори в

$$R^1_{C_1} = \{1, 2, 4, 8, 11, 16, 21, 31, 32, 38, 47, 55, 56, 59, 61, 62\}$$

(те са опашки в P_{110}, P_{101} или P_{011}) са с нечетно тегло. Сега неравенство 3.1 става равенство за $ijk = 111$ и следователно никоя опашка от F_{111} не е покрита от вектор от $R^1_{C_1}$ (в противен случай има припокриване в P_{111}). Директна проверка показва, че непокритите вектори от $R^1_{C_1}$ са с нечетно тегло (16 вектора с тегло 3). Следователно всички опашки в P_{111} са с нечетно тегло и има поне $32 - 6 - 22 = 4$ непокрити вектора с нечетно тегло в P_{111}, което е противоречие.

Случай 2: Нека $c^{pqr}_{ijk} = 7$ за всички $\{p, q, r\} \subset \{1, 2, \ldots, 9\}$ и $i, j, k \in \mathbb{F}_2$.

Лема 3.2.4. Ако $d(i_1i_2i_3i_4, j_1j_2j_3j_4) = 2$, то $c^{pqrs}_{i_1i_2i_3i_4} = c^{pqrs}_{j_1j_2j_3j_4}$.

Доказателство. Без ограничение нека $i_1i_2i_3i_4 = 0000, j_1j_2j_3j_4 = 0011$ и $pqrs = 1234$. Понеже $7 = c_{000} = c_{0000} + c_{0001}$, имаме $c_{0000} = 7 - c_{0001}$. Освен това

$$7 = c^{124}_{001} = c^{1234}_{0001} + c^{1234}_{0011}$$

и следователно $c_{0011} = 7 - c_{0001}$, откъдето $c_{0000} = c_{0011}$. □

Тъй като $7 = c_{000} = c_{0000} + c_{0001}$ с точност до еквивалентност

$$(c_{0000}, c_{0001}) = (7, 0), (6, 1), (5, 2), (4, 3).$$

Лесно се вижда, че ако $c_{0001} \leq 1$ неравенството 3.1 не е вярно за $i_1i_2i_3i_4 = 0001$ и $p_1p_2p_3p_4 = 1234$. Следователно $(c_{0000}, c_{0001}) = (5, 2)$ или $(4, 3)$. От Лема 3.2.4 следва, че c_{ijkp} са определени еднозначно. Продължаваме с построяване на петата координата. С подобни на горните аргументи получаваме, че има само две множества за C_{abcde}, които изпълняват $c^{pqr}_{ijk} = 7$ за $\{p, q, r\} \subset \{1, 2, 3, 4, 5\}; i, j, k \in \mathbb{F}_2$ и неравенство 3.1.

а) $c_{00000} = 4; c_{11111} = 2;$
$c_{abcde} = 0$ if $wt(abcde) = 1;$
$c_{abcde} = 3$ if $wt(abcde) = 2;$
$c_{abcde} = 1$ if $wt(abcde) = 3;$
$c_{abcde} = 2$ if $wt(abcde) = 4;$

б) $c_{00000} = 3c_{11111} = 3;$
$c_{abcde} = 1$ ако $wt(abcde) = 1;$
$c_{abcde} = 2$ ако $wt(abcde) = 2;$
$c_{abcde} = 2$ ако $wt(abcde) = 3;$
$c_{abcde} = 1$ ако $wt(abcde) = 4;$

Да разгледаме а) (случай б) се разглежда аналогично). Да забележим, че 3.1 става равенство за $wt(i_1i_2i_3i_4i_5) = 1$. Да допуснем, че съществува вектор с тегло 4, който е опашка в F_{00000} и F_{ijkpq} за някои $ijkpq, wt(ijkpq) = 2$. Тогава 3.1 не може да бъде вярно за поне две $i_1i_2i_3i_4i_5, wt(i_1i_2i_3i_4i_5) = 1$. Следователно опашките в $F_{ijkpq}, wt(ijkpq) = 2$ са измежду $16 - 4 = 12$ вектора. Тъй като съществуват 10.3=30 опашки в тези равнини, то съществува вектор $x_1x_2x_3x_4$, който е опашка в $F_{p_1p_2p_3p_4p_5}, F_{q_1q_2q_3q_4q_5}$ и $F_{r_1r_2r_3r_4r_5}$, където $wt(p_1p_2p_3p_4p_5) = wt(q_1q_2q_3q_4q_5) = wt(r_1r_2r_3r_4r_5) = 2$. Директно се проверява,

че без ограничение $p_1p_2p_3p_4p_5 = 11000$ и $q_1q_2q_3q_4q_5 = 10100$. Сега неравенство 3.1 не е вярно за $i_1i_2i_3i_4i_5 = 10000$ понеже $10000x_1x_2x_3x_4$ е покрит два пъти. С това доказателството е завършено. □

i	Q_{C_i}	$R^0_{C_i}$	$R^1_{C_i}$	$R^2_{C_i}$
1	11,12,13,14,18,19,21,22,26,28,30, 33,35,37,38,41,44,45,49,50,51,56		1,2,4,8,11,16,21,31 32,38,47,55,56,59,61,62	
2	10,12,13,14,18,19,20,22,26,28,31 33,34,36,38,40,44,45,48,50,52,56		1,3,5,9,11,17,21,31, 33,39,47,55,57,59,61,63	
3	3,6,10,12,18,22,24,25,26,27,30, 34,36,37,38,39,42,46,48,54,58,63		1,3,5,9,12,13,17,20,23,29, 33,40,43,45,48,49,53,57,61,63	
4	3,9,12,17,19,21,24,25,26,27,29, 35,38,41,48,49,50,51,55,57,59,63		2,4,5,6,7,10,12,14,20,30, 32,36,38,40,44,45,46,47,52,62	

Таблица 1.

i	Q_{B_i}	$R^0_{B_i}$	$R^1_{B_i}$	$R^2_{B_i}$
1	13,20,24,25,26,27,28,29,36,37,38,39, 40,44,45,49,52,53,56,57,60,61,62,63,	2,3	6,7,10,11,15,18, 19,22,34,35,42,51	4,5,8,9,16, 17,32,33
2	13,18,24,25,26,27,28,29,34,37,38,39, 40,44,45,49,50,51,56,57,58,61,62,63	3,4	6,7,10,11, 15,20,21,22	2,5,8,9,16, 17,22,32,33
3	13,18,20,24,25,26,27,29,34,36,37,38, 39,40,45,48,49,50,51,53,54,57,58,63	3	6,7,10,11,12,15, 20,30,40,46,63	2,4,5,8, 9,17,33
4	13,18,20,24,25,26,27,28,34,36,37,38, 39,40,44,48,49,50,51,52,54,56,58,62	3	6,7,10,11,13,15, 21,31,41,47,63	2,4,5,8, 9,17,33
5	7,13,18,20,21,23,24,28,34,35,36,37, 39,40,41,42,43,44,47,48,49,51,56,58		6,10,11,13,18, 25,30,31,62,63	2,3,4, 8,9,17
6	14,21,24,25,26,27,28,31,36,37,38,39, 41,44,47,50,52,55,56,59,60,61,62,63	1,2	4,7,8,14,16,19, 21,32,35,41,50	5,6,9,10, 17,18,33,34
7	14,17,24,25,26,27,28,31,33,36,38,39, 41,44,47,48,50,51,56,57,59,60,62,63	2	4,7,8,11, 14,20,21,23	1,6,9,10, 17,18,33,34
8	14,17,21,24,25,26,27,31,33,36,37,38, 39,41,47,48,49,50,51,53,55,57,59,63	2	4,7,8,11,12,14, 20,28,40,44,62	1,5,6,9, 10,18,34
9	10,17,24,25,26,27,28,31,33,34,36,39, 40,41,43,48,50,51,56,57,58,59,60,63	5,6	4,7,12,14,15,20, 21,23,36,39,45,54	1,2,9,10,17, 18,33,34
10	10,17,21,25,26,27,28,31,33,34,36,37, 39,41,43,49,50,51,52,53,55,59,61,63	6	4,7,8,12,14,15, 16,28,40,44,62	1,2,5,9, 10,18,34
11	10,17,21,24,26,27,28,31,33,34,36,37, 39,40,43,48,50,51,52,53,55,58,60,63	6,9	4,7,12,14, 15,40,43,45	1,2,5,10, 17,18,33,34
12	6,14,17,21,22,23,25,28,33,34,37,38, 39,40,41,42,43,44,46,49,50,51,56,57		4,8,11,15,16, 27,28,31,61,62	1,2,5, 9,10,18
13	6,10,17,20,21,23,24,27,33,36,37,38, 39,40,42,43,44,46,47,52,53,55,60,63	9,18	12,15,24,27, 29,48,51,58	1,2,5,6, 10,17,33,34
14	6,10,17,18,21,23,24,27,33,34,37,38, 39,40,42,43,44,46,47,50,51,55,58,63	9	4,12,15,20,24,27, 28,29,48,60,61	1,5,6,10, 17,18,33
15	6,10,17,18,21,23,24,25,33,34,37,38, 39,40,41,42,44,46,47,49,50,55,56,61		4,11,12,15,20, 27,28,31,61,62	1,5,6, 9,10,18
16	5,6,9,10,14,15,17,18,21,23,25,26, 31,33,34,36,39,40,42,46,48,49,53,56		12,20,36,39,43, 51,60,61,62,63	5,6,9, 18,33,34

Таблица 2.

3.3 Смесени покриващи кодове с $R = 1$

В тази част ще докажем долни граници за смесени кодове с дължина 6 и радиус на покритие 1. Като следствие на получените резултати ще определим точните стойности на $K(b, t, 1)$ за различни стойности на b и t.

За множеството $\mathcal{A} = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\} \subset \mathcal{F}_{t,b}$ дефинираме

$$\mathcal{C}_R^{(k)}(\mathcal{A}) = \bigcup_{i_1,\ldots,i_k} \bigcap_{j=1}^{k} \mathcal{B}_R(\mathbf{x}_{i_j}), \tag{3.2}$$

$$\mathcal{C}_R(\mathcal{A}) = \bigcup_{k \geq 1} \mathcal{C}_R^{(k)}(\mathcal{A}), \tag{3.3}$$

$$\mathcal{N}_R(\mathcal{A}) = \mathcal{C}_R^{(0)}(\mathcal{A}) = \mathcal{F}_{t,b} \setminus \mathcal{C}_R(\mathcal{A}). \tag{3.4}$$

Когато пропускаме долния индекс R считаме, че той е равен на 1. Нека

$$\varphi : \begin{cases} \mathcal{F}_{t,b} & \to & \mathcal{F}_{t,b} \\ x & \to & x^{\varphi} \end{cases} \tag{3.5}$$

е биекция от $\mathcal{F}_{t,b}$ в $\mathcal{F}_{t,b}$. Казваме, че то е *запазващо разстоянието* ако за всеки два вектора $\mathbf{x}, \mathbf{y} \in \mathcal{F}_{t,b}$ е изпълнено $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x}^{\varphi}, \mathbf{y}^{\varphi})$. Следните изображения са запазващи разстоянията:

(i) $\varphi_\sigma : \mathbf{x} = (x_1, x_2, \ldots, x_n) \to \mathbf{x}^{\varphi_\sigma} = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$, където $\sigma \in S_t \times S_b$ (S_n е симетричната група от ред n);

(ii) $\psi_{\mathbf{a}} : \mathbf{x} \to \mathbf{x}^{\psi_{\mathbf{a}}} = \mathbf{x} + \mathbf{a}$, където $\mathbf{a} \in \mathcal{F}_{t,b}$;

(iii) $\mu_{i,b} : \mathbf{x} = (x_1, x_2, \ldots, x_n) \to \mathbf{x}^{\mu_{i,b}} = (x_1, x_2, \ldots, bx_i, \ldots, x_n)$, където $0 \neq b \in \mathbf{F}_3$ и $i \in \{1, 2, \ldots, t\}$.

Нека $G = < \varphi_\sigma, \psi_a, \mu_{i,b} | \sigma \in S_t \times S_b, \mathbf{a} \in \mathcal{F}_{t,b}, i \in \{1, 2, \ldots, t\}, 0 \neq b \in \mathbf{F}_3 >$. За всеки код $\mathcal{C}$ и $\varphi \in G$ означаваме $\mathcal{C}^{\varphi} = \{\mathbf{x}^{\varphi} | \mathbf{x} \in \mathcal{C}\}$. Два кода $\mathcal{C}_1$ and $\mathcal{C}_2$ са еквивалентни ако съществува изображение $\varphi \in G$, за което $\mathcal{C}_1^{\varphi} = \mathcal{C}_2$. Дефинираме $Aut\,\mathcal{C} = \{\varphi \in G | \mathcal{C}^{\varphi} = \mathcal{C}\}$.

Лема 3.3.1. За всяко множество $\mathcal{A} \subset \mathcal{F}_{t,b}$ и всеки две цели числа $k \geq 0$, $R \geq 1$ е изпълнено $Aut\,\mathcal{A} < Aut\,\mathcal{C}_R^{(k)}\mathcal{A}$ и $Aut\,\mathcal{C}_R(\mathcal{A}) = Aut\,\mathcal{N}_R(\mathcal{A})$.

Дефиниция 3.3.1. Казваме, че непресичащите се множества $\mathcal{S}_j \subset \mathcal{F}_{t,b}$, $j = 1, 2, \ldots, m$ образуват *регулярно разделяне* на $\mathcal{F}_{t,b}$ ако:

(i) $\mathcal{F}_{t,b} = \cup_{j=1}^{m} \mathcal{S}_j$ и

(ii) за всяко $i, j \in \{1, 2, \ldots, m\}$ и всяко цяло число $R \geq 1$ броят на думите от $\mathcal{S}_j$ на разстояние R от всяко $\mathbf{x} \in \mathcal{S}_i$ е един и същ, т.е. не зависи от избора на $\mathbf{x}$. Означаваме тази константа с r_{ij}^R.

Лема 3.3.2. Нека $\mathcal{C} \subset \mathcal{F}_{t,b}$ е кода, за който $R(\mathcal{C}) = R$ и $\{\mathcal{S}_j | j = 1, 2, \ldots, m\}$ е регулярно разделяне на $\mathcal{F}_{t,b}$. Тогава за всяко $i \in \{1, 2, \ldots, m\}$ е изпълнено

$$\sum_{j=1}^{m} \big(|\mathcal{C} \cap \mathcal{S}_j| \sum_{k=0}^{R} r_{ij}^k \big) \;\geq\; |\mathcal{S}_i|.\diamond \tag{3.6}$$

В случая $m = 1$ горната граница съвпада с границата на сферичната опаковка.

За множеството $\mathcal{F}_{t,b}$ да изберем $t' \leq t$ троични и $b' \leq b$ двоични координати, например онези с номера $1, \ldots, t'$ и $t+1, \ldots, t+b'$. Нека $\mathbf{v} = (v_1, v_2, \ldots, v_{t'}, v_{t'+1}, \ldots, v_{t'+b'}) \in \mathcal{F}_{t',b'}$ и

$$\mathcal{S}_{\mathbf{v}} = \big\{ (x_1, x_2, \ldots, x_n) \in \mathcal{F}_{t,b} | x_i = v_i, i = 1, \ldots, t'; x_{t+j} = v_{t'+j}, j = 1, \ldots, b' \big\}. \tag{3.7}$$

$\{\mathcal{S}_{\mathbf{v}} | \mathbf{v} \in \mathcal{F}_{t',b'}\}$ дефинира регулярно разделяне на $\mathcal{F}_{t,b}$. За опростяване на записването със σ_i означаваме броят на думите от $\mathcal{F}_{t-t',b-b'}$, които се съдържат в сфера, с радиус i, като полагаме $\sigma_0 = 1$.

Нека $\mathcal{U} \subset \mathcal{F}_{t',b'}$ е такова, че $\{\mathcal{U}, \mathcal{F}_{t'b'} \setminus \mathcal{U}\}$ е регулярно разделяне на $\mathcal{F}_{t',b'}$. Константите от (ii) за това разделяне ще означаваме с ρ_{ij}^R, $i, j \in \{1, 2\}$ (множеството $\mathcal{U}$ се разглежда като първо).

Лема 3.3.3. Нека $\mathcal{C} \subset \mathcal{F}_{t,b}$ е код с радиус на покритие R и нека $\{\mathcal{S}_{\mathbf{v}} | \mathbf{v} \in \mathcal{F}_{t',b'}\}$ е регулярното разбиване, дефинирано по-горе. Тогава

$$\sum_{i=0}^{min\{R,t'+b'\}} \Big(\sum_{\mathbf{v} \in \mathcal{F}_{t',b'} \setminus \mathcal{U}} \sigma_{R-i} \rho_{21}^{i} |\mathcal{C} \cap \mathcal{S}_{\mathbf{v}}| + \sum_{\mathbf{u} \in \mathcal{U}} \sigma_{R-i} \rho_{11}^{i} |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}}| \Big) \geq 3^{t-t'} 2^{b-b'} |\mathcal{U}|. \quad (3.8)$$

Доказателство. Достатъчно е да сумираме двете страни на 3.6 за всички $\mathbf{u} \in \mathcal{U}$. □

Лема 3.3.4. Нека $b' = 2, t' = 0$ и $\mathcal{C} \subset \mathcal{F}_{t,b}$ е код с радиус на покритие $R = 1$. За всяко $\mathbf{u} \in \mathcal{F}_{t',b'}$ е изпълнено

$$|\mathcal{C} \cap \mathcal{S}_{\mathbf{v}}| \geq \frac{3^t 2^{b-2} - |\mathcal{C}|}{2t + b - 3}. \quad (3.9)$$

Доказателство. Нека $\mathbf{u} = (00), \mathbf{u}' = (11), \mathbf{v} = (10), \mathbf{v}' = (01)$ и да изберем $\mathcal{U} = \{\mathbf{u}, \mathbf{u}'\}$. От 3.8 следва, че

$$\begin{aligned} \sigma_1(|\mathcal{C} \cap \mathcal{S}_{\mathbf{u}}| + |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}'}|) + \sigma_0(|\mathcal{C} \cap \mathcal{S}_{\mathbf{v}}| + |\mathcal{C} \cap \mathcal{S}_{\mathbf{v}'}|) &\geq 3^t 2^{b-1}, \\ |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}}| + |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}'}| &\geq \frac{3^t 2^{b-1} - 2|\mathcal{C}|}{\sigma_1 - 2}. \end{aligned}$$

Имаме

$$\begin{aligned} |\mathcal{C}| &= |\mathcal{C} \cap (\cup_{\mathbf{w}} \mathcal{S}_{\mathbf{w}})| = |\cup_{\mathbf{w}} (\mathcal{C} \cap \mathcal{S}_{\mathbf{w}})| \\ &\geq |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}}| + |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}'}| + |\mathcal{C} \cap \mathcal{S}_{\mathbf{v}}| + |\mathcal{C} \cap \mathcal{S}_{\mathbf{v}'}| \\ &\geq |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}}| + \frac{3^t 2^{b-1} - 2|\mathcal{C}|}{\sigma_1 - 2} - |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}}| + 3^t 2^{b-2} - \sigma_1 |\mathcal{C} \cap \mathcal{S}_{\mathbf{u}}|, \end{aligned}$$

откъдето следва твърдението на лемата. □

Нека $\mathcal{T} = \{\mathcal{T}_1, \ldots, \mathcal{T}_p\}$ е разбиване на множеството на координатите със свойството, че всяко $\mathcal{T}_j$ съдържа или само двоични или само троични координати. За думата $\mathbf{u} \in \mathcal{F}_{t,b}$ с $\mathbf{u}|_{\mathcal{T}_j}$ означаваме думата, получена от $\mathbf{u}$ като

избираме само координатите от $\mathcal{T}_j$. Нека $\mathbf{a} = (a_1, a_2, \ldots, a_p)$, където всички a_i са неотрицателно цели числа и $a_i \leq |\mathcal{T}_i|$. Тогава $\{\mathcal{S}_\mathbf{a}\}$, където

$$\mathcal{S}_\mathbf{a} = \left\{\mathbf{u} \in \mathcal{F}_{t,b} | wt(\mathbf{u}|_{\mathcal{T}_j}) = a_j, j = 1, 2, \ldots, p\right\} \tag{3.10}$$

и $\mathbf{a}$ пробягва всички възможни p-орки, е регулярно разделяне на $\mathcal{F}_{t,b}$.

По-общо, ако H е подгрупа на G, то орбитите на H върху $\mathcal{F}_{t,b}$ дефинират регулярно разбиване. Разбиванията, дефинирани в 3.7 и 3.10 са от този вид.

Нека $\mathcal{C} \subset \mathcal{F}_{t,b}$ и $\mathcal{S}_\mathbf{v}$ са както са дефинирани в 3.7. С $\mathcal{C}_\mathbf{v}$ означаваме множеството от думи $\mathcal{F}_{t-t',b-b'}$, получени от $\mathcal{C} \cap \mathcal{S}_\mathbf{v}$ чрез изтриване на фиксираните координати. Нека $c_\mathbf{v} = |\mathcal{C}_\mathbf{v}|$.

Лема 3.3.5. Нека $\mathcal{C} \subset \mathcal{F}_{t,b}$ е код с радиус на покритие 1, $b \geq 2$ и нека $b' = 2, t' = 0$. Тогава $\mathcal{C}_{\mathbf{u}+(01)} \cup \mathcal{C}_{\mathbf{u}+(10)} \supset \mathcal{N}(\mathcal{C}_\mathbf{u})$. Освен това, ако $\mathcal{C}_{\mathbf{u}\cup(01)} \cup \mathcal{C}_{\mathbf{u}+(10)} = \mathcal{N}(\mathcal{C}_\mathbf{u}) \cup \mathcal{B}$, то $\mathcal{C}_{\mathbf{u}+(11)} \cup \mathcal{C}_\mathbf{u} \supset \cup_{k<2}\mathcal{C}^{(k)}(\mathcal{N}(\mathcal{C}_\mathbf{u}) \bigcup \mathcal{B})$.

3.3.1 Определяне на $K(1, 5, 1)$

В [19], [54] са представени границите $13 \leq K(1, 5, 1) \leq 16$. Да допуснем, че съществува код $\mathcal{C} \subset \mathcal{F}_{1,5}$ с радиус на покритие 1 и $|\mathcal{C}| = 15$. От Лема 3.3.4 следва, че $c_\mathbf{u} \geq 3$ за всяко $\mathbf{u} \in \mathcal{F}_{0,2}$.

Лема 3.3.6. Нека $\mathcal{A} \subset \mathcal{F}_{1,3}, |\mathcal{A}| = 3$. Тогава $|\mathcal{C}(\mathcal{A})| \leq 18, |\mathcal{C}(\mathcal{A})| \neq 17$. С точност до еквивалентност имае:

(i) Ако $|\mathcal{C}(\mathcal{A})| = 18$, то $\mathcal{A} = \{(0100), (1010), (2001)\}$.

(ii) Ако $|\mathcal{C}(\mathcal{A})| = 16$, то $\mathcal{A} = \{0000, 1111, 2011\}$ или $\{0011, 0101, 1110\}$.

(iii) Ако $|\mathcal{C}(\mathcal{A})| = 15$, то $\mathcal{A} = \{0000, 1000, 2110\}$, $\{0000, 1000, 0111\}$ или $\{0000, 1000, 2111\}$.

Без ограничение можем да допуснем, че $c_{00} = 3$. Сега от Лема 3.3.5 следва, че (ii) и (iii) от горната лема са невъзможни. Ако $\mathcal{C}_{00}$ е еквивалентен на $\mathcal{A}$ от (i), то същата лема дава $c_{01} + c_{10} = 8$ или 9.

Първо ще разгледаме случая $c_{01} + c_{10} = 9$. Без ограничение имаме $c_{11} = 3$, $c_{01} = 4$, $c_{10} = 5$. Да забележим, че $\mathcal{A}$ от Лема 3.3.6(i) има група от автоморфизми от ред 3. Тя се поражда от $\tau = \varphi_\sigma \psi_{\mathbf{a}}$, където $\sigma = (234) \in S_3$ и $\mathbf{a} = (1000)$. Вече знаем, че има само два (с точност до еквивалентност) избора за $\mathcal{C}_{11}$ и следователно $|\mathcal{N}(\mathcal{A}) \cup \mathcal{N}(\mathcal{C}_{11})| \leq 9$:

(а) $\mathcal{C}_{11} = \mathcal{A}^{\psi_{\mathbf{a}}}$;

(б) $\mathcal{C}_{11} = \mathcal{A}$.

(а) В този случай знаем думите от $\mathcal{C}_{01} \cup \mathcal{C}_{10}$. Директна проверка показва противоречие с Лема 3.3.5.

(б) В този случай три от думите в $\mathcal{C}_{01} \cup \mathcal{C}_{10}$ не са известни. За да покрием думите $(*01000)$ и $(*10000)$ две от думите в $\mathcal{C}_{01} \cup \mathcal{C}_{10}$ трябва да имат вида $(*000)$. Можем да ги изберем като (0000) и (1000). Има две възможности за третата дума в $\mathcal{C}_{01} \cup \mathcal{C}_{10}$. И в двата случая не получаваме код с радиус на покритие 1 при всяко разделяне на думите в $\mathcal{C}_{01} \cup \mathcal{C}_{10}$.

Сега да разгледаме случая $c_{01} + c_{10} = 8$. Ясно е, че $c_{01} = c_{10} = 4$. Да означим с $\rho^{p,q}_{\alpha,\beta}$, $\alpha, \beta \in \mathbb{F}_2$, $1 \leq p < q \leq 5$ броят на думите от $\mathcal{C}$, имащи α в p-та и β в q-та двоични координати. Доказахме, че за всеки избор на p, q, $1 \leq p < q \leq 5$, съществува двойка (α, β) от 0 и 1, за която $\rho^{p,q}_{\alpha,\beta} = 3$ и $\rho^{p,q}_{\alpha+i,\beta+j} = 4$ за $(i, j) \in \{(01), (10), (11)\}$. Без ограничение двоичната част от кодовите думи на $\mathcal{C}$ е:

	1 0 * * *
0 0 1 0 0	1 0 * * *
0 0 0 1 0	1 0 * * *
0 0 0 0 1	1 0 * * *
0 1 * * *	1 1 * * *
0 1 * * *	1 1 * * *
0 1 * * *	1 1 * * *
0 1 * * *	1 1 * * *

Да допуснем, че $\rho_{0,1}^{1,3} = 3$. Следователно $\rho_{0,1}^{2,3} = 3$ и директно се вижда, че думите от $\mathcal{S}_{001}$ не могат да бъдат покрити от $\mathcal{C}$, откъдето $\rho_{0,1}^{1,3} = 4$ и $\rho_{0,0}^{1,3} = 3$. По същия начин се доказва, че $\rho_{0,0}^{1,i} = 3$, $i = 4, 5$, и оттук $\rho_{0,0}^{i,j} = 3$ за всеки $i, j,\ 1 \leq i, j \leq 5$. Освен това всеки един от последните три стълба съдържа точно три нули в думите $(11 * **)$. Следователно двоичната част на кода $\mathcal{C}$ (с точност до еквивалентност) е

	1 0 0 1 1
0 0 1 0 0	1 0 1 0 1
0 0 0 1 0	1 0 1 1 0
0 0 0 0 1	1 0 1 1 1
0 1 0 1 1	1 1 1 0 0
0 1 1 0 1	1 1 0 1 0
0 1 1 1 0	1 1 0 0 1
0 1 1 1 1	1 1 0 0 0

Сега думите $(*11111)$ от $\mathcal{F}_{1,5}$ не могат да бъдат покрити от $\mathcal{C}$. С това доказахме следното твърдение.

Лема 3.3.7. Изпълнено е равенството $K(1, 5, 1) = 16$.

3.3.2 Определяне на $K(2, 4, 1)$

В [19], [54] са представени границите $17 \leq K(2, 4, 1) \leq 20$. Да допуснем, че за кода $\mathcal{C}$ е изпълнено $|\mathcal{C}| = 19$. Както по-горе имаме $c_{\mathbf{u}} \geq 4$ за всяко $\mathbf{u} \in \mathcal{F}_{0,2}$.

Лема 3.3.8. Нека $\mathcal{A} \subset \mathcal{F}_{2,2}, |\mathcal{A}| = 4$. Тогава $|\mathcal{C}(\mathcal{A})| \leq 28, |\mathcal{C}(\mathcal{A})| \neq 27$. С точност до еквивалентност имаме:

(i) ако $|\mathcal{C}(\mathcal{A})| = 28$, то $\mathcal{A} = \{0000, 1101, 2110, 0211\}$;

(ii) ако $|\mathcal{C}(\mathcal{A})| = 26$, то $\mathcal{A} = \{0000, 1100, 2210, 1011\}$, $\{0000, 0011, 1110, 2101\}$, $\{0000, 0011, 1110, 2201\}$, $\{0000, 0101, 1110, 2011\}$, $\{0000, 0101, 1110, 2211\}$ или $\{0000, 0101, 1210, 2011\}$;

(iii) ако $|\mathcal{C}(\mathcal{A})| = 25$, то

$$\mathcal{A} = \{0000, 1000, 2110, 2201\} \text{ или } \{0000, 1000, 2110, 0211\}.$$

Случаите (ii) и (iii) се отхвърлят както по-горе (като използваме Лема 3.3.5). По същия начин доказваме, че (i) е невъзможно когато $c_{01} + c_{10} = 8, 9$ или 11. В случая когато $c_{01} + c_{10} = 11$ използваме очевидното свойство, че $Aut\,\mathcal{A} > \{id, \mu_{1,2}\varphi_\sigma, \mu_{2,2}\psi_{\mathbf{a}}\psi_{\mathbf{b}}\varphi_\sigma, \mu_{2,2}\psi_{\mathbf{a}}\psi_{\mathbf{b}}\mu_{1,2}\}$, $\mathbf{a} = (0200)$, $\mathbf{b} = (0011)$, $\sigma = (34)$.

Остава да разгледаме случая $c_{01} + c_{10} = 10$. Очевидно $c_{01} = c_{10} = 5$ и $\mathcal{C}_{00} = \mathcal{A}$, където $\mathcal{A}$ е взето от (i). Можем да приемем, че това е вярно за всеки избор на двоична координата. Двоичната част на $\mathcal{C}$ е:

	$1\ 0\ *\ *$
$0\ 0\ 0\ 0$	$1\ 0\ *\ *$
$0\ 0\ 0\ 1$	$1\ 0\ *\ *$
$0\ 0\ 1\ 0$	$1\ 0\ *\ *$
$0\ 0\ 1\ 1$	$1\ 0\ *\ *$
$0\ 1\ *\ *$	$1\ 1\ *\ *$
$0\ 1\ *\ *$	$1\ 1\ *\ *$
$0\ 1\ *\ *$	$1\ 1\ *\ *$
$0\ 1\ *\ *$	$1\ 1\ *\ *$
$0\ 1\ *\ *$	$1\ 1\ *\ *$

Без ограничение можем да приеме, че $\rho_{0,0}^{i,j} = 4$ за всяко $i, j,\ 1 \le i < j \le 4$ (защото можем да разменим нулите и единиците в координатите). Третият и четвъртият стълб съдържат по две нули и три единици в думите от вида $(01**)$. Същото е вярно и за думите $(10**)$. Думата (0100) трябва да се среща измежду думите от вида $(01**)$, защото в противен случай елементите на $\mathcal{F}_{2,4}$ не могат да бъдат покрити от $\mathcal{C}$. По подобен начин (1000) е между думите от вида $(10**)$. Следователно с точност до еквивалентност двоичната

част на кода $\mathcal{C}$ става:

	1 0 0 0
0 0 0 0	1 0 0 1
0 0 0 1	1 0 1 0
0 0 1 0	1 0 1 1
0 0 1 1	1 0 1 1
0 1 0 0	1 1 0 0
0 1 0 1	1 1 0 1
0 1 1 0	1 1 0 1
0 1 1 1	1 1 1 0
0 1 1 1	1 1 1 0

Сега $\mathcal{C}$ не може да покрие всички думи от вида $(**1111)$. С това доказахме следното твърдение.

Лема 3.3.9. Изпълнено е равенството $K(2,4,1) = 20$.

3.3.3 Определяне на $K(4,2,1)$

Да припомним, че с $K(t,b) = K_{3,2}(t,b)$ означаваме минималната мощност на код с $b \neq 0$ двоични и $t \neq 0$ троични координати и радиус на покритие 1. В [19], [54] са доказани неравенствата $30 \leq K(4,2) \leq 36$. В тази част ще докажем, че $K(4,2,1) = 36$.

Да отбележим, че директното произведение на F_2^2 и троичния код на Хеминг е код с 2 двоични и 4 троични координати, радиус на покритие 1 и 36 кодови думи. Следователно, достатъчно е да докажем, че ако C е код с 2 двоични и 4 троични координати и радиус на покритие 1, то $|C| > 35$.
Без ограничение можем да считаме, че първите две координати са двоични. Ще използваме следните означения.

$$P_{ij} = \{(i,j,u_1,u_2,u_3,u_4); i,j \in F_2; u_1,u_2,u_3,u_4 \in F_3\}.$$

Множеството от вектори P_{ij} ще наричаме *равнина*.

Нека $c_{ij} = |P_{ij} \cap C|$, т.е. c_{ij} е броят на кодовите думи в равнината A_{ij}.

С p_{ij} ще означаваме броят на векторите от C_{ij}, които са покрити от кодовите думи от тази равнина. Тъй като всеки троичен вектор с дължина 4 покрива 9 вектора, то $p_{ij} \leq 9c_{ij}$.

Дефиниция 3.3.2. Троичен вектор (u_1, u_2, u_3, u_4) се нарича *опашка* ако съществуват $i, j \in F_2$, за които $(i, j, u_1, u_2, u_3, u_4)$ е кодова дума.

Теорема 3.3.1. Не съществува код C с 2 двоични и 4 троични координати, радиус на покритие 1 и 35 кодови думи.

Доказателство. Нека C е код с 2 двоични, 4 троични координати, радиус на покритие 1 и 35 кодови думи. Без ограничение можем да допуснем, че $c_{00} + c_{11} \leq c_{01} + c_{10}$ and $c_{00} \leq c_{11}$. Тъй като $|C| = 35$ получаваме

$$c_{00} \leq 8; \quad c_{00} + c_{11} \leq 17. \tag{3.11}$$

Ще извършим доказателството на теоремата като последователно отхвърлим случаите $c_{00} < 7$, $c_{00} = 7$ и $c_{00} = 8$.

Лема 3.3.10. За произволни $i, j \in F_2$ е изпълнено неравенството $c_{ij} \geq 7$.

Доказателство. Тъй като всяка кодова дума от C_{01} и C_{10} покрива точно един вектор от C_{00} и тъй като $|C_{ij}| = 81$ трябва да е изпълнено неравенството:

$$c_{01} + c_{10} + p_{00} \geq 81.$$

Прибавяме $c_{00} + c_{11}$ към двете страни на горното неравенство и получаваме:

$$35 \geq 81 - p_{00} + c_{00} + c_{11} \geq 81 - p_{00} + 2c_{00}.$$

Накрая

$$p_{00} - 2c_{00} \geq 46 \tag{3.12}$$

Това неравенство дава $7c_{00} \geq 46$. Следователно $c_{ij} \geq 7$ за произволни $i, j \in \mathbb{F}_2$. $\square$

Да отбележим, че ако знаем кодовите думи в C_{00}, (т.е. знаем c_{00} и p_{00}) то неизвестни опашки в равнините C_{01} и C_{10} са най-много

$$35 - 2c_{00} - (81 - p_{00}) = p_{00} - 46 - 2c_{00}. \tag{3.13}$$

От Лема 4.3.2 следва, че $c_{00} = 7$ или $c_{00} = 8$. Всяко цяло число между 0 и 80, записано в троична система представлява вектор с дължина 4 над F_3. За по-съкратено записване всеки троичен вектор с дължина 4 ще заместваме със съответното цяло число и ще наричаме това число вектор.

Лема 3.3.11. Изпълнено е неравенството $c_{00} \neq 7$.

Доказателство. Да допуснем, че $c_{00} = 7$. От 3.11 следва, че $c_{11} \leq 10$. Неравенство 3.12 показва, че $p_{00} \geq 60$ и следователно p_{00} е равно на $60, 61, 62$ или 63. С точност до еквивалентност за троични вектори с дължина 4 имаме:

а) съществуват две множества със 7 вектора, покриващи 60 вектора (това са {0,13,26,32,42,46,54} и {0,13,26,32,42,59,73})

б) съществува единствено множество със 7 вектора, покриващо 61 вектора (това множество е {0,13,26,32,42,55,75})

в) не съществува множество със 7 вектора, което покрива 62 вектора

г) съществува единствено множество със 7 вектора, покриващо 63 вектора (това множество е {0,13,26,32,42,46,61} и е подмножество на $[4, 2, 3]$ троичен кода на Хеминг);

Следователно за опашките в C_{00} има само 4 възможни множества. Ще разгледаме всеки един от горните случаи.

а) неравенството 3.13 показва, че и за двете множества има по 21 опашки в C_{01} и C_{10} и в тях няма повече опашки.

За първото множество има 18 (1,2,3,5,6,9,15,18,19,27,28,29,30,33,36,40,45,53) вектора, които не са покрити по два пъти в C_{01} и C_{10} от опашките в C_{00}, C_{01}

и C_{10}. Тези 18 вектора трябва да бъдат опашки в C_{11}. Това е противоречие с $c_{11} \leq 10$.

За второто множество има 15 (2,3,4,5,8,14,15,19,23,30,35,41,56,58,77) вектора, които не са покрити два пъти в C_{01} и C_{10} от опашките в C_{00}, C_{01} и C_{10}. Това означава, че $c_{11} \geq 15$, което е противоречие.

б) Същите разсъждения показват, че:

- има 20 известни опашки в C_{01} и C_{10}. (т.е. $c_{01} + c_{10} \geq 20$)

- има най-много още една опашка в C_{01} и C_{10}.

- поне в една от равнините C_{01} and C_{10} няма повече опашки (освен известните).

- в C_{01} and C_{10} има 10 (3,5,12,15,21,23,24,30,39,58) непокрити вектора (от известните опашки).

Следователно $c_{11} \geq 10$, което е противоречие с $|C| = 35$.

г) Както по-горе получаваме:

- има 18 известни опашни в C_{01} и C_{10}.

- има най-много още 3 опашки в C_{01} и C_{10}.

- в една от равнините C_{01} and C_{10} има най-много една нова опашка.

- имаме 20 (1,4,5,6,7,8,15,16,19,25,27,28,31,33,34,35,40,43,52,53) непокрити (от известните опашки) вектора в C_{01} и C_{10}.

Тъй като една опашка покрива 9 вектора в нейната равнина, то има поне $20-9 = 11$ вектора, които трябва да бъдат опашки в C_{11}. Това е противоречие с 3.11. □

Лема 3.3.12. Изпълнено е неравенството $c_{00} \neq 8$.

Доказателство. Нека $c_{00} = 8$. Неравенство 3.11 дава $c_{11} \leq 9$, а от неравенство 3.12 получаваме $p_{00} \geq 62$. Следователно трябва да опишем всички множества от 8 троични вектора, всяко от които покрива поне 62 вектора. С използване на компютър намираме, че с точност до еквивалентност за множествата с 8 вектора имаме:

а) 262 множества, покриващи 62 вектора;

б) 119 множества, покриващи 63 вектора;

в) 34 множества, покриващи 64 вектора;

г) 8 множества, покриващи 65 вектора;

д) 6 множества, покриващи 66 вектора;

е) едно множество, покриващо 67 вектора - {0,13,26,32,34,65,61,75};

ж) едно множество, покриващо 68 вектора - {0,13,26,32,28,42,65,75};

з) не съществува множество, покриващо 71, 70 или 69 вектора;

и) едно множество, покриващо 72 вектора - {13,26,32,42,46,61,65,75}.

Съответните множества могат да бъдат намерени в [37].

Нека сме определили векторите в C_{00}. Тогава знаем $81 - p_{00}$ опашки в C_{01} и C_{10}. Нека B_i за $i = 0, 1$ е множеството от вектори покрити i пъти в C_{10} и C_{01} от известните опашки в C_{00}, C_{01} и C_{10}. Тогава известните опашки от C_{11} (има 8 или 9 такива опашки) и неизвестните опашки от C_{01} и C_{10} (има $35-8-(81-p_{00})-c_{11} = p_{00}-54-c_{11}$ такива опашки) трябва да покриват в C_{01} и C_{10} всеки вектор от B_0 два пъти и всеки вектор от B_1 по един път. Всяка опашка от C_{11} покрива два вектора в C_{01} и C_{10}. Всеки вектор с дължина 4 покрива определен брой вектори от B_0 и B_1. Нека t_{max} е най-голямото от тези 81 числа (да отбележим, че $t_{max} \leq 9$). Тъй като имаме $p_{00} - 54 - c_{11}$ неизвестни опашки в C_{01} и C_{10}, имаме:

$$2c_{11} + t_{max}(p_{00} - 54 - c_{11}) \geq 2|B_0| + |B_1| \tag{3.14}$$

а) В този случай $c_{11} = 8$ и 3.14 е еквивалентно на $16 \geq 2|B_0| + |B_1|$. За нито едно от тези 262 множества това неравенство не е изпълнено.

б) Неравенство 3.14 е еквивалентно на $81 \geq 7c_{11}+2|B_0|+|B_1|$, където c_{11} е 8 или 9. Следователно $25 \geq 2|B_0| + |B_1|$. За нито едно от тези 119 множества това неравенство не е вярно.

в) Отново от 3.14 получаваме $10t_{max} \geq (t_{max} - 2)c_{11} + 2|B_0| + |B_1|$, където

c_{11} е равно на 8 или 9. Това неравенство не е изпълнено за нито едно от дадените 34 множества.

г) За 3 от дадените множества ($\{0, 13, 26, 32, 28, 42, 46, 65\}$; $\{0, 13, 26, 32, 28, 42, 46, 75\}$ и $\{0, 13, 26, 32, 42, 46, 55, 61\}$) получаваме противоречие директно от 3.14. Ще разгледаме едно от останалите множества.

Нека опашките в C_{00} са 0,13,26,32,36,69,59 и 73. Тогава $B_0 = \{5, 15, 19, 54, 67, 80\}$ и $B_1 = \{2, 3, 4, 8, 9, 10, 12, 14, 18, 23, 39, 41, 47, 56, 57, 58, 62, 63, 64, 66, 68, 72, 77\}$. Директна проверка показва, че всяка възможна опашка покрива най-много един вектор от B_0 и най-много 6 вектора от B_1. Понеже имаме най-много още 3 опашки в C_{01} и C_{10}, са възможни следните случаи:

- съществуват поне 5 вектора от B_0, които не са покрити по два пъти в C_{01} и C_{10} от тези 3 опашки и следователно тези 5 вектора са опашки в C_{11}.

- съществуват поне 5 вектора от B_1, които не са покрити в C_{01} и C_{10} от тези 3 опашки и следователно тези 5 вектора са опашки в C_{11}.

Следователно $c_{11} \geq 10$, което противоречи на 3.11.

д) Този случай е аналогичен на (г).

е) Нека опашките в C_{00} са 0,13,26,32,34,65,61 и 75. Имаме 14 неизвестни опашки в C_{01} и C_{10} и най-много 5 неизвестни опашки в C_{01} и C_{10}. В този случай $|B_0| = 20$ и $|B_1| = 12$. Директно се вижда, че ако в C_{01} и C_{10} има най-много една опашка, то $c_{11} \geq 11$, което е противоречие с 3.11. Следователно, без ограничение в C_{10} има две нови опашки. Директна проверка показва, че всяка възможна опашка покрива най-много 8 вектора от B_0 и B_1. Сега 3.14 дава $c_{11} = 8$. Следователно в C_{01} има 3 нови опашки. Отново директно се проверява, че единствената възможност (при която c_{11} може да бъде 8) за двете опашки в C_{10} е 5 и 59 (всеки от тези два вектора покрива 8 вектора от B_0 и 0 вектора от B_1). Следователно опашките от C_{01} трябва да покриват поне 24 вектора от B_0 и B_1. Лесно се ппроверява, че такова множество от три вектора не съществува.

ж) Този случай е аналогичен на (е).

и) Нека кодовите думи в C_{00} са 13,26,32,42,46,61,65,75. Знаем 9 опашки в C_{10} и C_{01}; $B_0 = \{14, 16, 17, 22, 23, 25, 31, 34, 35, 37, 38, 39, 40, 41, 43, 44, 47, 48, 49, 50, 51, 52, 53, 58, 59, 62, 64, 66, 67, 68, 69, 70, 71, 73, 74, 76, 77, 78, 79, 80\}$, като $B_1 = \phi$. Да забележим, че B_0 се състои от всички вектори с тегло 3 и 4 с изключение на опашките в C_{00}. Оказва се, че всеки вектор с тегло 0 или 1 не покрива нито един вектор от B_0; всеки вектор с тегло 2 покрива 3 вектора от B_0; всеки вектор с тегло 3 покрива 5 вектора от B_0; всеки вектор с тегло 4 покрива 8 вектора от B_0.

Да разгледаме множеството D от вектори с тегло 3 от B_0. Директно се проверява, че всеки вектор покрива най-много три вектора от D. Тъй като $|D| = 24$, ако броят на опашките в C_{ij} е n_{ij}, то $c_{11} \geq 24 - 3min(n_{01}, n_{10})$. Следователно:

$$3\min(n_{01}, n_{10}) + c_{11} \geq 24. \tag{3.15}$$

От друга страна понеже $|C| = 35$, то

$$n_{01} + n_{10} + c_{11} \leq 18. \tag{3.16}$$

Неравенства 3.15 и 3.16 показват, че $\min(n_{01}, n_{10}) \geq 6$. Това неравенство заедно с $c_{11} \geq 8$ противоречи на 3.16. □

От Лема 4.3.2, Лема 4.3.3 и Лема 3.3.12 следва, че код с 2 двоични, 4 троични координати, радиус на покритие 1 и 35 кодови думи не съществува. □

Лема 3.3.13. Нека $\mathcal{C}_1$ е троичния $[7, 4, 3]$ код на Хеминг. Тогава декартовото произведение

$$C = F_2^2 \times \mathcal{C}$$

представлява код с 2 двоични, 4 троични координати, радиус на покритие 1 и 36 кодови думи.

Доказателство. Нека $b_1b_2t_1t_2t_3t_4$ е произволен вектор от $F_2^2 \times F_3^4$. Тъй като троичния $[7, 4, 3]$ код на Хеминг има радиус на покритие 1, то съществува

кодова дума $x_1x_2x_3x_4$, за която $d(t_1t_2t_3t_4, x_1x_2x_3x_4) \leq 1$. Тогава $b_1b_2x_1x_2x_3x_4$ е кодова дума от C, за която

$$d(b_1b_2t_1t_2t_3t_4, b_1b_2x_1x_2x_3x_4) = d(t_1t_2t_3t_4, x_1x_2x_3x_4) \leq 1.$$

□

От Теорема 3.3.1 и Лема 3.3.13 следва, че $K(4,2) = 36$.

В [39] е доказано, че всеки троичен код с дължина 5 и радиус на покритие 1 се получава като директно произведение на F_3 и троичния код на Хеминг с дължина 4. Полученото равенство $K(4,2)$=36 поставя въпроса дали всеки смесен код с две двоични и четири троични координати и радиус на покритие 1 се получава чрез конструкцията от Лема 3.3.13.

3.4 Покриващи кодове с $R > 1$

В тази част ще намерим точните стойности на $K(1, 2R+1, R)$, $K(2, 2R-1, R)$, $K(2, 2R, R)$, $K(3, 2R-2, R)$ при $R > 1$ и на $K(5, 0, 2)$.

3.4.1 Определяне на $K(1, 2R+1, R)$

Лема 3.4.1. За всяко цяло число $R \geq 1$ е изпълнено равенството $K(1, 2R+1, R) = 6$.

Доказателство. Известно е, че $K(1,3,1) = 6$. Да допуснем, че за всяко $R' < R$ е изпълнено $K(1, 2R'+1, R') \geq 6$. Нека $\{\mathcal{S}_{\mathbf{u}} | \mathbf{u} \in \mathcal{F}_{0,2}\}$ е регулярното разделяне от 3.7 и нека $\mathcal{C} \subset \mathcal{F}_{1,2R+1}$ е код с радиус на покритие R. Според индукционното допускане $|\mathcal{C} \cap \mathcal{S}_{\mathbf{u}}| \geq 1$ за всяко $\mathbf{u} \in \mathcal{F}_{0,2}$. Да допуснем, че $|\mathcal{C}| = 5$. (Ако $\mathcal{C}$ съдържа по-малко от пет думи, той може да бъде разширен чрез добавяне на произволен елемент от $\mathcal{F}_{1,2R+1}$.) Всеки две двоични координати

съдържат всяка дума от $\mathcal{F}_{0,2}$ поне веднъж. Следователно без ограничение двоичната част на кода е

$$\begin{array}{cccccc} 0 & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & * & * & \ldots & * \\ 0 & 1 & \alpha & * & \ldots & * \\ 1 & 0 & \beta & * & \ldots & * \\ 1 & 1 & \gamma & * & \ldots & * \end{array}$$

Лесно се вижда, че $\alpha = \beta \neq \gamma$, откъдето $2R+1 \leq 4$. С това доказахме, че $K(1, 2R+1, R) \geq 6$. Кодът

$$\mathcal{C} = \{(i\underbrace{000\ldots00}_{2R+1}), (i\underbrace{111\ldots11}_{2R+1}) \mid i \in \mathbf{F}_3\} \tag{3.17}$$

има радиус на покритие R и следователно $K(1, 2R+1, R) = 6$. □

3.4.2 Определяне на $K(2, 2R-1, R)$, $K(2, 2R, R)$, $K(3, 2R-2, R)$

Лема 3.4.2. За всяко цяло число $R \geq 1$ е изпълнено равенството $K(2, 2R-1, R) = 4$.

Доказателство. По индукция лесно се доказва, че $K(2, 2R-1, R) \geq 4$. Кодът

(3.2) $$\mathcal{C} = \{(00\underbrace{000\ldots00}_{2R-1}), (00\underbrace{111\ldots11}_{2R-1}), (11\underbrace{000\ldots00}_{2R-1}), (22\underbrace{111\ldots11}_{2R-1})\}$$

доказва, че $K(2, 2R-1, R) = 4$. □

Лема 3.4.3. За всяко цяло число $R \geq 1$ е изпълнено равенството $K(2, 2R, R) = 6$.

Доказателство. Доказателството на неравенството $K(2, 2R, R) \geq 6$ повтаря стъпките от Лема 3.4.1. Чрез изследване на двоичните координати на кодовите думи, получаваме, че $2R \leq 4$. Тъй като $K(2, 2, 1) = 6$, трябва да докажем, че $K(2, 4, 2) \geq 6$. Да допуснем, че съществува код $\mathcal{C} \subset \mathcal{F}_{2,4}$, за който $|\mathcal{C}| = 5$ и $R(\mathcal{C}) = 2$. С точност до еквивалентност кодовите думи са

$$\begin{array}{cccccc} * & * & 0 & 0 & 0 & 0 \\ * & * & 0 & 0 & 1 & 1 \\ * & * & 0 & 1 & 0 & 1 \\ * & * & 1 & 0 & 0 & 1 \\ * & * & 1 & 1 & 1 & 0 \end{array}$$

Директно се проверява, че думите от $\mathcal{F}_{2,4}$ от вида $(**1111)$ не могат да бъдат покрити със сфери с радиус 2.

Да допуснем, че $\mathcal{C}$ съдържа следните кодови думи:

$$\begin{array}{cccc} 0 & 0 & 0\ldots0 & 0\ldots0 \\ 0 & 0 & 1\ldots1 & 1\ldots1 \\ 1 & 2 & 0\ldots0 & 1\ldots1 \\ 2 & 1 & 0\ldots0 & 1\ldots1 \\ 1 & 1 & 1\ldots1 & 0\ldots0 \\ 2 & 2 & \underbrace{1\ldots1}_{p} & \underbrace{0\ldots0}_{q} \end{array}$$

където p, q са нечетни и $p + q = 2R$. Ще докажем, че $R(\mathcal{C}) = R$.

Да фиксираме регулярно разделяне на $\{\mathcal{S}_{\mathbf{u}} | \mathbf{u} \in \mathcal{F}_{2,0}\}$. Думите от $\mathcal{S}_{00}$ са покрити. Нека $\mathbf{x} \in \mathcal{F}_{2,2R}$ е непокрита дума от някое от $\mathcal{S}_{01}$, $\mathcal{S}_{02}$, $\mathcal{S}_{10}$, $\mathcal{S}_{20}$. Поради симетрията на кода можем да приемем, че

$$\mathbf{x} = (0\,1\,\underbrace{1\,1\ldots1}_{a}\,\underbrace{0\,0\ldots0}_{p-a}\,\underbrace{1\,1\ldots1}_{b}\,\underbrace{0\,0\ldots0}_{p-b})$$

Ако $a+b \neq R$, то $\mathbf{x}$ е покрит от $\mathcal{C} \cap \mathcal{S}_{00}$ и следователно $a+b=R$. Думите от $\mathcal{C} \cap \mathcal{S}_{21}$ и $\mathcal{C} \cap \mathcal{S}_{11}$ не покриват $\mathbf{x}$, откъдето

$$\begin{aligned} a+q-b &\geq R \\ p-a+b &\geq R \end{aligned}$$

От $b=R-a$ намираме

$$\begin{aligned} 2a+q-R &\geq R \\ p-2a+R &\geq R \end{aligned}$$

т.е. $2a \geq 2R-q=p$ и $2a \leq p$. Следователно $2a=p$, което е невъзможно.

Нека $\mathbf{x}$ не е покрит от $\mathcal{C}$ и се съдържа в някое от множествата $\mathcal{S}_{11}$, $\mathcal{S}_{12}$, $\mathcal{S}_{21}$, $\mathcal{S}_{22}$. Без ограничение можем да допуснем, че

$$\mathbf{x} = (1\,1\,\underbrace{1\,1\ldots1}_{a}\,\underbrace{0\,0\ldots0}_{p-a}\,\underbrace{1\,1\ldots1}_{b}\,\underbrace{0\,0\ldots0}_{p-b})$$

Както по-горе, тъй като $\mathbf{x}$ не е покрит от $\mathcal{C} \cap \mathcal{S}_{11}$ и от $\mathcal{C} \cap \mathcal{S}_{12}$ води до

$$\begin{aligned} p-a+b &\geq R+1 \\ a+q-b &\geq R \end{aligned}$$

откъдето $p+q \geq 2R+1$, което е противоречие. □

Лема 3.4.4. За всяко цяло число $R \geq 1$ е изпълнено равенството $K(3, 2R-2, R) = 5$.

Доказателство. Лесно се доказва по индукция, че $K(3, 2R-2, R) \geq 5$. Ще докажем, че кодът $\mathcal{C}$, съставен от думите

$$\begin{array}{ccccc} 0 & 0 & 0 & 0\ldots0 & 0\ldots0 \\ 1 & 1 & 1 & 1\ldots1 & 1\ldots1 \\ 1 & 1 & 1 & 0\ldots0 & 1\ldots1 \\ 2 & 2 & 2 & 1\ldots1 & 1\ldots1 \\ 2 & 2 & 2 & \underbrace{1\ldots1}_{p} & \underbrace{0\ldots0}_{q} \end{array}$$

където p, q са нечетни и $p + q = 2R - 2$ има радиус на покритие R.

Да допуснем, че съществува вектор $\mathbf{x} \in \mathcal{F}_{3,2R-2}$, който не е покрит от $\mathcal{C}$. Нека

$$\mathbf{x} = (* * * \underbrace{1\,1 \ldots 1}_{a}\ \underbrace{0\,0 \ldots 0}_{p-a}\ \underbrace{1\,1 \ldots 1}_{b}\ \underbrace{0\,0 \ldots 0}_{p-b})$$

и да означим с d_i, $i = 0, 1, 2$, разстоянието на троичната част на $\mathbf{x}$ до вектора (iii). Очевидно $\sum_{i=0}^{2} d_i = 6$ за всяко $\mathbf{x} \in \mathcal{F}_{3,2R-2}$. Тъй като $\mathbf{x}$ не е покрит от вяка от петте думи на кода, имаме

$$\begin{array}{lcl} a + b & \geq & R + 1 - d_0 \\ p + q - a - b & \geq & R + 1 - d_1 \\ a + q - b & \geq & R + 1 - d_1 \\ p + q - a - b & \geq & R + 1 - d_2 \\ p - a + b & \geq & R + 1 - d_2 \end{array} \tag{3.18}$$

откъдето

$$3(p + q) - (a + b) \geq 5R + 5 + d_0 - 2\sum_{i=0}^{2} d_i = 5R - 7 + d_0.$$

Изпълнено е $a + b + d_0 \leq R + 1$ с равенство тогава и само тогава, когато имаме равенство във всички неравенства от 3.18. От друга страна

$$a + b + d_0 \geq R + 1,$$

защото в противен случай $\mathbf{x}$ ще бъде покрит от $(000\underbrace{0 \ldots 0}_{p}\underbrace{0 \ldots 0}_{q})$.

Следователно $a + b + d_0 = R + 1$. Сега от последните две неравенства от 3.18 получаваме $p + q - a - b = p - a + b$, т.е. $q = 2b$, което е противоречие. □

3.4.3 Определяне на $K(5, 0, 2)$

Накрая ще разгледаме случая $t = 5, b = 0, R = 2$. Известно е, че $5 \leq K(5, 0, 2) \leq 8$, [19], [54]. Ще докажем, че $K(5, 0, 2) = 8$.

Лема 3.4.5. Изпълено е равенството $K(5,0,2) = 8$.

Доказателство. Нека $\mathcal{C} \subset \mathcal{F}_{5,0}$ е код с радиус на покритие 2, за който $|\mathcal{C}| = 7$. Да разгледаме едно регулярно разделяне $\{\mathcal{S}_{\mathbf{u}} | \mathbf{u} \in \mathcal{F}_{2,0}\}$.

Без ограничение можем да приемем, че $c_{00} = 0$. От Лема 3.3.3 следва, че $c_{01}+c_{10}+c_{02}+c_{20} \geq 4$. Но за всеки четири сфери с радиус 1 в $\mathcal{F}_{3,0}$ съществуват поне 4 непокрити думи. Следователно за всяка дума $\mathbf{u} \in \mathcal{F}_{3,0}$, за която $c_{\mathbf{u}} = 0$ имаме

$$\sum_{d(\mathbf{u},\mathbf{v})=1} c_{\mathbf{v}} \geq 5. \tag{3.19}$$

Съществуват (с точност до еквивалентност) две възможности:

(1) $c_{00} = 0,\ c_{11} = 0,\ c_{22} = 0$;

(2) $c_{00} = 0,\ c_{12} = 0,\ c_{22} = 0$.

В първия случай от 3.19 следва

$$\begin{array}{ccccccccc} c_{01} & + & c_{02} & + & c_{10} & + & c_{20} & \geq & 5 \\ c_{01} & + & c_{10} & + & c_{12} & + & c_{21} & \geq & 5 \\ c_{02} & + & c_{20} & + & c_{12} & + & c_{21} & \geq & 5 \end{array}$$

и следователно $2\sum_{i\neq j} c_{ij} \geq 15$, което е противоречие с $|\mathcal{C}| = 7$.

Във втория случай $c_{11} = c_{21} = 1$ и

$$\begin{array}{ccccccccc} c_{01} & + & c_{02} & + & c_{10} & + & c_{20} & \geq & 5 \\ c_{10} & + & c_{02} & + & c_{11} & + & c_{22} & \geq & 5 \\ c_{02} & + & c_{20} & + & c_{12} & + & c_{21} & \geq & 5, \end{array}$$

което има следните решения

$$\begin{array}{llll} c_{02} = 4, & c_{01} = 1, & c_{10} = 0, & c_{20} = 0; \\ c_{02} = 3, & c_{01} = 0, & c_{10} = 1, & c_{20} = 1. \end{array}$$

Първото решение противоречи на 3.19 за $\mathbf{u} = (10)$. Нека $\rho_{\alpha\beta}^{p,q}$, $\alpha, \beta \in \mathbf{F}_3$, $1 \leq p < q \leq 5$ означава броят на думите в $\mathcal{C}$, съдържащи α в p-та и β в

q-та позиция. До сега доказахме, че за всяка двойка $(p,q), 1 \leq p < q \leq 5$ от координати

- съществува двойка $(\gamma,\delta), \gamma,\delta \in \mathbf{F}_3$, за която $\rho^{p,q}_{\gamma,\delta} = 3$;
- $\rho^{p,q}_{\alpha,\beta} = 0$ за всяка двойка $(\alpha,\beta), \alpha,\beta \in \mathbf{F}_3$, за която $d((\alpha,\beta),(\gamma,\delta)) = 1$;
- $\rho^{p,q}_{\alpha,\beta} = 1$ за всяка двойка $(\alpha,\beta), \alpha,\beta \in \mathbf{F}_3$, за която $d((\alpha,\beta),(\gamma,\delta)) = 2$.

От горните разсъждения следва, че с точност до еквивалентност кодът $\mathcal{C}$ съдържа думите

$$\begin{array}{ccccc} 0 & 0 & \alpha_1 & * & * \\ 0 & 0 & \alpha_2 & * & * \\ 0 & 0 & \alpha_3 & * & * \end{array}$$

Сега лесно се вижда, че за всеки избор на $(\alpha_1,\alpha_2,\alpha_3)$ получаваме противоречие с ограниченията за числата $\rho^{p,q}_{\alpha,\beta}$. Например, ако $\alpha_1 \neq \alpha_2 \neq \alpha_3 \neq \alpha_1$, получаваме противоречие за $p = 1$, $q = 3$. □

По същия начин може да се докаже, че $K(4,1,2) = 6$.

3.5 Оптимални покрития със сфери

В тази част ще представим резултати, получени в [48] и [51]. Да припомним, че задачата за намирането на минималния брой колонки при играта ТОТО 1, които ни осигуряват определен брой познати резултати, е известна като *the football pool problem* [20]. Разглеждаме задачата за намиране на оптимални покрития на $\mathbb{F}_3^n$ за $n \leq 13$ със сфери с радиус n. Това означава, че търсим код C със следното свойство: за всеки елемент $\mathbf{y} \in \mathbb{F}_3^n$ съществува $\mathbf{x} \in C$, за който $\mathbf{d}(\mathbf{x},\mathbf{y}) = n$. Минималната мощност на такъв код се бележи с $T(n)$. Кодът се нарича оптимален, ако $|C| = T(n)$.

Редицата от стойностите на $T(n)$ е част от The on-line encyclopedia of integer sequences, номер A086676 [73].

При разглежданата задача целта е, независимо от резултатите от срещи-

те, винаги да имаме колонка, без нито един познат резултат. Ето защо в [5] тази задача е наречена *inverse football pool problem.*

Първите известни резултати, свързани с определяне на стойностите на $T(n)$ са получени във Финландското списание Veikkaaja през 50-тте години на миналия век. В Таблица 1 за $n \leq 13$ са представени известните резултати за $T(n)$.

n	T(n)	7	29
1	2	8	44
2	3	9	66–68
3	5	10	99–104
4	8	11	149–172
5	12	12	224–264
6	18	13	336–408

Таблица 1.

Точните стойности на $T(n)$ са известни за $n \leq 8$, като за всяко $n \leq 7$ съществува единствено с точност до еквивалентност покритие [5].

При $n = 8$ имаме $T(8) = 44$ като не е известно колко покрития съществуват. Ще докажем, че при $n = 8$ с точност до еквивалентност съществуват две оптимални покрития [48]. Ще определим [51] и точната стойност на $T(9) = 68$.

Ще представим една рекурсивна граница за $T(n)$.

Лема 3.5.1. В сила е неравенството

$$T(n) \geq \frac{3}{2}T(n-1).$$

Доказателство. Да разгледаме оптимално покритие C на $\mathbb{F}_3^n$, т.е. C е покритие и $|C| = T(n)$. Да разгледаме множествата C_0, C_1 и C_2. Тогава

$$C = \{\mathbf{x}0 \mid \mathbf{x} \in C_0\} \cup \{\mathbf{x}1 \mid \mathbf{x} \in C_1\} \cup \{\mathbf{x}2 \mid \mathbf{x} \in C_2\}.$$

Ясно е, че за $\{i,j,k\} = \{0,1,2\}$ множеството $C_i \cup C_j$ е покритие на $\mathbb{F}_3^{n-1}$. Следователно $c_i + c_j \geq T(n-1)$. Аналогично получаваме неравенствата $c_i + c_k \geq T(n-1)$ и $c_j + c_k \geq T(n-1)$. Сумираме тези три неравенства и получаваме

$$2T(n,3) = 2(C_i + C_j + C_k) \geq 3T(n-1,3),$$

откъдето намираме $T(n,3) \geq \frac{3}{2}T(n-1,3)$. □

Известните резултати за $n \leq 6$ както и границите $T(7) \leq 29$ и $T(8) \leq 44$ са получени във Финландското списание Veikkaaja. Очевидно имаме $T(1) = 2$ и като използваме неравенството от Лема 3.5.1, получаваме $T(2) \geq 3$, $T(3) \geq 5$, $T(4) \geq 8$, $T(5) \geq 12$, $T(6) \geq 18$. В долната таблица е представено покритие на $\mathbb{F}_3^6$ с 18 елемента [5].

1.	0 0 0 0 0 0
2.	1 1 1 1 0 0
3.	2 2 1 0 1 0
4.	1 0 2 2 1 0
5.	0 2 2 1 2 0
6.	2 1 0 2 2 0
7.	1 2 2 0 0 1
8.	2 0 1 2 0 1
9.	2 1 2 1 1 1

10.	0 2 0 2 1 1
11.	0 1 1 0 2 1
12.	1 0 0 1 2 1
13.	2 2 0 1 0 2
14.	0 1 2 2 0 2
15.	1 1 0 0 1 2
16.	0 0 1 1 1 2
17.	2 0 2 0 2 2
18.	1 2 1 2 2 2

Таблица 2: Оптимално покритие на $\mathbb{F}_3^6$.

Следователно $T(2) = 3$, $T(3) = 5$, $T(4) = 8$, $T(5) = 12$, $T(6) = 18$.

Да забележим, че за всяко $n \leq 6$ е изпълнено $T(n) = \left\lceil \frac{3}{2}T(n-1) \right\rceil$.

Първата стойност на n, за която $T(n,3) \neq \left\lceil \frac{3}{2}T(n-1) \right\rceil$ е $n = 7$. С търсене с компютър в [5] е доказано, че $T(7) = 29$, докато границата от Лема 3.5.1 дава $T(7) \geq 27$. Като използваме отново неравенството от Лема 3.5.1,

получаваме $T(8) \geq 44$ и понеже съществува покритие на $\mathbb{F}_3^8$ с 44 елемента, то $T(8) = 44$. Горните граници за $n = 9$ и $n = 10$ са получени в [64] чрез т.н. *tabu search*.

След като сме определили точната стойност на $T(n)$ за някое n, се интересуваме колко оптимални нееквивалентни покрития съществуват.

В [5] с компютър е доказано, че при за всяко $n \leq 7$ с точност до еквивалентност съществува единствено покритие. Единственото покритие при $n = 7$ е дадено в Таблица 3. Да означим това покритие с $\mathcal{C}_7$.

1.	0 0 0 0 0 0 0	11.	2 2 2 2 2 2 0	21.	1 2 1 2 2 2 1
2.	1 1 1 1 0 0 0	12.	2 1 2 1 0 0 1	22.	0 1 1 0 2 0 2
3.	2 2 1 0 1 0 0	13.	0 2 0 2 0 0 1	23.	1 0 0 1 2 0 2
4.	1 0 2 2 1 0 0	14.	1 2 2 0 1 0 1	24.	0 2 2 1 2 1 2
5.	1 2 2 0 0 1 0	15.	2 0 1 2 1 0 1	25.	2 1 0 2 2 1 2
6.	2 0 1 2 0 1 0	16.	2 2 1 0 0 1 1	26.	1 1 0 0 0 2 2
7.	2 1 2 1 1 1 0	17.	1 0 2 2 0 1 1	27.	0 0 1 1 0 2 2
8.	0 2 0 2 1 1 0	18.	0 0 0 0 1 1 1	28.	2 2 0 1 1 2 2
9.	1 0 1 0 2 2 0	19.	1 1 1 1 1 1 1	29.	0 1 2 2 1 2 2
10.	0 1 0 1 2 2 0	20.	2 0 2 0 2 2 1		

Таблица 3: Единственото оптимално покритие при $n = 7$.

Директна проверка показва, че за всеки $\mathbf{x}, \mathbf{y} \in \mathcal{C}_7$, $\mathbf{x} \neq \mathbf{y}$ имаме $\mathbf{d}(\mathbf{x}, \mathbf{y}) \geq 3$.

3.5.1 Нееквивалентни покрития за $n = 8$

Ще намерим всички нееквивалентни оптимални покрития при $n = 8$.

Теорема 3.5.1. С точност до еквивалентност съществуват две оптимални покрития при $n = 8$.

Доказателство. Да разгледаме оптимално покритие C на $\mathbb{F}_3^8$, т.е. $|C| = 44$.

Без ограничение можем да приемем, че $c_1 = \min\{c_0, c_1, c_2\}$. Тъй като $c_0 + c_1 + c_2 = 44$ и $T(7) = 29$, намираме, че $c_i + c_j \geq 29$ за произволни i, j, $i \neq j$, $i, j \in \{0, 1, 2\}$. Следователно $c_1 = 14$ и $c_0 = c_2 = 15$.

Освен това $c_0 + c_1 = c_1 + c_2 = 29$, откъдето намираме, че $C_0 \cup C_1$ и $C_1 \cup C_2$ са еквивалентни на $\mathcal{C}_7$. Следователно всяко от множествата C_0, C_1 и C_2 е еквивалентно на подмножество на $\mathcal{C}_7$. Това означава, че за всяко $i \in \{0, 1, 2\}$ и всяко $1 \leq t \leq 8$ множеството C_i^t е еквивалентно на подмножество на $\mathcal{C}_7$.

Лема 3.5.2. Ако C е оптимално покритие на $\mathbb{F}_3^8$, то за всеки две кодови думи $\mathbf{u}, \mathbf{v} \in C$ е изпълнено $d(\mathbf{u}, \mathbf{v}) \geq 3$.

Доказателство. Да допуснем, че $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ и $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ са такива, че $\mathbf{u}, \mathbf{v} \in C$ и $d(\mathbf{u}, \mathbf{v}) < 3$. Без ограничение нека $u_n = v_n$, като тогава $\mathbf{d}((u_1, u_2, \ldots, u_{n-1}), (v_1, v_2, \ldots, v_{n-1})) < 3$. От направеното по-горе наблюдение векторите $(u_1, u_2, \ldots, u_{n-1})$ и $(v_1, v_2, \ldots, v_{n-1})$ могат да се разглеждат като елементи на $\mathcal{C}_7$. Но за всеки два елемента $\mathbf{x}, \mathbf{y} \in \mathcal{C}_7$ знаем, че $d(\mathbf{x}, \mathbf{y}) \geq 3$, което е противоречие. □

Без ограничение можем да считаме, че $C_1 \cup C_2 = \mathcal{C}_7$. Освен това знаем, че множеството $C_1 \cup C_0$ е еквивалентно на $\mathcal{C}_7$. Според Лема 3.5.2 имаме $C_0 \cap C_1 = \emptyset$ (в противен случай съществуват $\mathbf{u}$ и $\mathbf{v}$ от C, за които $d(\mathbf{u}, \mathbf{v}) = 1$), откъдето намираме $|(C_1 \cup C_0) \cap (C_1 \cup C_2)| = |C_1| = 14$. Следователно C_1 е сечение на две копия на $\mathcal{C}_7$.

Компютърно търсене проверява всяко от $7!.6^7$ копия на $\mathcal{C}_7$ и намира такива $\mathcal{C}_7'$, за които $|\mathcal{C}_7' \cap \mathcal{C}_7| = 14$. Тогава елементите на C_1 са точно 14-те елемента на $\mathcal{C}_7' \cap \mathcal{C}_7$, елементите на C_2 са $\mathcal{C}_7 \setminus C_1$ и елементите на C_0 са $\mathcal{C}_7' \setminus C_1$.

В резултат на търсенето намираме 384 множества с 44 елемента. За всяко такова множество проверяваме дали то е покритие (трябва да проверим само, че $C_0 \cup C_2$ е покритие на $\mathbb{F}_3^7$). Оказва се, че всички получени множества са покрития. Стандартна проверка за еквивалентност показва, че съществу-

ват само две нееквивалентни покрития. Двете покрития (означаваме ги с $\mathcal{C}_8^1$ и $\mathcal{C}_8^2$) са представени в Таблица 4 и Таблица 5.

1.	0 0 0 0 0 0 0 0 2
2.	1 1 1 1 0 0 0 1
3.	2 2 1 0 1 0 0 2
4.	1 0 2 2 1 0 0 2
5.	1 2 2 0 0 1 0 2
6.	2 0 1 2 0 1 0 2
7.	2 1 2 1 1 1 0 1
8.	0 2 0 2 1 1 0 2
9.	1 0 1 0 2 2 0 1
10.	0 1 0 1 2 2 0 2
11.	2 2 2 2 2 2 0 1
12.	2 1 2 1 0 0 1 2
13.	0 2 0 2 0 0 1 1
14.	1 2 2 0 1 0 1 1
15.	2 0 1 2 1 0 1 1

16.	2 2 1 0 0 1 1 1
17.	1 0 2 2 0 1 1 1
18.	0 0 0 0 1 1 1 1
19.	1 1 1 1 1 1 1 2
20.	2 0 2 0 2 2 1 2
21.	1 2 1 2 2 2 1 2
22.	0 1 1 0 2 0 2 1
23.	1 0 0 1 2 0 2 2
24.	0 2 2 1 2 1 2 2
25.	2 1 0 2 2 1 2 1
26.	1 1 0 0 0 2 2 2
27.	0 0 1 1 0 2 2 1
28.	2 2 0 1 1 2 2 1
29.	0 1 2 2 1 2 2 2
30.	1 0 2 0 0 0 2 0

31.	2 2 1 2 0 0 2 0
32.	0 0 0 2 1 0 2 0
33.	0 2 0 0 0 1 2 0
34.	2 0 1 0 1 1 2 0
35.	1 2 2 2 1 1 2 0
36.	1 1 2 1 2 2 2 0
37.	2 1 0 0 2 0 1 0
38.	0 1 1 2 2 1 1 0
39.	2 0 0 1 0 2 1 0
40.	0 2 1 1 1 2 1 0
41.	0 0 2 1 2 0 0 0
42.	1 2 0 1 2 1 0 0
43.	0 1 2 0 0 2 0 0
44.	1 1 0 2 1 2 0 0

Таблица 4: Оптимално покритие $\mathcal{C}_8^1$.

1.	0 0 0 0 0 0 0 2	16.	2 2 1 0 0 1 1 2	31.	1 2 1 2 0 0 2 0
2.	1 1 1 1 0 0 0 2	17.	1 0 2 2 0 1 1 2	32.	0 2 0 2 2 2 2 0
3.	2 2 1 0 1 0 0 1	18.	0 0 0 0 1 1 1 1	33.	2 1 2 1 2 2 2 0
4.	1 0 2 2 1 0 0 1	19.	1 1 1 1 1 1 1 1	34.	1 0 1 0 1 1 2 0
5.	1 2 2 0 0 1 0 1	20.	2 0 2 0 2 2 1 1	35.	2 2 2 2 1 1 2 0
6.	2 0 1 2 0 1 0 1	21.	1 2 1 2 2 2 1 1	36.	0 1 0 1 1 1 2 0
7.	2 1 2 1 1 1 0 2	22.	0 1 1 0 2 0 2 1	37.	1 1 0 0 2 0 1 0
8.	0 2 0 2 1 1 0 2	23.	1 0 0 1 2 0 2 1	38.	0 0 1 1 2 0 1 0
9.	1 0 1 0 2 2 0 2	24.	0 2 2 1 2 1 2 2	39.	0 1 1 0 0 2 1 0
10.	0 1 0 1 2 2 0 2	25.	2 1 0 2 2 1 2 2	40.	1 0 0 1 0 2 1 0
11.	2 2 2 2 2 2 0 2	26.	1 1 0 0 0 2 2 1	41.	2 1 0 2 1 2 0 0
12.	2 1 2 1 0 0 1 1	27.	0 0 1 1 0 2 2 1	42.	0 2 2 1 1 2 0 0
13.	0 2 0 2 0 0 1 1	28.	2 2 0 1 1 2 2 2	43.	0 1 2 2 2 1 0 0
14.	1 2 2 0 1 0 1 2	29.	0 1 2 2 1 2 2 2	44.	2 2 0 1 2 1 0 0
15.	2 0 1 2 1 0 1 2	30.	2 0 2 0 0 0 2 0		

Таблица 5: Оптимално покритие $\mathcal{C}_8^2$.

□

Директно се проверява, че двойките разстояния за двата кода са:

t	1	2	3	4	5	6	7	8
двойки от $\mathcal{C}_8^1$ на разстояние t	0	0	0	210	320	240	128	48
двойки от $\mathcal{C}_8^2$ на разстояние t	0	0	0	222	320	216	128	60

Да отбележим, че за всеки два елемента $\mathbf{x}, \mathbf{y}$ от $\mathcal{C}_8^i$, $i = 1, 2$ е в сила $d(\mathbf{x}, \mathbf{y}) \geq 4$.

3.5.2 Намиране на точната стойност на $T(9)$

Като използваме свойствата на намерените две покрития на $\mathbb{F}_3^8$ ще определим точната стойност на $T(9)$.

Теорема 3.5.2. Изпълнено е равенството $T(9) = 68$.

Доказателство. Да допуснем, че съществува покритие C на $\mathbb{F}_3^9$ с 67 думи. От $T(8) = 44$ следва, че $c_i^t + c_j^t \geq 44$ за всяко $t = 1, 2, \ldots, 9$ и произволни i, j, $i \neq j$, $i, j \in \{0, 1, 2\}$. Директно се проверява, че множеството $\{c_0^t, c_1^t, c_2^t\}$ съвпада с някое от множествата $\{21, 23, 23\}$ или $\{22, 22, 23\}$.

И в двата случая съществува *специален елемент* $i \in \{0, 1, 2\}$ за който $c_j^t + c_k^t = 44$ за $\{i, j, k\} = \{0, 1, 2\}$. Да отбележим, че в случая $\{21, 23, 23\}$ съществуват два специални елемента.

Без ограничение можем да допуснем, че $c_1^9 + c_2^9 = 44$. Следователно множеството $C_1^9 \cup C_2^9$ е еквивалентно на $\mathcal{C}_8^1$ или $\mathcal{C}_8^2$.

Лема 3.5.3. Нека $\mathbf{u} = (u_1, \ldots, u_8)$ и $\mathbf{v} = (v_1, \ldots, v_8)$ са елементи от $C_1^9 \cup C_2^9$, за които $d(\mathbf{u}, \mathbf{v}) = 4$. Ако съществува t, $1 \leq t \leq 8$, за което $u_t \neq v_t$ и $\{0, 1, 2\} \setminus \{u_t, v_t\}$ е специален елемент за координата t, то $\mathbf{u}$ и $\mathbf{v}$ не са едновременно елементи на C_i^9 за $i = 0, 1$.

Доказателство. Нека $\mathbf{u}$ и $\mathbf{v}$ са вектори, удовлетворяващи условието на лемата. Да означим разширенията на $\mathbf{u}$ и $\mathbf{v}$ в C без координата t с $\overline{\mathbf{u}}$ и $\overline{\mathbf{v}}$. Тъй като $\{0, 1, 2\} \setminus \{u_t, v_t\}$ е специален елемент за координата t, то $\overline{\mathbf{u}}$ и $\overline{\mathbf{v}}$ са елементи на $\mathcal{C}_8^1$ или $\mathcal{C}_8^2$.

Ако $\mathbf{u}, \mathbf{v} \in C_i^9$ за $i = 0$ или 1, то $\mathbf{d}(\overline{\mathbf{u}}, \overline{\mathbf{v}}) = 3$. Това е противоречие с $d(\mathbf{x}, \mathbf{y}) \geq 4$ за всеки $\mathbf{x}, \mathbf{y} \in \mathcal{C}_8^i$ за $i = 1$ или 2. □

Дефиниция 3.5.1. Векторът $(u_1, \ldots, u_8)$ се нарича *характеристичен* вектор за оптималното покритие C ако за всяко t, $1 \leq t \leq 8$ елементът u_t е специален елемент за координата t.

Да допуснем, че за даден характеристичен вектор съществуват три вектора $\mathbf{u}, \mathbf{v}, \mathbf{w}$ всеки два от които удовлетворяват условията на Лема 3.5.3. Тъй като поне два от тях са елементи на C_i^9 за фиксирано $i = 0$ или 1, получаваме противоречие с Лема 3.5.3.

С търсене с компютър проверяваме всички $3^8 = 6561$ характеристични вектори и за всеки един от тях търсим три елемента $\mathbf{u}, \mathbf{v}, \mathbf{w}$ от $\mathcal{C}_8^i$ за $i = 1$ или 2, всеки два от които удовлетворяват условията на Лема 3.5.3.

За втория код се оказва, че за всеки характеристичен вектор съществуват три вектора, удовлетворяващи условията на Лема 3.5.3. Следователно $C_1^9 \cup C_2^9$ не може да е еквивалентно на този код.

За първия код получаваме само четири възможности за характеристичен вектор:

$$(00021002); (02000102); (10221020); (12200120).$$

С помощта на Лема 3.5.3 лесно определяме как да разделим тези вектори в двете множества C_9^1 и C_9^2, т.е. как да разширим всеки от тези вектори с 1 или 2. За целта, без ограничение поставяме първия вектор $\mathbf{x} = (00000002)$ в множество C_9^1, след което намираме всички кодови думи $\mathbf{y}$, за които е изпълнено $d(\mathbf{x}, \mathbf{y}) \leq 3$. Ако $\mathbf{x}$ и $\mathbf{y}$ имат обща специална координата, то според Лема 3.5.3, векторът $\mathbf{y}$ трябва да бъде разширен с 2. Тази процедура може да бъде извършена с всеки вектор, който е разширен. По този начин получаваме 8 възможности за разширяване (по две за всеки характеристичен вектор).

В долната таблица са представени възможните разширения за кодовите думи на $\mathcal{C}_8^1$ (i-ят елемент на представения вектор с дължина 44 показва разширението на i-та кодова дума) за всеки от характеристичните вектори.

Характер. вектор	Разширения на кодовите думи
00021002	11122121221212112111222121112122221211222112
00021002	12122111122112112122112111222122221222112112
02000102	11122121221212112111211212221122221222111221
02000102	12122111122112112122121222111122221211221221
10221020	11222211222221111221122111122112211212212112
10221020	12222221121121111212212121211221122112212112
12200120	11222211222221111221111222211112211221121221
12200120	12222221121121111212222121212111221121221221

Остава да определим елементите на C_0^9, т.е. елементите на кода с последна координата 0. Ясно е, че ако $\mathbf{xi}$ за $i = 1, 2$ и $\mathbf{y0}$ са елементи на покритието, които имат общ специален елемент, то $d(\mathbf{x}, \mathbf{y}) \geq 3$. Следователно за да определим възможните опашки $\mathbf{y}$ с последна координата 0, трябва да намерим всички вектори $\mathbf{y}$ с дължина 8, имащи горното свойство. Директна проверка показва, че съществуват 178 такива вектори.

За всеки два елемента $\mathbf{x}$ и $\mathbf{y}$ от тези 177 вектора отново имаме, че ако те имат общ специален елемент, то $d(\mathbf{x}, \mathbf{y}) \geq 4$. С компютърно търсене намираме 360 възможни множества от 23 вектора (да припомним, че $c_9^0 = 23$) с последна координата 0. Оказва се, че нито едно от тях не дава покритие.

За 72 от тези множества е възможно, с добавянето на един вектор с последна коориданата 0, да получим покритие с 68 елемента. □

Получената в Теорема 3.5.2 стойност $T(9) = 68$ и неравенството от Лема 3.5.1 позволяват подобряване на известните граници за $T(n)$ при $10 \leq n \leq 13$. Получаваме

$$T(10) \geq 102, T(11) \geq 153, T(12) \geq 230, T(13) \geq 345.$$

Глава 4

Задачи за търсене

В тази глава са представени резултати, получени в [14], [15], [42], [43], [44], [45], [46], [47], [50], [53].

4.1 Постановка на основната задача за търсене

Общата постановка на класическата задача за търсене е следната: Дадено е множество A от което е избран неизвестен за нас елемент x. Можем да задаваме въпроси от вида: принадлежи ли елемента x на избрано от нас подмножество B на A. Отговорът на всеки от въпросите е „да“ или „не“. Целта е да намерим елемента x с възможно най-малко въпроси. Когато елемента x е намерен, казваме, че сме решили съответната задача за търсене.

За избор на множеството-въпрос B могат да бъдат наложени различни ограничения. Най-общо множеството B може да бъде избирано само от дадена фамилия $\mathcal{A}$ от подмножества на A. В зависимост от контекста на задачата множеството $\mathcal{A}$ се задава по различни начини. Възможно е ограниченията, наложени върху възможните въпроси, да правят съответната задача за търсене нерешима.

В зависимост от начина на задаване на въпросите са възможни следните видове търсене:

- **Адаптивно търсене.** Когато всеки въпрос се задава след като е получен отговора на предишния, говорим за адаптивно търсене. Тогава е възможно всеки следващ въпрос да използва получената от отговорите на предишните въпроси информация. По този начин използваната стратегия се адаптира към получените отговори.
- **Неадаптивно търсене.** Когато всички въпроси се задават едновременно, говорим за неадаптивно търсене.

В общия случай е ясно, че при една и съща задача за търсене при адаптивното търсене са необходими не по-голям брой въпроси в сравнение с неадаптивното търсене.

В замисимост от истинността на получаваните отговори са възможни следните видове търсене:

- Търсене, при което всички отговори са верни.
- Търсене, при което се допускат определен брой неверни отговори.
- Търсене, при което част от отговорите се „загубват“.

Ясно е, че когато се допускат и неверни отговори за намиране на неизвестния елемент са необходими повече въпроси. В такива случаи задачата се моделира в термините на теорията на кодирането. Това позволява да се използват свойствата на кодове, поправящи грешки.

Възможни са разновидности на основната задача за търсене. Например, когато се търсят два или повече елемента от A отговорите на въпросите могат да съдържат информация дали в B има поне един от търсените елементи или точно колко от търсените елементи се съдържат в B.

Следната лема дава долна граница за минималния брой въпроси за решаване на класическата задача за търсене.

Лема 4.1.1. За решаване на класическата задача за търсене са необходими поне $\lceil \log_2 |A| \rceil$ въпроса.

Доказателство. Да допуснем, че задачата може да бъде решена с k въпроса. Тъй като всички възможни последователности от отговори при задаване на k въпроса са 2^k и след всяка такава последователност от отговори трябва да определим неизвестния елемент, то $2^k \geq |A|$. Оттук следва търсеното неравенство $k \geq \lceil \log_2 |A| \rceil$. □

При решаване на задачи за търсене основен е въпроса дали решението на съответната задача се реализира с минималния брой въпроси.

4.2 Неадаптивно търсене на неизвестен елемент с множества с равни тегла

Разглеждаме произволно крайно множество A и функция $\mathrm{w} : A \to \mathbb{N}$, наречена *теглова функция* за множеството A. За произволно подмножество B на A дефинираме *тегло на подмножеството* B по следния начин:

$$\mathrm{w}(B) = \sum_{x \in B} \mathrm{w}(x).$$

За неизвестен елемент $x \in A$ и дадено естествено число S множествата-въпроси са онези подмножества B на A за които $\mathrm{w}(B) = S$. Ще наречем така описаната задача (A, w, S) задача за търсене. Естественото число S се нарича „добро “ ако съответната (A, w, S) задача е решима, т.е. неизвестния елемент x може да бъде намерен с неадаптивно търсене. Това означава, че съществува някакъв брой от множества-въпроси, с помощта на които се

намира x. За различни добри стойности на S броят на множествата-въпроси за намиране на x е различен. Естественото число S се нарича *подходящо*, ако неизвестния елемент x може да бъде намерен с минималния възможен брой въпроси.

Основната задача, която ще разгледаме е намирането на всички добри и подходящи числа при $A = \{1, 2, \ldots, 2^n\}$ и теглова функция от вида:

$$\mathrm{w}_h(i) = \left[\frac{i-1}{2^h}\right] + 1$$

за $h = 1, 2, \ldots, n$ където $[x]$ е цялата част на x.

За различни стойности на h получаваме различни теглови функции и съответно различни по трудност задачи за търсене.

1. При $h = n$, т.е. $\mathrm{w}(i) = 1$ за $i = 1, 2, \ldots, 2^n$ задачата е тривиална, като добри са всички числа S, $1 \leq S < 2^n$, а единственото подходящо число S е $S = 2^{n-1}$.

2. При $h = 0$, т.е. $\mathrm{w}(i) = i$ for $i = 1, 2, \ldots, 2^n$ получаваме задачата, разгледана и решена в Част 4.2.1.

3. При $h = n-1$ и $n = 2t+1$, т.е. $\mathrm{w}(i) = 1$ за $i = 1, 2, \ldots, 2^{n-1}$ и $\mathrm{w}(i) = 2$ за $i = 2^{n-1}+1, \ldots, 2^n$. В Част 4.2.2 ще докажем, че S е подходящо тогава и само тогава, когато

$$S \in \left[3.2^{n-2} - \binom{n-2}{t}, 3.2^{n-2} + \binom{n-2}{t}\right].$$

4. При $h = n-2$ имаме $\mathrm{wt}(i) = 1$ за $i = 1, 2, \ldots, 2^{n-2}$, $\mathrm{wt}(i) = 2$ за $i = 2^{n-2}+1, \ldots, 2^{n-1}$, $\mathrm{wt}(i) = 3$ за $i = 2^{n-1}+1, \ldots, 3.2^{n-2}$ и $\mathrm{wt}(i) = 4$ за $i = 3.2^{n-2}+1, \ldots, 2^n$. Основният резултат в този случай е получен в Част 4.2.3.

4.2.1 Неадаптивно търсене за теглова функция $\mathrm{w}(\mathbf{i}) = \mathbf{i}$

В тази част са представени резултати, получени в [43] и [42].

При теглова функция $w(i) = i$ разглежданата задача за търсене е следната. Дадени са множество $A = \{1, 2, 3, \ldots, 2^n\}$, естествено число S и неизвестен за нас елемент $x \in A$. Разрешено е да задаваме въпроси от вида: принадлежи ли елемента x на подмножество B на A при условие, че сборът от елементите на B е равен на S, т.е.

$$\sum_{i \in B} i = S.$$

Когато е изпълнено горното равенство, ще казваме, че множеството-въпрос B има тегло S.

На всеки от въпросите се отговаря с „да “ или „не “, като не се допускат грешни отговори. При това разглеждаме неадаптивно търсене, т.е. предполагаме, че всички въпроси се задават едновременно.

Да наречем така представената задача (n, S) задача за търсене.

От Лема 4.1.1 следва, че минималният брой въпроси за решаване на една (n, S) задача за търсене е $\log_2 2^n = n$. Следователно при фиксирано n възниква въпроса за определяне на всички естествени числа S, за които съответната (n, S) задача е решима и определяне на всички естествени числа S, за които съответната (n, S) задача е решима с минимален брой въпроси.

Едно естествено число S ще наричаме *добро* ако съществува множество от въпроси $B_1, B_2, \ldots, B_m$, всеки от които е с тегло S и което решава съответната (n, S) задача. Когато $m = n$, т.е. за решаване на задачата сме използвали минималния възможен брой въпроси, числото S се нарича *подходящо*.

Ще решим следните две задачи:

Задача А. Да се намерят всички добри числа S.

Задача Б. Да се намерят всички подходящи числа S.

Намиране на всички добри числа S

Теорема 4.2.1 дава необходимо и достатъчно условие едно естествено число S да бъде добро, като по този начин се решава поставената **Задача А**.

Теорема 4.2.1. Естественото число S е добро тогава и само тогава, когато

$$S \in [2^n - 1, 2^{2n-1} - 2^{n-1} + 1].$$

Доказателство. Да допуснем първо, че числото S е добро. Това означава, че за всеки два различни елемента a и b от A съществува множество B, със сбор на елементите S, за което $a \in B$ и $b \notin B$ или $a \notin B$ и $b \in B$. С други думи множеството B *разделя* a и b. Да означим с $B^S_{a,b}$ множество с тегло S, което разделя числата a и b. Ако $S < 2^n - 1$, то никой от елементите $a = 2^n - 1$ и $b = 2^n$ не може да бъде елемент на множество B с тегло S. Следователно не съществува множество с тегло S, което разделя a и b.

Сега да допуснем, че

$$S > 2^{2n-1} - 2^{n-1} + 1 = 2^{2n-1} + 2^{n-1} - (2^n - 1).$$

Тъй като $\sum_{i=1}^{2^n} i = 2^{2n-1} + 2^{n-1}$, то всяко множество B с тегло S ще съдържа елементите $a = 2^n - 1$ и $b = 2^n$. Следователно тези два елемента не могат да бъдат разделени. Получихме, че ако S подходящо, то

$$S \in [2^n - 1, 2^{2n-1} - 2^{n-1} + 1].$$

Да допуснем, че $S \in [2^n - 1, 2^{2n-1} - 2^{n-1} + 1]$. Ще докажем с индукция по S, че за всеки два елемента a и b от A съществува множество $B^S_{a,b}$.

1. Нека $S = 2^n - 1$ и $a, b \in A$, като $a < b$. Ясно е, че $a \leq S = 2^n - 1$. Ако $a = 2^n - 1$ избираме $B^S_{a,b} = \{2^n - 1\}$. Нека $a \neq 2^n - 1$. Ако $a + b \neq 2^n - 1$, т.е. $b \neq 2^n - 1 - a$ избираме $B^S_{a,b} = \{a, 2^n - 1 - a\}$. Когато $a + b = 2^n - 1$ и $a \leq 2$ избираме $B^S_{a,b} = \{1, 2, 2^n - 4\}$. Накрая, когато $a + b = 2^n - 1$ и $a > 2$ избираме $B^S_{a,b} = \{1, a - 1, b\}$.

2. Допускаме, че за някое $S \in [2^n - 1, 2^{2n-1} - 2^{n-1}]$ и за всеки два елемента $a, b \in A$, $a < b$ съществува разделящо множество $B^S_{a,b}$.

3. Ще намерим множество $B^{S+1}_{a,b}$. Използваме следното наблюдение. Ако $l \neq 2^n$, $l \in B^S_{a,b}$, $l + 1 \notin B^S_{a,b}$ и $\{l, l + 1\} \cap \{a, b\} = \emptyset$, то

$$B^{S+1}_{a,b} = B^S_{a,b} \backslash \{l\} \cup \{l + 1\}.$$

Освен това, ако $a \neq 1$ и $1 \notin B^S_{a,b}$, то $B^{S+1}_{a,b} = B^S_{a,b} \cup \{1\}$. От горните разсъждения следва, че ако $\{1, 2, \ldots, a - 1\} \not\subset B^S_{a,b}$, можем да намерим множество $B^{S+1}_{a,b}$. Остава да разгледаме случая $\{1, 2, \ldots, a - 1\} \subset B^S_{a,b}$

Първо да допуснем, че $a > 2$, $b \neq 2^n$ и $a + 1 \neq b$. Ако $a + 1 \notin B^S_{a,b}$ намираме

$$B^{S+1}_{a,b} = B^S_{a,b} \backslash \{1, a - 1\} \cup \{a + 1\}.$$

Ако $a+1 \in B^S_{a,b}$ и $\{a+2, a+3, \ldots, b-1\} \not\subset B^S_{a,b}$, то според направеното по-горе наблюдение можем да намерим $B^{S+1}_{a,b}$. Когато $\{a + 2, a + 3, \ldots, b - 1\} \subset B^S_{a,b}$, ако $b + 1 \notin B^S_{a,b}$ имаме $B^{S+1}_{a,b} = B^S_{a,b} \backslash \{1, b - 1\} \cup \{b + 1\}$. Ако $b + 1 \in B^S_{a,b}$ и $\{b + 2, \ldots, 2^n\} \not\subset B^S_{a,b}$ според направеното по-горе наблюдение можем да намерим $B^{S+1}_{a,b}$. Да допуснем, че $\{b+2, \ldots, 2^n\} \subset B^S_{a,b}$. Тогава $\{1, 2, \ldots, a - 1, a + 1, \ldots, b - 1, b + 1, \ldots, 2^n\} \subset B^S_{a,b}$. Понеже $B^S_{a,b}$ е разделящо множество за a и b, имаме $a \in B^S_{a,b}$ или $b \in B^S_{a,b}$. Тогава $S \geq 2^{2n-1} + 2^{n-1} - b$, което заедно с $b \neq 2^n$ е противоречие с $S \leq 2^{2n-1} - 2^{n-1}$.

Сега да допуснем, че $a > 2$, $b \neq 2^n$ и $a+1 = b$. Понеже $B^S_{a,b}$ е разделящо ма a и b, имаме два случая. Ако $a \in B^S_{a,b}$ и $b = a+1 \notin B^S_{a,b}$ намираме $B^{S+1}_{a,b} = B^S_{a,b} \backslash \{a\} \cup \{a+1\}$. Ако $a \notin B^S_{a,b}$ и $b = a+1 \in B^S_{a,b}$ и $a+2 \notin B^S_{a,b}$ намираме

$$B^{S+1}_{a,b} = B^S_{a,b} \backslash \{1, a-1, a+1\} \cup \{a, a+2\}.$$

Ако $a+2 \in B^S_{a,b}$ и $\{a+2, \ldots, 2^n\} \not\subset B^S_{a,b}$ намираме $B^{S+1}_{a,b}$ както по-горе, а когато $\{a+2, \ldots, 2^n\} \subset B^S_{a,b}$ получаваме противоречие с $S \leq 2^{2n-1} - 2^{n-1}$.

Остава да разгледаме случаите $a = 1$, $a = 2$ или $b = 2^n$. Във всеки от тях намирането на разделящо множество $B^S_{a,b}$ е тривиално.

С това индукцията е завършена. □

Намиране на всички подходящи числа S

Да припомним, че едно естествено число S се нарича *подходящо*, ако съществуват n подмножества $B_1, B_2, \ldots, B_n$ на множеството $A = \{1, 2, 3, \ldots, 2^n\}$, всяко от които с тегло S и с помощта на които се решава съответната (n, S) задачата.

Основният резултат, който ще докажем в тази част се дава от следната Теорема.

Теорема 4.2.2. а) Ако $n \neq 2^k$, то числото S е подходящо тогава и само тогава, когато

$$S \in \left[2^{2n-2} + 2^{n-2} - \frac{\binom{2n-1}{n-1}}{2}; 2^{2n-2} + 2^{n-2} + \frac{\binom{2n-1}{n-1}}{2} \right].$$

б) За $n = 2^k$, $k \geq 2$ числото S е подходящо тогава и само тогава, когато

$$S \in \left[2^{2n-2} + 2^{n-2} - \frac{1}{2}\left(\binom{2n-1}{n-1} - 1 \right); 2^{2n-2} + 2^{n-2} + \frac{1}{2}\left(\binom{2n-1}{n-1} - 1 \right) \right].$$

Ще разделим доказателството на Теорема 4.2.2 на 4 стъпки:

1. Намиране на необходимо условие едно число S да е подходящо за произволно n.

2. Доказване на Теорема 4.2.2 а) при n нечетно число.

3. Доказване на Теорема 4.2.2 а) при $n \neq 2^k$ четно число.

4. Доказване на Теорема 4.2.2 б).

Дефиниция 4.2.1. Векторът $V = (v_1, v_2, \ldots, v_{2^n})$ се нарича *характеристичен вектор* за подмножеството B на A, ако $v_i = 1$ когато $i \in B$ и $v_i = 0$ когато $i \notin B$. Тогава

$$\sum_{y \in B} y = \sum_{i=1}^{2^n} i v_i.$$

Дефиниция 4.2.2. Нека $B_1, B_2, \ldots, B_n$ е множество от подмножества на A. Матрицата G с размери $n \times 2^n$ и с редове характеристичните вектори на $B_1, B_2, \ldots, B_n$ се нарича *характеристична матрица* за даденото множество. *Тегло на характеристичната матрица* G със стълбове $V_1, V_2, \ldots, V_{2^n}$ се дефинира като

$$\mathrm{wt}(G) = \frac{1}{n} \sum_{i=1}^{2^n} i \mathrm{wt}(V_i).$$

Да разгледаме множество $B_1, B_2, \ldots, B_n$ от подмножества на A, всяко от които е с тегло S. Когато питаме дали x принадлежи на B_i за $i = 1, 2, \ldots, n$ получаваме като отговори редица от „да“ и „не “ с дължина n. За да можем да определим еднозначно неизвестния елемент x, на всеки елемент на A трябва да съответства единствена редица от „да“ и „не“. Да забележим още, че ако $x = i$, то отговорите са точно елементите на V_i (1 означава „да“ и 0 означава „не“).

Следователно неизвестният елемент може да бъде намерен само когато стълбовете на съответната характеристична матрица са всички двоични

вектори с дължина n. Това означава, че S е подходящо число, ако съществува $n \times 2^n$ матрица G със стълбове всички двоични вектори с дължина n и скаларното произведение на всеки ред на G с вектора $(1, 2, 3, \ldots, 2^n)$ равно на S. Ще наричаме матрица с горните свойства *подходяща*. Ясно е, че за подходяща матрица G имаме $\mathrm{wt}(G) = S$.

Да означим с $\overline{G}$ матрицата, получена от G чрез смяна на 0 и 1. Лесно се вижда, че $\overline{G}$ е също подходяща матрица с тегло $2^{2n-1} + 2^{n-1} - \mathrm{wt}(G)$.

За доказване на резултата от стъпка 1 ще използваме някои комбинаторни тъждества, представени в следната Лема.

Лема 4.2.1. За всяко естествено число n са изпълнени тъждествата:

$$\text{а)} \sum_{i=1}^{n} i\binom{n}{i}^2 = n\binom{2n-1}{n-1}; \quad \text{б)} \sum_{i=1}^{n} i\binom{n}{i} = n2^{n-1};$$

$$\text{с)} \sum_{i=2}^{n} \binom{n}{i} \sum_{j=1}^{i-1} j\binom{n}{j} = n\left(2^{2n-2} - \binom{2n-1}{n-1}\right).$$

Доказателството на тъждествата от Лема 4.2.1 се извършва със стандартни комбинаторни подходи.

Следната теорема дава необходимо условие едно число S да е подходящо.

Теорема 4.2.3. Ако естественото число S е добро, то

$$S \in \left[2^{2n-2} + 2^{n-2} - \frac{\binom{2n-1}{n-1}}{2}, 2^{2n-2} + 2^{n-2} + \frac{\binom{2n-1}{n-1}}{2}\right].$$

Доказателство. Нека S е подходящо число, а G е подходяща матрица с тегло S. Първо ще докажем, че $S \geq 2^{2n-2} + 2^{n-2} - \frac{\binom{2n-1}{n-1}}{2}$. Да номерираме стълбовете на матрицата G с $1, 2, 3, \ldots, 2^n$ и да означим с S_i, $i = 1, 2, 3, \ldots, 2^n$ сборът от номерата на стълбовете с тегло i.

Тогава имаме $nS = n\mathrm{wt}(G) = \sum_{i=0}^{n} iS_i$. Тъй като имаме $\binom{n}{i}$ стълбове с тегло i, намираме

$$S_n \geq 1, \quad S_n + S_{n-1} \geq 1 + 2 + \cdots + \left(\binom{n}{n} + \binom{n}{n-1}\right),$$

$$S_n + S_{n-1} + S_{n-2} \geq 1 + 2 + \cdots + \left(\binom{n}{n} + \binom{n}{n-1} + \binom{n}{n-2}\right)$$

и т.н. до

$$S_n + S_{n-1} + \cdots + S_1 \geq 1 + 2 + \cdots + \left(\binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{1}\right).$$

Събираме горните неравенства и получаваме

$$\begin{aligned}\sum_{i=0}^{n} iS_i \quad \geq \quad & 1 + \frac{\left(\binom{n}{n} + \binom{n}{n-1}\right)\left(\binom{n}{n} + \binom{n}{n-1} + 1\right)}{2} + \\ & + \frac{\left(\binom{n}{n} + \binom{n}{n-1} + \binom{n}{n-2}\right)\left(\binom{n}{n} + \binom{n}{n-1} + \binom{n}{n-2} + 1\right)}{2} + \\ & \cdots + \frac{\left(\binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{1}\right)\left(\binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{1} + 1\right)}{2}.\end{aligned}$$

След преобразувания получаваме, че горното неравенство е еквивалентно на

$$2n\mathrm{wt}(G) \geq \sum_{i=1}^{n} i\binom{n}{i}^2 + \sum_{i=1}^{n} i\binom{n}{i} + 2\sum_{i=2}^{n}\binom{n}{i}\sum_{j=1}^{i-1} j\binom{n}{j}.$$

Като използваме тъждествата от Лема 4.2.1, намираме

$$\mathrm{wt}(G) \geq 2^{2n-2} + 2^{n-2} - \frac{\binom{2n-1}{n-1}}{2}$$

и понеже $\mathrm{wt}(G) = S$ получаваме търсеното.

За доказване на неравенството $S \leq 2^{2n-2} + 2^{n-2} + \frac{\binom{2n-1}{n-1}}{2}$ използваме, че

$$\mathrm{wt}(G) = 2^{2n-1} + 2^{n-1} - \mathrm{wt}(\overline{G}).$$

Понеже $\overline{G}$ също е добра матрица, то $\mathrm{wt}(\overline{G}) \geq 2^{2n-2} + 2^{n-2} - \frac{\binom{2n-1}{n-1}}{2}$, откъдето намираме

$$\mathrm{wt}(G) \leq 2^{2n-2} + 2^{n-2} + \frac{\binom{2n-1}{n-1}}{2}.$$

С това теоремата е доказана. □

Да отбележим и следното свойство на биномния коефициент $\binom{2n-1}{n-1}$.

Лема 4.2.2. Числото $\frac{\binom{2n-1}{n-1}}{2}$ е цяло, тогава и само тогава, когато n не е степен на двойката.

Доказателството на Лема 4.2.2 се извършва с помощта на известната теорема на Люка.

Ще въведем понятия и означения, необходими за по-нататъшното изложение. За всеки двоичен вектор-стълб $V = (v_1, v_2, \ldots, v_n)^t$ с дължина n означаваме с π циклично преместване на елементите на V на една позиция, т.е.

$$\pi(V) = (v_2, v_3, \ldots, v_n, v_1)^t.$$

Известно е, че π разделя множеството на всички двоични вектори с дължина n на орбити и дължината на всяка орбита е делител на n. Освен това елементите в една и съща орбита имат равни тегла. Нека дължината на орбитата, съдържаща вектора V с тегло $\mathrm{wt}(V) = w$ е равна на l. С $C_{w,l}$ ще означаваме матрицата, със стълбове съответно равни на $V, \pi(V), \pi^2(V), \ldots, \pi^{l-1}(V)$. Такава матрица ще наричаме *орбитна матрица с тегло w и дължина l*. Известно е, че n дели lw и във всеки ред на $C_{w,l}$ има точно $\frac{lw}{n}$ единици. Да отбележим, че $\overline{C_{w,l}}$ е орбитна матрица с тегло $n - w$.

Ще докажем твърдението от Теорема 4.2.2 а) при n нечетно число. Нека $n = 2k + 1$ е нечетно число. За доказване на основния резултат ще са необходими няколко леми.

Лема 4.2.3. Матрицата $G = C_1C_2 \dots C_m$, където $C_1, C_2, \dots, C_m$ е пермутация на всички орбитни матрици с тегла $n, n-1, \dots, k+1$ и техните допълнителни е подходяща.

Доказателство. Достатъчно е да докажем, че матриците $C_{w,l}$ и $\overline{C_{w,l}}$ за $k+1 \leq w \leq n$ имат еданкъв принос към скаларното произведение на всеки ред с вектора $(1, 2, \dots, 2^n)$. Нека първите стълбове на $C_{w,l}$ и $\overline{C_{w,l}}$ са съответно на позиции p и q. Като използваме, че $C_{w,l}$ и $\overline{C_{w,l}}$ са допълнителни, намираме, че скаларното произведение на всеки ред с $(1, 2, \dots, 2^n)$ е равен на

$$p + (p+1) + \dots + (p+l-1) + (q-p)\frac{l(n-w)}{n} = \frac{l(l-1)}{2} + ql - (q-p)\frac{lw}{n}.$$

С това доказателстовото е завършено. □

Пример 4.2.1. Нека $n = 3$. Съществуват четири орбитни матрици:

$$C_{3,1} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad C_{2,3} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \overline{C_{2,3}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \overline{C_{3,1}} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Интервалът от Теорема 4.2.3 е $[13, 23]$. Оказва се, че за всяко $S \in [13, 23]$ съществува подходяща матрица G с тегло S, която е образувана от пермутация на $C_{3,1}, C_{2,3}, \overline{C_{2,3}}$ и $\overline{C_{3,1}}$. Наистина, ако G_S е подходяща матрица с тегло S, то

$$G_{13} = (C_{3,1}C_{2,3}\overline{C_{2,3}C_{3,1}}) = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$G_{14} = (C_{3,1}C_{2,3}\overline{C_{3,1}C_{2,3}}) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{15} = (C_{2,3}C_{3,1}\overline{C_{3,1}C_{2,3}}) = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{16} = (C_{2,3}\overline{C_{3,1}}C_{3,1}\overline{C_{2,3}}) = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{17} = (\overline{C_{3,1}}C_{3,1}C_{2,3}\overline{C_{2,3}}) = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{18} = (C_{3,1}\overline{C_{2,3}C_{3,1}}C_{2,3}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

$$G_{19} = \overline{G_{17}}, \quad G_{20} = \overline{G_{16}}, \quad G_{21} = \overline{G_{15}}, \quad G_{22} = \overline{G_{14}}, \quad G_{23} = \overline{G_{13}}.$$

Нека H_1 е подматрица на G, съставена от няколко последователни стълба на G. Ако H_2 е матрица с размерите на H_1 означаваме с $G(H_1 \to H_2)$ матрицата, получена от G чрез заместване на H_1 с H_2. Следващите няколко леми показват как от дадена подходяща матрица с помощта на трансформация от вида $H_1 \to H_2$ могат да се получат нови добри матрици.

Лема 4.2.4. Нека G е подходяща матрица и $C_{p,t}$, $C_{q,h}$ са съседни орбитни матрици в G. Тогава $G_1 = G(C_{p,t}C_{q,h} \to C_{q,h}C_{p,t})$ е подходяща матрица с тегло $\mathrm{wt}(G_1) = \mathrm{wt}(G) + \dfrac{th(p-q)}{n}$.

Доказателство. От Лема 4.2.3 имаме, че матрицата

$$G_1 = G(C_{p,t}C_{q,h} \to C_{q,h}C_{p,t})$$

е подходяща. Знаем, че в $C_{p,t}$ и $C_{q,h}$ има съответно tp и hq единици. Тъй като трансформацията $C_{p,t}C_{q,h} \to C_{q,h}C_{p,t}$ е еквивалентна на преместване напред

на $C_{p,t}$ с h позиции и преместване назад на $C_{q,h}$ с t позиции, намираме, че $n.\mathrm{wt}(G_1) = n.\mathrm{wt}(G) + tph - hqt$, откъдето следва $\mathrm{wt}(G_1) = \mathrm{wt}(G) + \dfrac{th(p-q)}{n}$. $\square$

Лема 4.2.5. Нека V е вектор-стълб с тегло w, $k+1 \leq w \leq 2k+1$ и нека

$$C_{w,l} = \left(V\pi(V)\pi^2(V)\dots\pi^{l-1}(V)\right)$$

е орбитна матрица с тегло w и дължина l. Да означим

$$T_{w,n-w} = \left(V\overline{V}\pi\left(V\right)\pi\left(\overline{V}\right)\dots\pi^{l-1}\left(V\right)\pi^{l-1}\left(\overline{V}\right)\right)$$

и $T_{n-w,w} = \overline{T_{w,n-w}}$.

а) Ако G е подходяща матрица, за която $C_{w,l}$ и $\overline{C_{w,l}}$ са съседни матрици, то матрицата $G_1 = G\left(C_{w,l}\overline{C_{w,l}} \to T_{w,n-w}\right)$ е подходяща и

$$\mathrm{wt}(G_1) = \mathrm{wt}(G) + (2w-n)\frac{l(l-1)}{2n};$$

б) Ако $T_{w,n-w}$ е подматрица на подходяща матрица G, то матрицата $G_2 = G\left(T_{w,n-w} \to T_{n-w,w}\right)$ е подходяща и $\mathrm{wt}(G_2) = \mathrm{wt}(G) + (2w-n)\dfrac{l}{n}$.

Доказателство. а) Ако първият стълб на на $C_{w,l}$ е на позиция p, то първият стълб на $\overline{C_{w,l}}$ е на позиция $p+l$. От Лема 4.2.3 намираме, че приносът на $C_{w,l}$ и $\overline{C_{w,l}}$ към скаларното произведение на всеки ред с $(1,2,\dots,2^n)$ е равен на $X = l\left(\dfrac{(l-1)}{2} + p + l - \dfrac{lw}{n}\right)$.

Освен това във всеки ред на $C_{w,l}$ има $\dfrac{lw}{n}$ единици и във всекиред на $\overline{C_{w,l}}$ има $\dfrac{l(n-w)}{n}$ единици. Следователно, ако $(v_1, v_2, \dots, v_{2l})$ е ред в $T_{w,n-w}$, то имаме $\dfrac{lw}{n}$ двойки от вида $v_{2m+1}v_{2m+2} = 10$ и $\dfrac{l(n-w)}{n}$ двойки от вида $v_{2m+1}v_{2m+2} = 01$. Това означава, че скаларното произведение на всеки ред на $T_{w,n-w}$ с $(p, p+1, \dots, p+2l-1)$ е равно на

$$Y = p + p + 2 + p + 4 + \dots + p + 2l - 2 + \frac{l(n-w)}{n} = pl + l(l-1) + \frac{l(n-w)}{n}.$$

Следователно G_1 е подходяща и тъй като $Y - X = (2w-n)\frac{l(l-1)}{2n}$ получаваме търсеното.

б) Заместваме $n-w$ с w в израза за Y в а) и получаваме, че скаларното произведение на всеки ред на $T_{n-w,w}$ с $(p, p+1, \ldots, p+2l-1)$ е равно на

$$Z = p + p + 2 + p + 4 + \cdots + p + 2l - 2 + \frac{l(n-w)}{n} = pl + l(l-1) + \frac{lw}{n}.$$

Тъй като $Z - Y = (2w-n)\frac{l}{n}$ получаваме търсеното. □

Доказателствата на следващите две леми са аналогични на доказателствата на Лема 4.2.4 и Лема 4.2.5.

Лема 4.2.6. Нека G е подходяща матрица. Ако V е вектор стълб за който $V\overline{V}$ е подматрица на G, то $G\left(V\overline{VC_{w,l}} \to \overline{C_{w,l}}V\overline{V}\right)$ е подходяща матрица с тегло $\mathrm{wt}(G) + (2w-n)\dfrac{l}{n}$.

Лема 4.2.7. Нека G е походяща матрица и V е вектор стълб. Да означим с $C_{n,1}$ вектор стълба с тегло n. Тогава:

а) $G\left(V\overline{V\,C_{n,1}} \to \overline{C_{n,1}}V\overline{V}\right)$ е подходяща матрица с тегло $\mathrm{wt}(G)+1$;

б) $G\left(C_{n,1}V\overline{V} \to V\overline{V}\,C_{n,1}\right)$ е подходяща матрица с тегло $\mathrm{wt}(G)+1$;

в) $G\left(C_{n,1}\overline{C_{n,1}} \to \overline{C_{n,1}}C_{n,1}\right)$ е подходяща матрица с тегло $\mathrm{wt}(G)+1$.

Дефиниция 4.2.3. За подходяща матрица G с тегло S трансформацията $H_1 \to H_2$ се нарича *допустима* за G ако:

1. матрицата $G_1 = G(H_1 \to H_2)$ е подходяща и

2. ако $\mathrm{wt}(G_1) = \mathrm{wt}(G) + m$, то за всяко w, $\mathrm{wt}(G)+1 \le w \le \mathrm{wt}(G)+m-1$ съществува подходяща матрица с тегло w.

Ясно е, че ако съществува последователност от допустими трансформации, които преобразуват матрица G_1 в матрица G_2, то за всяко S, за което $\mathrm{wt}(G_1) \le S \le \mathrm{wt}(G_2)$ съществува подходяща матрица с тегло S.

Ако G и $G_1 = G(H_1 \to H_2)$ са подходящи матрици и $w = \mathrm{wt}(G_1) - \mathrm{wt}(G)$ записваме $\mathrm{wt}^+(H_1 \to H_2) = w$.

Пример 4.2.2. Нека $n = 7$. Тогава интервалът от Теорема 4.2.3 е $[2412, 5844]$. Ще докажем, че за всяко $S \in [2412, 5844]$ съществува подходяща матрица с тегло S.

Тъй като 7 е просто число всички орбитни матрици с тегло w, $1 \leq w \leq 6$ са с дължина 7. Да означим с s_w броят на орбитните матрици с тегло w. Тогава $s_7 = 1$, $s_6 = 1$, $s_5 = 3$, $s_4 = 5$, $s_3 = 5$, $s_2 = 3$, $s_1 = 1$ и $s_0 = 1$. Да означим с $C^t_{w,7}$ за $w = 6, 5$ или 4 и $t = 1, 2, \ldots, s_w$ всички орбитни матрици с тегло w. Нека $C_{7,1}$ е единствената орбитна матрица с тегло 7 и за опростяване приемаме, че $C_{6,7} = C^1_{6,7}$. Да разгледаме матрицата G_1, зададена с

$$C_{7,1}C_{6,7}C^1_{5,7}C^2_{5,7}C^3_{5,7}C^1_{4,7}C^2_{4,7}C^3_{4,7}C^4_{4,7}C^5_{4,7}\overline{C^5_{4,7}C^4_{4,7}C^3_{4,7}C^2_{4,7}C^1_{4,7}C^3_{5,7}C^2_{5,7}C^1_{5,7}C_{6,7}C_{7,1}}$$

От Лема 4.2.3 следва, че матрицата G_1 е подходяща. От доказателството на теорема 4.2.3 получаваме, че G_1 е от минималното възможно тегло, т.е. $\mathrm{wt}(G_1) = 2412$. Да забележим, че $\overline{G_1}$ е с тегло 5844. Ще докажем, че съществува последователност от допустими трансформации, които преобразуват G_1 в $\overline{G_1}$.

От Лема 4.2.4 получаваме

$$\mathrm{wt}^+\left(\overline{C_{6,7}C_{7,1}} \to \overline{C_{7,1}C_{6,7}}\right) = \mathrm{wt}^+\left(C_{7,1}C_{6,7} \to C_{6,7}C_{7,1}\right) = 1$$

и $\mathrm{wt}^+\left(C_{7,1}C^t_{5,7} \to C^t_{5,7}C_{7,1}\right) = 2$ за $t = 1, 2$ или 3. Следователно можем да получим подходяща матрица с тегло $\mathrm{wt}(G_1)+t$ за $t = 1, 2, \ldots, 7$. Това означава, че трансформацията $C^5_{4,7}\overline{C^5_{4,7}} \to T^5_{43}$ (според Лема 4.2.5 $\mathrm{wt}^+\left(C^5_{4,7}\overline{C^5_{4,7}} \to T^5_{43}\right) = 3$) е допустма за G_1. Намираме

$$G_2 = C_{7,1}C_{6,7}C^1_{5,7}C^2_{5,7}C^3_{5,7}C^1_{4,7}C^2_{4,7}C^3_{4,7}C^4_{4,7}T^5_{43}\overline{C^4_{4,7}C^3_{4,7}C^2_{4,7}C^1_{4,7}C^3_{5,7}C^2_{5,7}C^1_{5,7}C_{6,7}C_{7,1}}.$$

Матрицата T^5_{43} се състои от седем двойки от вида $V\overline{V}$, където $\mathrm{wt}(V) = 4$. От лема 4.2.6 получаваме $\mathrm{wt}^+\left(V\overline{VC^t_{w,7}} \to \overline{C^t_{w,7}}V\overline{V}\right) = 2w - 7$ за $w = 4, 5, 6$

и $t = 1, \ldots, s_w$. Тъй като $2w - 7 < 7$ и $\mathrm{wt}^+\left(V\overline{VC_{7,1}} \to \overline{C_{7,1}}V\overline{V}\right) = 1$ намираме, че трансформацията $V\overline{VC^t_{w,7}} \to \overline{C^t_{w,7}}V\overline{V}$ е допустима за всяка матрица съдържаща $C_{7,1}C_{6,7}C^1_{5,7}C^2_{5,7}C^3_{5,7}$ и $\overline{C_{6,7}C_{7,1}}$ (или $V\overline{VC_{7,1}}$ вместо $\overline{C_{6,7}C_{7,1}}$).

Следователно премествайки една по една всички двойки $V\overline{V}$ от T^5_{43} на дясно прескачайки една по една матриците $\overline{C^4_{4,7}}$, $\overline{C^3_{4,7}}$, $\overline{C^2_{4,7}}$, $\overline{C^1_{4,7}}$,$\overline{C^3_{5,7}}$, $\overline{C^2_{5,7}}$, $\overline{C^1_{5,7}}$ и $\overline{C_{6,7}}$ намираме

$$G_3 = C_{7,1}C_{6,7}C^1_{5,7}C^2_{5,7}C^3_{5,7}C^1_{4,7}C^2_{4,7}C^3_{4,7}C^4_{4,7}\overline{C^4_{4,7}C^3_{4,7}C^2_{4,7}C^1_{4,7}C^3_{5,7}C^2_{5,7}C^1_{5,7}C_{6,7}}T^5_{43}\overline{C_{7,1}}.$$

Повтаряйки горната операция последователно с $C^t_{4,7}\overline{C^t_{4,7}}$ за $t = 4, 3, 2$ и 1 ще получим

$$G_4 = C_{7,1}C_{6,7}C^1_{5,7}C^2_{5,7}C^3_{5,7}\overline{C^3_{5,7}C^2_{5,7}C^1_{5,7}C_{6,7}}T^1_{43}T^2_{43}T^3_{43}T^4_{43}T^5_{43}\overline{C_{7,1}}$$

чрез последователност от допустими трансформации. Използвайки двойките от вида $V\overline{V}$ от петте матрици T^t_{43} (имаме 35 такива матрици) и $\overline{C_{7,1}}$ можем да получим подходяща матрица с тегло $\mathrm{wt}(G_4) + t$ за всяко $t \in [1, 35]$. Следователно трансформацията $C^3_{5,7}\overline{C^3_{5,7}} \to T^3_{52}$ (според лема 4.2.5 $\mathrm{wt}^+\left(C^3_{5,7}\overline{C^3_{5,7}} \to T^3_{52}\right) = 9$) е допустима за G_4. След това преместваме една по една всички двойки $V\overline{V}$ от T^3_{52} на дясно като прескачаме една по една матриците $\overline{C^2_{5,7}C^1_{5,7}}$ и $\overline{C_{6,7}}$ (лесно се проверява, че всички трансформации са допестими) намираме

$$G_5 = C_{7,1}C_{6,7}C^1_{5,7}C^2_{5,7}\overline{C^2_{5,7}C^1_{5,7}C_{6,7}}T^3_{52}T^1_{43}T^2_{43}T^3_{43}T^4_{43}T^5_{43}\overline{C_{7,1}}.$$

Повтаряме горните операции с $C^t_{5,7}\overline{C^t_{5,7}}$ за $t = 2, 1$ и $C_{6,7}\overline{C_{6,7}}$ и получаваме

$$G_6 = C_{7,1}T_{61}T^1_{52}T^2_{52}T^3_{52}T^1_{43}T^2_{43}T^3_{43}T^4_{43}T^5_{43}\overline{C_{7,1}}$$

Да припомним, че

$$\begin{aligned}\mathrm{wt}^+\left(V\overline{VC_{7,1}} \to \overline{C_{7,1}}V\overline{V}\right) &= \mathrm{wt}^+\left(C_{7,1}V\overline{V} \to V\overline{V}C_{7,1}\right) = \\ &= \mathrm{wt}^+\left(C_{7,1}\overline{C_{7,1}} \to \overline{C_{7,1}}C_{7,1}\right) = 1.\end{aligned}$$

Тъй като имаме $2^6 - 1$ двойки от допълнителни вектор стълбове $V\overline{V}$, следва, че всяка трансформация на матрица от вида $C_{7,1}V_1\overline{V_1}\dots V_{2^6-1}\overline{V_{2^6-1}C_{7,1}}$ увеличаваща теглото с най-много $2^7 - 2$ е допустима трансформация за тази матрица.

От Лема 4.2.5 имаме $\mathrm{wt}^+\left(T^t_{w,7-w} \to T^t_{7-w,w}\right) = 2w - 7$ for $w = 6, 5$ or 4 (да отбележим, че всяка от матриците $T^t_{w,7-w}$ и $T^t_{7-w,w}$ са образувани от седем двойки от вида $V\overline{V}$) и следователно е допустима за всяка матрица от горния вид. Така намираме

$$G_7 = \overline{C_{7,1}T_{16}T^1_{25}T^2_{25}T^3_{25}T^1_{34}T^2_{34}T^3_{34}T^4_{34}T^5_{34}}C_{7,1}$$

Да забележим, че $G_7 = \overline{G_6}$. Тъй като за всяко S, за което $\mathrm{wt}(G_1) \le S \le \mathrm{wt}(G_6)$ съществува подходяща матрица с тегло S, ясно е, че за всяко S, $\mathrm{wt}(\overline{G_1}) \ge S \ge \mathrm{wt}(\overline{G_6})$ съществува подходяща матрица с тегло S. И така, доказахме, че за всяко $S \in [2412, 5844]$ съществува подходяща матрица с тегло S.

Следвайки стъпките от горния пример, ще докажем следната теорема.

Теорема 4.2.4. Ако $n = 2k + 1$ е нечетно число, и

$$S \in \left[2^{2n-2} + 2^{n-2} - \frac{\binom{2n-1}{n-1}}{2}; 2^{2n-2} + 2^{n-2} + \frac{\binom{2n-1}{n-1}}{2}\right],$$

то S е подходящо.

Доказателство. Тъй като

$$\gcd(2k+1, k) = \gcd(2k+1, k+1) = \gcd(2k+1, 2) = 1$$

всички орбитни матрици с тегло $k+1$, k и 2 са с дължина $n = 2k+1$. Освен това има само една орбитна матрица за всяко $w = n, n-1, 1, 0$ и k орбитни матрици за $w = n-2$ и $w = 2$. Означаваме с $C_{n,1}$ единствената орбитна матрица с тегло n и за опростяване нека $C_{n-1,n} = C^1_{n-1,n}$.

Да разгледаме матрицата, получена от наредба на всички орбитни матрици с нарастващо тегло:

$$G_1 = C_{n,1}C_{n-1,n}C^1_{n-2,n}\dots C^k_{n-2,n}\dots C^k_{k+1,n}\overline{C^k_{k+1,n}}\dots\overline{C^k_{n-2,n}}\dots\overline{C^1_{n-2,n}C_{n-1,n}C_{n,1}}.$$

Според Лема 4.2.3 матрицата G_1 е подходяща, а според Теорема 4.2.3 тази матрица е с минимално тегло. От Лема 4.2.4 имаме

$$\mathrm{wt}^+\left(C_{n,1}C_{n-1,n}\to C_{n-1,n}C_{n,1}\right) = \mathrm{wt}^+\left(\overline{C_{n-1,n}C_{n,1}}\to\overline{C_{n,1}C_{n-1,n}}\right) = 1$$

и $\mathrm{wt}^+\left(C_{n,1}C^t_{n-2,n}\to C^t_{n-2,n}C_{n,1}\right) = 2$ за $t = 1,2,\dots,k$. Лесно се вижда, че чрез трансформации от горния вид може да се получи подходяща матрица с тегло $\mathrm{wt}(G_1)+w$ за всяко $w = 1,2,\dots,2k+2$. Да отбележим, че според Лема 4.2.7 имаме $\mathrm{wt}^+\left(V\overline{VC_{n,1}}\to\overline{C_{n,1}}V\overline{V}\right) = 1$.

От горното следва, че ако една матрица съдържа като подматрици $C_{n,1}C_{n-1,n}C^1_{n-2,n}\dots C^k_{n-2,n}$ и $\overline{C_{n-1,n}C_{n,1}}$ (или $V\overline{VC_{n,1}}$ вместо $\overline{C_{n-1,n}C_{n,1}}$), то всяка трансформация $H_1\to H_2$, за която $\mathrm{wt}^+(H_1\to H_2)\le 2k+3$ е допустима за тази матрица.

Ще използваме следната последователност от стъпки:

1. Прилагаме трансформация от вида $C^k_{k+1,n}\overline{C^k_{k+1,n}}\to T^k_{k+1,k}$. Тази трансформация е допустима за G_1 и според Лема 4.2.5 е изпълнено равенството $\mathrm{wt}^+\left(C^k_{k+1,n}\overline{C^k_{k+1,n}}\to T^k_{k+1,k}\right) = k$.

2. Преместваме една по една всички двойки от допълнителни стълбове на $T^k_{k+1,k}$ като прескачаме една по една матриците $\overline{C^t_{w,l}}$ за $k+1\le w\le n$ в ляво от $\overline{C_n}$. От Лема 4.2.6 имаме, че $\mathrm{wt}^+\left(V\overline{VC^t_{w,l}}\to\overline{C^t_{w,l}}V\overline{V}\right) = (2w-n)\frac{l}{n}$. Понеже $l\le n$ и $w\le n$ имаме $(2w-n)\frac{l}{n}\le n$, което означава, че всички такива трансформации са допустими. Получаваме матрицата

$$G_2 = C_{n,1}C_{n-1,n}C^1_{n-2,n}\dots C^{k-1}_{k+1,n}\dots\overline{C^{k-1}_{k+1,n}}\dots\overline{C^1_{n-2,n}C_{n-1,n}}T^k_{k+1,k}\overline{C_{n,1}}$$

3. Повтаряме стъпки 1. и 2. за всички двойки $C^t_{k+1,n}\overline{C^t_{k+1,n}}$ за $t = k-1$, $k-2,\dots,1$. Означаваме получената матрица с G_3.

$$G_3 = C_{n,1}C_{n-1,n}C^1_{n-2,n}\dots C^t_{k+2,l}\overline{C^t_{k+2,l}}\dots\overline{C^1_{n-2,n}C_{n-1,n}}T^1_{k+1,k}\dots T^k_{k+1,k}\overline{C_{n,1}}.$$

Тъй като имаме $\binom{2k+1}{k}$ двойки от допълнителни вектор стълбове в $T^1_{k+1,k}T^2_{k+1,k}\dots T^k_{k+1,k}$ и $\mathrm{wt}^+\left(V\overline{V}\,\overline{C_{n,1}} \to \overline{C_{n,1}}V\overline{V}\right) = 1$, то всички трансформации за матрица съдържаща $T^1_{k+1,k}T^2_{k+1,k}\dots T^k_{k+1,k}\overline{C_{n,1}}$ и увеличаваща теглото с най-много $\binom{2k+1}{k}+1$ са допустими за тази матрица.

4. Прилагаме 1., 2. и 3. за средните две матрици $C^t_{w,l}\overline{C^t_{w,l}}$. Тези две матрици са допълнителни една на друга. Лесно се проверява, че трансформацията $C^t_{w,l}\overline{C^t_{w,l}} \to T^t_{w,n-w}$ е допустима. Също така преместването на една по една на всички двойки допълнителни стълбове на $T_{w,n-w}$ от ляво на $T_{w-1,n-w+1}$ са допустими трансформации.

5. Накрая получаваме матрицата

$$G_4 = C_{n,1}T_{n-1,1}T^1_{n-2,2}\dots T^k_{n-2,2}\dots T^1_{k+1,k}\dots T^k_{k+1,k}\overline{C_{n,1}}.$$

Да припомним, че $\mathrm{wt}^+\left(V\overline{VC_{n,1}} \to \overline{C_{n,1}}V\overline{V}\right) = \mathrm{wt}^+\left(C_{n,1}V\overline{V} \to V\overline{V}C_{n,1}\right) = 1$ и $\mathrm{wt}^+\left(C_{n,1}\overline{C_{n,1}} \to \overline{C_{n,1}}C_{n,1}\right) = 1$. Тъй като имаме $2^{n-1}-1$ двойки $V\overline{V}$, $\mathrm{wt}(V) \neq n$ от допълнителни вектор стълбове, то всяка трансформация на матрица от вида $C_{n,1}V_1\overline{V_1}\dots V_{2^{n-1}-1}\overline{V_{2^{n-1}-1}C_{n,1}}$, увеличаваща теглото с най-много 2^n е допустима за тази матрица.

От $\mathrm{wt}^+\left(T^t_{w,n-w} \to T^t_{n-w,w}\right) = (2w-n)\frac{l}{n} < 2^n$, където l е дължината на $C^t_{w,l}$, следва, че $T_{w,n-w} \to T_{n-w,w}$ е допустима трансформация. Намираме

$$G_5 = \overline{C_{n,1}}T_{1,n-1}T^1_{2,n-2}\dots T^k_{2,n-2}\dots T^1_{k,k+1}\dots T^k_{k,k+1}C_{n,1}.$$

Да забележим, че $G_5 = \overline{G_4}$. Понеже за всяко S, $\mathrm{wt}(G_1) \leq S \leq \mathrm{wt}(G_4)$ съществува подходяща матрица с тегло S, то за всяко S, за което $\mathrm{wt}\left(\overline{G_1}\right) \geq S \geq \mathrm{wt}\left(\overline{G_4}\right)$ съществува подходяща матрица с тегло S. С това доказателството е завършено. □

Нека сега n е четно число, но не е степен на двойката.

В този случай матриците C_k и $\overline{C_k}$ не винаги добавят една и съща стойност към скаларното произведение на всеки ред с $(1, 2, \ldots, 2^n)$. Един пример е $C_k = (1, 0, 1, 0 \ldots 1, 0)^t$, имаща k единици и k нули.

Лема 4.2.8. Нека $n = 2k$, като n не е степен на двойката. Съществува $2k \times \binom{2k}{k}$ матрица G от вида $V_1\overline{V_1}\,V_2\overline{V_2}\,\ldots V_t\overline{V_t}$ за $t = 2^{\binom{2k}{k}/2}$, всички стълбове на която са вектори с тегло k и скаларното произведение на всеки ред на G с $\left(1, 2, \ldots, \binom{2k}{k}\right)$ е равно на $\dfrac{\binom{2k}{k}\left(\binom{2k}{k}+1\right)}{4}$.

Доказателство. Съществуват $\binom{2k-1}{k}$ вектор стълба с тегло k, имащи 0 в последната позиция. Тъй като $\binom{2k-1}{k} = \frac{1}{2}\binom{2k}{k}$ и $\binom{2k-1}{k}$ е четно число, тогава и само тогава, когато n не е степен на двойката, можем да разположим тези вектори на позиции $1, 3, 5, \ldots, \binom{2k-1}{k} - 1, \binom{2k-1}{k} + 2, \binom{2k-1}{k} + 4, \ldots, \binom{2k}{k}$. За всеки вектор в първата половина на матрицата поставяме от лявата му страна неговия допълнителен, а за всеки вектор от втората половина на матрицата поставяме от дясно неговия допълнителен. Директно се проверява, че така получената матрица има исканото свойство. □

Като използваме Лема 4.2.8 и повторим аргументите от Теорема 4.2.4 лесно се доказва следната Теорема.

Теорема 4.2.5. Ако n е четно число, $n \neq 2^k$ и

$$S \in \left[2^{2n-2} + 2^{n-2} - \frac{\binom{2n-1}{n-1}}{2}; 2^{2n-2} + 2^{n-2} + \frac{\binom{2n-1}{n-1}}{2}\right],$$

то S е подходящо.

Остана да докажем твърдението от Теорема 4.2.2 б). Нека $n = 2^k$ за $k \geq 2$.

За илюстриране на основния подход в този случай първо ще разгледаме случая $n = 4$.

Пример 4.2.3. Когато $n = 4$ за всяко $w = 4, 3, 1$ и 0 съществува единствена орбитна матрица:

$$C_{4,1} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, C_{3,4} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, C_{1,4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \text{ и } C_{0,1} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Съществуват две орбитни матрици с тегло 2:

$$C_{2,2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ и } C_{2,4} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

Да разгледаме матрицата:

$$C_2 = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Да забележим, че редовете на матрицата C_2 са всички вектори с тегло 2. Интервалът от Теорема 4.2.3 за $n = 2^2$ е $[50, 5; 85, 5]$. Оказва се, че за всяко $S \in [51; 85]$ съществува подходяща матрица с тегло S. За да конструираме всички такива матрици ще използваме матриците $C_{4,1}$, $C_{3,4}$, C_2, $C_{1,4}$ и $C_{0,1}$. Например, матрицата $G = (C_{4,1}C_{3,4}C_2C_{1,4}C_{0,1})$ е характеристична матрица за множествата $B_1 = \{1, 3, 4, 5, 7, 9, 10, 12\}$, $B_2 = \{1, 2, 4, 5, 7, 8, 11, 13\}$, $B_3 = \{1, 2, 3, 5, 6, 9, 11, 14\}$ и $B_4 = \{1, 2, 3, 4, 6, 8, 10, 15\}$. Освен това

$$\sum_{y \in B_1} y = \sum_{y \in B_2} y = \sum_{y \in B_3} y = 51 \text{ и } \sum_{y \in B_4} y = 49$$

Чрез транспозицията $(10, 12)$ върху редовете на G получаваме подходяща матрица с тегло 51:

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

По подобен начин могат да се намерят подходящи матрици с тегло S за всяко $S \in [51; 85]$.

Оказва се, че за всяко $n = 2^k$, $k \geq 2$, чрез подходящо подреждане на орбитните матрици може да се намери матрица със специално свойство (както матрицата G в Пример 4.2.3)и след транспозиция на два от стълбовете на тази матрица можем да получим подходяща матрица с тегло S за всяко S от интервала, даден в Теорема 4.2.3.

Дефиниция 4.2.4. Матрица G се нарича *специална матрица от тип* S ако G е характеристична матрица за подмножествата $B_1, B_2, \ldots, B_n$, $\sum_{y \in B_i} y = S$ за $i = 1, 2, \ldots, n-1$ и $\sum_{y \in B_n} y = S - 2^{k-1}$. С други думи, скаларните произведения на всички без последния редове на G с вектора $(1, 2, \ldots, 2^n)$ са равни на S, но скаларното произведение на последния ред със същия вектор е равно на $S - 2^{k-1}$. За специална матрица G от тип S ще записваме $t(G) = S$.

В следващата Лема е показана връзка между специалните и подходящите матрици.

Лема 4.2.9. Ако в специална матрица G от тип S съществуват вектор стълбове $V_i = (v_1, v_2, \ldots, v_{n-1}, 1)$ и $V_j = (v_1, v_2, \ldots, v_{n-1}, 0)$, за които $j - i = 2^{k-1}$, то съществува подходяща матрица с тегло S.

Доказателство. Достатъчно е да сменим местата на стълбове номера i и j от G. $\square$

Лема 4.2.10. Нека G е специална матрица и V, W са вектор стълбове. Ако $A = V\overline{V}$ и $B = W\overline{W}$ са подматрици на G, то смяната на местата на A и B дава специална матрица от същия тип.

Доказателство. Нека (a_1, a_2) и (b_1, b_2) са двойките, които се получават при пресичане на A и B с i-ия ред на G. Тъй като $(a_1, a_2), (b_1, b_2) \in \{(0,1), (1,0)\}$, то $(a_1, a_2) = (b_1, b_2)$ или $(a_1, a_2) = (\overline{b_1}, \overline{b_2})$. И в двата случая смяната на местата на A и B не променя скаларното произведение на i-ия ред с $(1, 2, 3, \ldots, 2^n)$. $\square$

Лема 4.2.11. Нека G е специална матрица, V е вектор-стълб, а $C_{n,1}$ е стълб с тегло n. Тогава:

а) $G\left(V\overline{V\,C_{n,1}} \to \overline{C_{n,1}}V\overline{V}\right)$ е специална матрица от тип $\mathrm{t}(G) + 1$;

б) $G\left(C_{n,1}V\overline{V} \to V\overline{V}\,C_{n,1}\right)$ е специална матрица от тип $\mathrm{t}(G) + 1$;

в) $G\left(C_{n,1}\overline{C_{n,1}} \to \overline{C_{n,1}}C_{n,1}\right)$ е специална матрица от тип $\mathrm{t}(G) + 1$.

Доказателството е аналогично на доказателството Лема **??**.

Лема 4.2.12. Нека G е специална матрица. Ако вектор-стълба V и орбитната матрица $C_{w,l}$ са такива, че $V\overline{VC_{w,l}}$ е подматрица на G, то матрицата $G\left(V\overline{VC_{w,l}} \to \overline{C_{w,l}}V\overline{V}\right)$ е специална матрица от тип $\mathrm{t}(G) + (2w - n)\dfrac{l}{n}$.

Доказателство. За всеки ред дадената трансформация означава, че $\dfrac{(n-w)l}{n}$ единици (да припомним, че имаме $\dfrac{(n-w)l}{n}$ единици във всеки ред на $\overline{C_{w,l}}$) се преместват две позиции назад и една двойка $(0,1)$ (или $(1,0)$) се премества l позиции напред. Следователно промяната в скаларното произведение на i-ия ред за $i = 1, 2, \ldots, n$ на G с $(1, 2, 3, \ldots, 2^n)$ е равна на

$$-\frac{2(n-w)l}{n} + l = (2w - n)\frac{l}{n}.$$

□

Лема 4.2.13. Нека $C_{w,l} = \left(V\pi(V)\pi^2(V)\dots\pi^{l-1}(V)\right)$ е орбитна матрица с тегло w и дължина l, където V е вектор с тегло w. Нека освен това

$$T_w = \left(V\overline{V}\pi\left(V\right)\pi\left(\overline{V}\right)\dots\pi^{l-1}\left(V\right)\pi^{l-1}\left(\overline{V}\right)\right)$$

и $T_{n-w} = \overline{T_w}$.

а) Ако G е специална матрица, за която $C_{w,l}\overline{C_{w,l}}$ е подматрица, то $G\left(C_{w,l}\overline{C_{w,l}} \to T_w\right)$ е специална матрица от тип $\mathrm{t}(G) + (2w-n)\dfrac{l(l-1)}{2n}$;

б) Ако G е специална матрица, за която T_w е подматрица, то $G\left(T_w \to T_{n-w}\right)$ е специална матрица от тип $\mathrm{t}(G) + (2w-n)\dfrac{l}{n}$.

Доказателство. а) Без ограничение можем да считаме, че първият стълб на $C_{w,l}$ е първи стълб и на G. Тогава приносът на $C_{w,l}\overline{C_{w,l}}$ към скаларното произведение на i-ия ред на G с $(1,2,3,\dots,2^n)$ е равен на $\dfrac{l(l+1)}{2} + \dfrac{(n-w)l^2}{n}$.

Нека $(\alpha_1,\beta_1,\alpha_2,\beta_2,\dots\alpha_l,\beta_l)$ е ред от T_w. Измежду двойките (α_k,β_k) за $k = 1,2,\dots,l$ съществуват $\dfrac{wl}{n}$ двойки $(1,0)$ и $\dfrac{(n-w)l}{n}$ двойки $(0,1)$. Ако всички двойки бяха $(1,0)$, то скаларното произведение на i-ия ред на T_w с $(1,2,3,\dots,2l)$ ще бъде $1+3+\dots+(2l-1)$. Тъй като променяме $\dfrac{(n-w)l}{n}$ двойки от $(1,0)$ на $(0,1)$ и всяка промяна увеличава скаларното произведение с 1, получаваме, че приносът на T_w към скаларното произведение на i-ия ред на G с $(1,2,3,\dots,2^n)$ е равен на $1+3+\dots+(2l-1)+\dfrac{(n-w)l}{n} = l^2+\dfrac{(n-w)l}{n}$.

Следователно промяната на скаларното произведение за всеки ред е равна на

$$l^2 + \frac{(n-w)l}{n} - \frac{l(l+1)}{2} + \frac{(n-w)l^2}{n} = (2w-n)\frac{l(l-1)}{2n}.$$

б) Както в а) получаваме, че приносът на T_w към скаларното произведение на i-ия ред на G с $(1,2,3,\dots,2^n)$ е равен на $l^2 + \frac{(n-w)l}{n}$. Същите аргументи, приложени към T_{n-w} означават, че съответният принос е равен на $l^2 + \frac{wl}{n}$. Общо промяната на скаларното произведение е $(2w-n)\frac{l}{n}$. □

Теорема 4.2.6. Съществува матрица G с 2^k реда и $\binom{2^k}{2^{k-1}}$ стълба от вида $(V_1\overline{V_1}, V_2\overline{V_2}, \ldots, V_t\overline{V_t})$, за която:

- $V_1, \overline{V_1}, V_2, \overline{V_2}, \ldots, V_t, \overline{V_t}$ са всички двоични вектори с дължина 2^k и тегло 2^{k-1};

- скаларните произведения на първите $2^k - 1$ реда с $\left(1, 2, \ldots, \binom{2^k}{2^{k-1}}\right)$ са равни на

$$S = \frac{1}{4}\left(\binom{2^k}{2^{k-1}}\left(\binom{2^k}{2^{k-1}} + 1\right) + 2\right)$$

- скаларното произведение на последния ред със същия вектор е равен на $S - 2^{k-1}$.

Доказателство. Съществуват $\binom{2^k}{2^{k-1}}$ вектора с тегло 2^{k-1} и следователно всички такива вектори образуват матрица с исканите размери. Освен това, всички такива вектори се разделят на орбити с дължини, които делят 2^k. Тъй като имаме само една орбита с дължина 2 (съдържаща $(1010\ldots10)^t$ и $\pi(1010\ldots10)^t$) и само една орбита с дължина 4 (от $(11001100\ldots1100)^t$ и $\pi^l(11001100\ldots1100)^t$ за $l = 1, 2, 3$), то $\binom{2^k}{2^{k-1}} = 8s+6$. Следователно $t = 4s+3$, откъдето $S = t^2 + \frac{t+1}{2}$. Тъй като $\frac{t+1}{2} = 2s + 2$ е четно числоь то S е нечетно число.

Ще докажем, че за дадена матрица от вида $G = (V_1\overline{V_1}, V_2\overline{V_2}, \ldots, V_t\overline{V_t})$ скаларните произведения на редовете $\left(1, 2, \ldots, \binom{2^k}{2^{k-1}}\right)$ имат една и съща четност. Без ограничения всеки два реда на дадената матрица могат да бъдат записани във вида $ABCD$, където

$$A = \begin{pmatrix} 0101\ldots0101 \\ 0101\ldots0101 \end{pmatrix}, \quad B = \begin{pmatrix} 0101\ldots0101 \\ 1010\ldots1010 \end{pmatrix},$$

$$C = \begin{pmatrix} 1010\ldots1010 \\ 0101\ldots0101 \end{pmatrix}, \quad D = \begin{pmatrix} 1010\ldots1010 \\ 1010\ldots1010 \end{pmatrix}.$$

Да означим броят на редовете на A, B, C и D съответно с $2a$, $2b$, $2c$ и $2d$. Ясно е, че ако b и c са с еднаква четност, то скаларните произведения също имат една и съща четност. Броят на стълбовете на G имащи две фиксирани позиции 01 или 10 е равен на $2\binom{2^k-2}{2^{k-1}-1}$. Следователно $b+c=\binom{2^k-2}{2^{k-1}-1}$ и тъй като $\binom{2^k-2}{2^{k-1}-1}$ се дели на 2^{k-1} (понеже $k \geq 2$) получаваме, че $b+c$ е четно число, т.е. b и c са с еднаква четност.

Ако $b > c$, то скаларното произведение на първия ред с вектора $\left(1,2,\ldots,\binom{2^k}{2^{k-1}}\right)$ е по-голямо от скаларното произведение на втория ред със същия вектор. Разглеждаме всички стълбове от G, които пресичат първия ред на B в 1. Има $\binom{2^k-2}{2^{k-1}-1}$ възможности за такъв стълб и тъй като $b > \frac{1}{2}\binom{2^k-2}{2^{k-1}-1}$ получаваме, че има два допълнителни вектора. Следователно

$$G=\begin{pmatrix} \ldots & 0\ 1 & \ldots & 0\ 1 & \ldots \\ \ldots & 1\ 0 & \ldots & 1\ 0 & \ldots \\ \ldots & v_1\overline{v_1} & \ldots & \overline{v_1}v_1 & \ldots \\ \ldots & v_2\overline{v_2} & \ldots & \overline{v_2}v_2 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & v_{2^k}\overline{v_{2^k}} & \ldots & \overline{v_{2^k}}v_{2^k} & \ldots \end{pmatrix}.$$

Стълбовете на матрицата

$$G_1=\begin{pmatrix} \ldots & 10 & \ldots & 10 & \ldots \\ \ldots & 01 & \ldots & 01 & \ldots \\ \ldots & v_1\overline{v_1} & \ldots & \overline{v_1}v_1 & \ldots \\ \ldots & v_2\overline{v_2} & \ldots & \overline{v_2}v_2 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & v_{2^k}\overline{v_{2^k}} & \ldots & \overline{v_{2^k}}v_{2^k} & \ldots \end{pmatrix}$$

са всички вектори с тегло 2^{k-1}, скаларното произведение на първия ред с

вектора $\left(1,2,3,\ldots,\binom{2^k}{2^{k-1}}\right)$ намалява с 2, скаларното произведение на втория ред със същия вектор се увеличава с 2 и всички останали скаларни произведения не се променят.

Окончателно получаваме, че ако скаларните произведения на два реда с $\left(1,2,3,\ldots,\binom{2^k}{2^{k-1}}\right)$ са S_1 и S_2, като $S_2 > S_1$, то можем да намерим матрица от търсения вид, за която съответните скаларни произведения са S_1+2 и S_2-2, а всички останали скаларни произведения не се променят.

Тъй като $G = (V_1\overline{V_1}, V_2\overline{V_2}, \ldots, V_t\overline{V_t})$, то всеки ред на G е съставен от двойки $v_{2s-1}v_{2s}$, където $v_{2s} = \overline{v_{2s-1}}$ за $s = 1,2,\ldots,t$. Ясно е, че можем да подредим стълбовете на G така, че всички двойки $v_{2s-1}v_{2s}$ в последния ред да са такива, че $v_{2s-1}=1$ и $v_{2s}=0$. Тогава скаларното произведение на този ред с $\left(1,2,3,\ldots,\binom{2^k}{2^{k-1}}\right)$ е равно на $1+3+\cdots+\left(\binom{2^k}{2^{k-1}}-1\right) = t^2$. Следователно всички скаларни произведения имат четността на S, т.е. са четни числа.

Тъй като всички стълбове на G имат тегло 2^{k-1}, получаваме че сборът на всички скаларни произведения на редовете на G с $\left(1,2,3,\ldots,\binom{2^k}{2^{k-1}}\right)$ е равен на

$$2^{k-1}\sum_{i=1}^{\binom{2^k}{2^{k-1}}} i = 2^kS - 2^{k-1}.$$

Следователно ако скаларните произведения на първите 2^k-1 реда с $\left(1,2,3,\ldots,\binom{2^k}{2^{k-1}}\right)$ са равни на S, то скаларното произведение на последния ред е равно на $S-2^{k-1}$.

Да разгледаме някой от първите $\left(2^k-1\right)$ реда на G. Броят на двойките $v_{2s-1}v_{2s}=01$ за $s=1,2,\ldots,t$ е равен на $\binom{2^k-2}{2^{k-1}-1}$. Следователно скаларното произведение на този ред е равно на $t^2+\binom{2^k-2}{2^{k-1}-1} > t^2+\frac{t+1}{2} = S$. Можем да приложим описаната процедура за да получим скаларно произведение да този ред равно на $t^2+\binom{2^k-2}{2^{k-1}-1}-2$ и скаларното произведение на последния ред да е равно на t^2+2. Продължавайки по този начин ще получим матрица от търсения вид със свойството: скаларното произведение за фиксиран ред

е $t^2+\frac{t+1}{2}=S$, скаларното произведение на последния ред е $t^2+\binom{2^k-2}{2^{k-1}-1}-\frac{t+1}{2}$, а скаларното произведение на останалите редове не се променя. Да отбележим, че скаларното произведение на последния ред не става по-голямо от S. Повтаряйки тази операция с всеки от останалите 2^k-2 редове, получаваме матрица с исканото свойство. □

Да означим матрицата от Теорема 4.2.6 с $C_{2^{k-1}}$.

Лема 4.2.14. Матрицата $G=C_1C_2\dots C_m$, където $C_1,C_2,\dots,C_m$ е пермутация на всички орбитни матрици с тегла $2^k,2^k-1,\dots,2^{k-1}+1$, техните допълнения и $C_{2^{k-1}}$ е специална матрица.

Доказателство. Всяка орбитна матрица $C_{w,l}$ и нейното допълнение $\overline{C_{w,l}}$ прибавят едно и също число към скаларното произведение на всеки ред с $(1,2,3,\dots,2^n)$. Да отбележим, че това свойство е вярно без значение как са разположени стълбовете на $C_{w,l}$. □

Забележка 4.2.1. Нека V, където $\mathrm{wt}(V)=w$ е вектор стълб и $(V,\pi(V),\pi^2(V),\dots,\pi^{l-1}(V))$ са орбитите на V. От доказателството на Лема 4.2.14 следва, че стълбовете на съответната орбитна матрица $C_{w,l}$ могат да се изберат като произволна пермутация на горните вектори. Следователно едновременна смяна $C^p_{w,l}\leftrightarrow C^q_{w,l}$ и $\overline{C^p_{w,l}}\leftrightarrow\overline{C^q_{w,l}}$ води до специална матрица от същия тип.

Когато w е нечетно, то $\gcd(w,2^k)=1$ и следователно всички орбитни матрици с нечетно тегло са с дължина $n=2^k$.

Лема 4.2.15. Ако за специална матрица G от тип S е изпълнено някое от изброените по-долу условия, то съществува подходяща матрица с тегло S.

а) $C_{2^k,1}C_{2^k-1,2^k}$ е подматрица на G;

б) Съществуват две двойки $V\overline{V}$ и $W\overline{W}$ за които $V=(v_1,v_2,\dots,v_{n-1},v_n)$ и $W=(v_1,v_2,\dots,v_{n-1},\overline{v_n})$ и две произволни двойки от допълнителни вектори с разлика на техните номера, равна на 2^{k-1}.

Доказателство. Ще използваме Лема 4.2.9 и Забележка 4.2.1. а) Според Забележка 4.2.1 можем да предположим, че 2^{k-1}-ия (да напомним, че $n = 2^k$) стълб на $C_{2^k-1,2^k}$ е равен на $(1,1,1,\ldots,1,0)^t$. Сега от Лема 1 следва, че съществува подходяща матрица с тегло S.

б) Следва директно то Лема 4.2.10 и Лема 4.2.9. □

Пример 5.3.3 (Продължение) За $n = 4$ ще конструираме подходящи матрици за всяко $S \in [51;85]$. За опростяване на записването нека $C_4 = C_{4,1}$, $C_3 = C_{3,4}$, $C_1 = C_{1,4}$ и $C_0 = C_{0,1}$. Освен това, ако $V_1 = (0,0,1,1)^t$, $V_2 = (0,1,0,1)^t$ и $V_3 = (1,0,0,1)^t$, то $C_2 = (V_1\overline{V_1}\,V_2\overline{V_2}\,V_3\overline{V_3})$. По-долу са дадени всички специални матрици от тип $S \in [51;61]$.

специална матрица G	тип
$C_4C_3C_2C_1C_0$	51
$C_4C_3C_2C_0C_1$	52
$C_4\ C_3V_1\overline{V_1}\,V_2\overline{V_2}\,C_1V_3\overline{V_3}\,C_0$	53
$C_4C_3V_1\overline{V_1}\,V_2\overline{V_2}\,C_1C_0V_3\overline{V_3}$	54
$C_4C_3V_1\overline{V_1}\,C_1V_2\overline{V_2}\,V_3\overline{V_3}\,C_0$	55
$C_4C_3V_1\overline{V_1}\,C_1V_2\overline{V_2}\,C_0V_3\overline{V_3}$	56
$C_4C_3V_1C_1\overline{V_1}\,V_2\overline{V_2}\,V_3\overline{V_3}\,C_0$	57
$C_4C_3C_1V_1\overline{V_1}\,V_2\overline{V_2}\,C_0V_3\overline{V_3}$	58
$C_4C_3C_1V_1\overline{V_1}\,C_0V_2\overline{V_2}\,V_3\overline{V_3}$	59
$C_4C_3C_1C_0V_1\overline{V_1}\,V_2\overline{V_2}\,V_3\overline{V_3}$	60
$C_4C_3C_0C_1V_1\overline{V_1}\,V_2\overline{V_2}\,V_3\overline{V_3}$	61

Да отбележим, че според Лема 4.2.15, ако C_4C_3 е подматрица на специална матрица от тип S, то съществува подходяща матрица с тегло S. Следователно за всяко $S \in [51;61]$ съществува подходяща матрица с тегло S. Тъй като $\mathrm{wt}(\overline{G}) = 136 - \mathrm{wt}(G)$, то съществува и подходяща матрица за всяко

$S \in [75; 85]$. Матрицата

$$T_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} = \left(W_1\overline{W_1}W_2\overline{W_2}W_3\overline{W_3}W_4\overline{W_4}\right)$$

е получана чрез трансформацията $C_3C_1 \longrightarrow T_3 \longrightarrow T_1$. В таблицата са дадени специални матрици от тип $S \in [62; 68]$.

специална матрица G	тип
$C_4T_1C_2C_0$	62
$C_4T_1V_1\overline{V_1}V_2\overline{V_2}C_0V_3\overline{V_3}$	63
$C_4T_1V_1\overline{V_1}C_0V_2\overline{V_2}V_3\overline{V_3}$	64
$C_4T_1C_0C_2$	65
$C_4W_1\overline{W_1}W_2\overline{W_2}C_0W_3\overline{W_3}C_2$	66
$C_4W_1\overline{W_1}C_0W_2\overline{W_2}W_3\overline{W_3}C_2$	67
$C_4C_0T_1C_2$	68

Да забележим, че всяка от горните матрици се състои от два вектор стълба (C_4 и C_0) и 7 двойки от взаимно допълнителни стълбове (4 двойки от T_1 и 3 двойки от C_2). Освен това винаги съществуват две последователни двойки от допълнителни вектори. Без ограничение (виж Лема 4.2.10) можем да считаме, че ако $W\overline{W}V\overline{V}$ са двете последователни двойки, то $V = (1, 0, 0, 0)^t$ и $W = (1, 0, 0, 1)^t$. От Лема 4.2.9 сега следва, че съществува подходяща матрица с тегло $S \in [62; 68]$. Тъй като $\mathrm{wt}(\overline{G}) = 136 - \mathrm{wt}(G)$, то съществува и подходяща матрица да всяко $S \in [69; 74]$.

Преминаваме към доказателството на Теорема 4.2.2 б) Нека $n = 2^k$ за $k \geq 3$. Ще докажем, че числото S е подходящо тогава и само тогава, когато

$$S \in \left[2^{2n-2} + 2^{n-2} - \frac{1}{2}\left(\binom{2n-1}{n-1} - 1\right); 2^{2n-2} + 2^{n-2} + \frac{1}{2}\left(\binom{2n-1}{n-1} - 1\right)\right].$$

Тъй като $\binom{2n-1}{n-1}$ е нечетно, от Теорема 4.2.3 следва, че всички подходящи числа са от дадения интервал. Остава да докажем, че ако

$$S \in \left[2^{2n-2}+2^{n-2}-\frac{1}{2}\left(\binom{2n-1}{n-1}-1\right); 2^{2n-2}+2^{n-2}+\frac{1}{2}\left(\binom{2n-1}{n-1}-1\right)\right],$$

то S е подходящо число. Ще покажем, че за всяко S от дадения интервал съществува специална матрица с тегло S за която е изпълнено някое от условията на Лема 4.2.15. Освен това от $\mathrm{wt}(\overline{G})+\mathrm{wt}(G) = 2^{n-1}(2^n+1)$ следва, че е достатъчно да докажем твърдението за първата половина на интервала, т.е. до $2^{2n-2}+2^{n-2}$.

Ясно е, че за всяко $w = 2^k, 2^k-1$ съществува единствена орбитна матрица. Да означим с $C_{2^k,1}$ единствената орбитнаматрица с тегло 2^k и с $C_{2^k-1,2^k}$ единствената орбитна матрица с тегло 2^k-1. Освен това, нека $C_{2^{k-1}}$ е матрица със стълбове всички вектори с тегло 2^{k-1}, която притежава свойството от Теорема 2.

Да разгледаме специална матрица G от тип S. Ще наричаме трансформация $H_1 \longrightarrow H_2$ *допустима*, ако за всяко $S \in [t(G); t(G(H_1 \longrightarrow H_2))]$ съществува специална матрица от тип S за която е изпълнено някоя от условията на Лема 4.2.15. Ако G и $G_1 = G(H_1 \longrightarrow H_2)$ са специални матрици и $w = \mathrm{t}(G_1) - \mathrm{t}(G)$, то ще пишем $t^+(H_1 \longrightarrow H_2) = w$. Да разгледаме следната матрица:

$$G_1 = C_{2^k,1}C_{2^k-1,2^k}C^1_{2^k-2,l_1}\dots C^p_{2^{k-1}+1,2^k}C_{2^{k-1}}\overline{C^p_{2^{k-1}+1,2^k}C^1_{2^k-2,l_1}\dots C_{2^k-1,2^k}C_{2^k,1}}.$$

Тази матрица е получена чрез подреждане на орбитните матрици $C_{w,l}$ в намаляващ ред на техните тегла. Освен това, всеки две матрици, които са симетрични по отношение на $C_{2^{k-1}}$ са допълнителни една на друга. От Лема 4.2.14 следва, че матрицата G_1 е специална. От доказателството на Теорема 4.2.3 и от Лема 4.2.15 (матрицата $C_{2^k,1}C_{2^k-1,2^k}$ и подматрица на G_1) следва, че съществува подходяща матрица с тегло $S = 2^{2n-2}+2^{n-2}-\frac{1}{2}\left(\binom{2n-1}{n-1}-1\right)$.

Започвайки от G_1 преместваме една по една всички двойки от допълнителни вектори от $C_{2^{k-1}}$ като прескачаме една по една матриците $\overline{C^t_{w,l}}$ за $2^{k-1}+1 \leq w \leq 2^k$ в ляво от $\overline{C_{2^k,1}}$. От Лема 4.2.12 следва $t^+(\overline{C_{2^k-1,2^k}C_{2^k,1}} \longrightarrow \overline{C_{2^k,1}C_{2^k-1,2^k}}) = 1$, $t^+(V\overline{V}\overline{C_{w,l}} \longrightarrow \overline{C_{w,l}}V\overline{V}) = (2w-2^k)\frac{l}{2^k}$ (в частност $t^+(V\overline{V}\overline{C_{2^{k-1}+1,2^k}} \longrightarrow \overline{C_{2^{k-1}+1,2^k}}V\overline{V}) = 2$). Да напомним, че $C_{2^{k-1}}$ се състои от $\frac{1}{2}\binom{2^k}{2^{k-1}}$ двойки от вида $V\overline{V}$. Освен това матрицата $C_{2^k,1}C_{2^k-1,2^k}$ е подматрица на G_1.

Директно се проверява, че всяка от описаните операции представлява допустима трансформация. Получаваме матрицата

$$G_2 = C_{2^k,1}C_{2^k-1,2^k}C^1_{2^k-2,l_1}\dots C^s_{2^{k-1}+1,2^k}\overline{C^s_{2^{k-1}+1,2^k}C^1_{2^k-2,l_1}C_{2^k-1,2^k}}C_{2^{k-1}}\overline{C_{2^k,1}}.$$

Лема 4.2.13 а) приложена за $w = 2^{k-1}+1$ и $l = 2^k$ означава, че

$$t^+(C^s_{2^{k-1}+1,2^k}\overline{C^s_{2^{k-1}+1,2^k}} \to T^s_{2^{k-1}+1}) = 2^k - 1,$$

а от Лема 4.2.11 а) следва, че $t^+(V\overline{V}\overline{C_{2^k,1}} \to \overline{C_{2^k,1}}V\overline{V}) = 1$. Следователно тъй като имаме $\frac{1}{2}\binom{2^k}{2^{k-1}}$ двойки от вида $V\overline{V}$ в $C_{2^{k-1}}$ и $\frac{1}{2}\binom{2^k}{2^{k-1}} > 2^k - 1$, следва че $C^s_{2^{k-1}+1,2^k}\overline{C^s_{2^{k-1}+1,2^k}} \to T^s_{2^{k-1}+1}$ е допустима трансформация. Да преместим една по една всички двойки от допълнителни вектори от $T^s_{2^{k-1}+1}$ като прескачаме една по една всяка от матриците $\overline{C^t_{w,l}}$ за $2^{k-1}+1 \leq w \leq 2^k-1$ в ляво от $C_{2^{k-1}}$. Повтаряме тази операция за всички двойки $C^t_{2^{k-1}+1,n}\overline{C^t_{2^{k-1}+1}}$ for $t = s-1, s-2, \dots, 1$. Означаваме получената матрица

$$C_{2^k,1}C_{2^k-1,2^k}C^1_{2^k-2,l_1}\dots C^s_{2^k-2,l_s}\overline{C^s_{2^k-2,l_s}C^1_{2^k-2,l_1}C_{2^k-1,2^k}}T^1_{2^{k-1}+1}\dots T^s_{2^{k-1}+1}C_{2^{k-1}}\overline{C_{2^k,1}}$$

с G_3. Директно се проверява, че всяка от горните трансформации е допустима. Да отбележим, че ако $T^s_{2^{k-1}+1}C_{2^{k-1}}$ е подматрица на специална матрица от тип S, то от Лема 4.2.15 б) следва, че съществува подходяща матрица с тегло S. Продължавайки по този начин, чрез редица от допустими трансформации можем да получим матрицата

$$G_4 = C_{2^k,1}T_{2^k-1}T^1_{2^k-2}\dots T^1_{2^{k-1}+1}\dots T^s_{2^{k-1}+1}C_{2^{k-1}}\overline{C_{2^k,1}}.$$

С допустими трансформации от вида $T_w \to T_{n-w}$ (което е еквивалентно на $T_w \to \overline{T_w}$), $V\overline{VC_{2^k,1}} \to \overline{C_{2^k,1}}V\overline{V}$ и $C_{2^k,1}V\overline{V} \to V\overline{V}\,C_{2^k,1}$ можем да получим

$$G_5 = \overline{C_{2^k,1}T_{2^k-1}T^1_{2^k-2}\dots T^1_{2^{k-1}+1}\dots T^s_{2^{k-1}+1}}C_{2^{k-1}}C_{2^k,1}.$$

Нека $(v_1, v_2, \dots v_n)$ е първият ред на G_5 (да отбележим, че $v_1 = 0$ и $v_n = 1$). Всяка двойка $v_{2s}v_{2s+1}$ за $s = 1, 2, \dots, 2^{n-1} - 1$ е такава, че $v_{2s} + v_{2s+1} = 1$. Следователно минималаната възможна стойност за скаларното произведение на такъв ред с $(1, 2, \dots, 2^n)$ се достига при $v_{2s} = 1$ за всяко $s = 1, 2, \dots, 2^{n-1} - 1$. Тъй като скаларното произведение на $(0, 1, 0, 1, 0, \dots, 1, 0, 1, 0, 1)$ с $(1, 2, \dots, 2^n)$ е равно на $2 + 4 + 6 + \dots + 2^n = 2^{2n-2} + 2^{n-1}$, имаме $t(G_5) > 2^{2n-2} + 2^{n-2}$. С това доказателството е завършено.

4.2.2 Неадаптивно търсене за теглова функция $\left[\frac{\mathbf{i-1}}{\mathbf{2^{n-1}}}\right] + \mathbf{1}$

В този случай [45] задачата е еквивалентна на намирането на двоична $n \times 2^n$ матрица G, чийто стълбове са всички двоични вектори с дължина n и скаларното произведение на всеки ред на G с вектора $(\underbrace{1, 1, \dots, 1}_{2^{n-1}}, \underbrace{2, 2, \dots, 2}_{2^{n-1}})$ е равно на S.

При нечетно $n = 2t + 1$ ще намерим необходимо и достатъчно условие едно число S да е подходящо.

Лема 4.2.16. Ако S е подходящо число, то

$$S \in \left[3.2^{n-2} - \binom{n-2}{t}, 3.2^{n-2} + \binom{n-2}{t}\right].$$

Доказателство. Матрицата G има минимално тегло когато стълбовете и са наредени в намаляващ ред на теглата. За теглото на такава матрица G получаваме

$$n.\mathrm{wt}(G) = \sum_{i=n}^{t+1} i\binom{n}{i} + 2\sum_{i=t}^{0} i\binom{n}{i}.$$

За пресмятане на горната сума използваме тъждествата $\binom{n}{k}.k = n\binom{n-1}{k-1}$ и $\sum_{i=0}^{t}\binom{n}{i} = 2^{n-1}$. Директно пресмятане показва, че сумата е равна на

$$n\left(3.2^{n-1} - \binom{n-2}{t}\right).$$

Остава да отбележим, че $\mathrm{wt}(G) + \mathrm{wt}(\overline{G}) = 3.2^{n-1}$. □

Лема 4.2.17. Съществува подходяща матрица с тегло $S = 3.2^{n-2} - \binom{n-2}{t}$.

Доказателство. Да образуваме матрица G като наредим всички двоични вектори в намаляващ ред на техните тегла до тегло $t+1$ и след това да поставим допълнителните матрици на вече избраните. Както знаме така получената матрица е подходяща. Според Лема 4.2.16 теглото на тази матрица е равно на $3.2^{n-2} - \binom{n-2}{t}$. □

Теорема 4.2.7. Числото S е подходящо тогава и само тогава, когато

$$S \in \left[3.2^{n-2} - \binom{n-2}{t}, 3.2^{n-2} + \binom{n-2}{t}\right].$$

Доказателство. Необходимостта следва от Лема 4.2.16. Нека $C_{l,w}$ е орбитна матрица от първата половина на G, като тогава допълнителната орбитна матрица $\overline{C_{l,w}}$ ще бъде във втората половина на G. Директно пресмятане показва, че смяната на местата на $C_{l,w}$ и $\overline{C_{l,w}}$ води до подходяща матрица G_1 с тегло $\mathrm{wt}(G_1) = \mathrm{wt}(G) + \frac{2lw}{n} - l$. Така при $l = 1$, $w = n$ имаме $\mathrm{wt}(G_1) = \mathrm{wt}(G) + 1$. Тъй като $n = 2t+1$ и $t+1$ са взаимно прости, при $w = t+1$ имаме $l = n$ и тогава $\mathrm{wt}(G_1) = \mathrm{wt}(G) + 1$. Както в доказателството на Теорема 4.2.6 директно се вижда, че чрез подходящи разместванията на орбитните матрици може да се получи подходяща матрица за всяко $S \in \left[3.2^{n-2} - \binom{n-2}{t}, 3.2^{n-2} + \binom{n-2}{t}\right]$. □

Ще илюстрираме конструкцията от Теорема 4.2.7 със следния пример.

Пример 4.2.4. При $n = 5$ от Лема 4.2.16 следва, че ако S е подходящо, то $S \in [21, 27]$. Като използваме Теорема 4.2.7 ще покажем как можем да намерим подходяща матрица с тегло S за всяко $S \in [21, 27]$. Имаме 8 орбитни матрици:

$$C_{1,5} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, C_{4,5} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

$$C^1_{3,5} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}, C^2_{3,5} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix},$$

и техните допълнителни. Да означим с G_S подходяща матрица с тегло S. Чрез смяна на местата на някои от матриците $C_{l,w}$ с техните допълнителни намираме пидходящи матрици за всяко $S \in [21, 27]$.

$$G_{21} = C_{5,1}C_{4,5}C^1_{3,5}C^2_{3,5}\overline{C^2_{3,5}C^1_{3,5}C_{4,5}C_{5,1}}$$

$$G_{22} = \overline{C_{5,1}}C_{4,5}C^1_{3,5}C^2_{3,5}\overline{C^2_{3,5}C^1_{3,5}C_{4,5}}C_{5,1}$$

$$G_{23} = C_{5,1}C_{4,5}C^1_{3,5}\overline{C^2_{3,5}C^1_{3,5}C_{4,5}C_{5,1}}C^2_{3,5}$$

$$G_{24} = \overline{C_{5,1}}C_{4,5}C^1_{3,5}\overline{C^2_{3,5}C^1_{3,5}C_{4,5}}C_{5,1}C^2_{3,5}$$

$$G_{25} = \overline{G_{23}},\ G_{26} = \overline{G_{22}},\ G_{27} = \overline{G_{21}}.$$

4.2.3 Неадаптивно търсене за теглова функция $\left[\frac{\mathbf{i-1}}{\mathbf{2^{n-2}}}\right] + \mathbf{1}$

В този случай [46] задачата е еквивалентна на намирането на двоична $n \times 2^n$ матрица G, чийто стълбове са всички двоични вектори с дължина

n и скаларното произведение на всеки ред на G с вектора

$$(\underbrace{1,1,\ldots,1}_{2^{n-2}},\underbrace{2,2,\ldots,2}_{2^{n-2}},\underbrace{3,3,\ldots,3}_{2^{n-2}},\underbrace{4,4,\ldots,4}_{2^{n-2}})$$

е равно на S.

Ще намерим интервал от подходящи числа S.

Да означим с I_n^h множеството от всички подходящи числа S за множеството $A = \{a_1, a_2, a_3, \ldots, a_{2^n}\}$ и теглова функция $\mathrm{w}_h(x_i) = \left[\frac{i-1}{2^h}\right] + 1$ за $h = 0, 1, \ldots, n$.

Теорема 4.2.8. Ако $a, b \in I_{n-1}^{n-1}$, то $a + b + 2^{n-1} \in I_n^{n-2}$.

Доказателство. Тъй като $a, b \in I_{n-1}^{n-1}$, то съществуват подходящи матрици G_a и G_b с размерност $(n-1) \times 2^{n-1}$. Да припомним, че стълбовете на G_a и G_b са всички двоични вектори с дължина $n-1$. Освен това, скаларното произведение на всеки ред на G_a (съответно G_b) с $(\underbrace{1,1,\ldots 1}_{2^{n-1}},\underbrace{2,2,\ldots,2}_{2^{n-1}})$ е равно на a (съответно b). Тъй като във всеки ред на G_a и G_b има точно 2^{n-2} единици, то $a > 2^{n-2}$, $b > 2^{n-2}$ и скаларното произведение на всеки ред на G_b с $(\underbrace{3,3,\ldots 3}_{2^{n-1}},\underbrace{4,4,\ldots,4}_{2^{n-1}})$ е равно на $b + 2^{n-1}$.

Да разгледаме следната матрица:

$$G = \begin{pmatrix} G_a & G_b \\ \underbrace{00\ldots0}_{2^{n-1}} & \underbrace{11\ldots1}_{2^{n-1}} \end{pmatrix}.$$

Скаларното произведение на всеки (без последния) от редовете на G с

$$(\underbrace{1,\ldots,1}_{2^{n-1}},\underbrace{2,\ldots,2}_{2^{n-1}},\underbrace{3,\ldots,3}_{2^{n-1}},\underbrace{4,\ldots,4}_{2^{n-1}})$$

е равно на $a + b + 2^{n-1}$. Скаларното произведение на последния ред е $w = 7.2^{n-2}$.

Произволен вектор $v \in F_2^{n-1}$ се появява като стълб във всяка от матриците G_a и G_b. Ако сменим местата на 0 и 1 в последния ред в позициите на появяване на v ще увеличим стойността на w.

Да означим с X множеството от първите 2^{n-2} стълба на G_a и с Y множеството от първите 2^{n-2} стълба на G_b.

Ако $v \in X \cap Y$ или $v \in \left(F_2^{n-1} \backslash X\right) \cap \left(F_2^{n-1} \backslash Y\right)$, стойността на w ще намалее с 2. Ако $v \in \left(F_2^{n-1} \backslash X\right) \cap Y$, то стойността на w намалява с 1. Накрая, ако $v \in X \cap \left(F_2^{n-1} \backslash Y\right)$ стойността на w намалява с 3.

Ако $X \equiv Y$, то $a = b$ и следователно $a + b + 2^{n-1}$ е четно число. От друга страна е възможно да се получат всички четни стойности на w между 7.2^{n-2} и 3.2^{n-2}.

Когато $X \not\equiv Y$ отново лесно се съобразява, че всички стойности на w между 7.2^{n-2} и 3.2^{n-2} са възможни. Тъй като $a+b+2^{n-1} > 3.2^{n-2}$, намираме подходяща матрица с тегло $a + b + 2^{n-1}$. □

Теорема 4.2.9. Ако $n = 2t$, то $\left[2^{n+1} - \binom{n-2}{t-1}, 2^{n+1} - \binom{n-2}{t-1}\right] \subset I_n^{n-2}$.

Доказателство. От Теорема 4.2.7 следва, че ако S е подходящо число за $h = n - 1$ и $n = 2t - 1$, то

$$S \in \left[3.2^{n-2} - \binom{n-2}{t-1}, 3.2^{n-2} + \binom{n-2}{t-1}\right].$$

Сега твърдението е директно следствие от Теорема 4.2.8. □

4.2.4 Неадаптивно търсене на два елемента

В тази част ще разгледаме задачата за неадаптивно търсене на два неизвестни елемента от множеството $A = \{1, 2, 3, \ldots, 2^n\}$, като множествата въпроси са с равни суми [47].

Нека от множеството $A = \{1, 2, 3, \ldots, 2^n\}$ са избрани два елемента x и y. За дадено естествено число S множествата въпроси са всички подмножества $B \subset A$ със сбор на елементите си равен на S. Възможните отговори на множество въпрос B са: 0, ако нито един от елементите x и y не е от B; 1, ако точно един от двата елемента е в B и 2, ако и двата елемента са в B. Ще намерим всички стойности на S, за които е възможно да намерим неизвестните елементи x и y.

Да разгледаме множество от въпроси $B_1, B_2, \ldots, B_k$ и да означим с $a = (a_1, a_2, \ldots, a_k)^t$ вектора от получените отговори. Ако можем за определим x и y, то сборът от стълбове x и y на характеристичната матрица G е равен на a, като не съществуват други два стълба с това свойство.

Следователно, за решаването на така поставената задача за търсене, трябва да намерим двоична матрица G със следните две свойства:

1. Скаларното произведение на всеки ред на G с вектора $(1, 2, \ldots, 2^n)$ е равно на S.

2. Не съществуват различни двойки от стълбове на G, които имат един и същи сбор.

Ще намерим всички естествени числа S, за които съществува матрица G_S с горните свойства.

Теорема 4.2.10. Матрицата G_S съществува тогава и само тогава, когато

$$S \in \left[2^n - 1, 2^{2n-1} - 2^{n-1} + 1\right].$$

Доказателство. Нека $S \in [2^n - 1, 2^{2n-1} - 2^{n-1} + 1]$ и да разгледаме всички

възможни множества въпроси. Да означим с G_S съответната характеристична матрица.

Първо ще докажем, че матрицата G_S не съдържа равни стълбове. Достатъчно е да докажем, че за всеки два елемента a и b, $a < b$ от A съществува множество въпрос B, за което $a \notin B$ и $b \in B$ или $a \in B$ и $b \notin B$. Прилагаме т.н. лаком алгоритъм за представянето на числото $S - b$ като сбор на елементи от $A \backslash \{a, b\}$. Ако този алгоритъм е успешен, то търсеното множество съществува. Когато $a \geq 4$ имаме $a = 1 + (a - 1)$ и $b = 1 + (b - 1) = 2 + (b - 2)$ и следователно лакомият алгоритъм е успешен. При $a = 3$ и $b \geq 5$ имаме $a = 1 + 2$ и $b = 1 + (b - 1)$ и отново алгоритъма е успешен. При $a = 3$ и $b = 4$ алгоритъмът е неуспешен само ако в даден момент за завършването му е необходимо числото 4. Тъй като $S \leq 2^{2n-1} - 2^{n-1} + 1$, то числото 5 не е включено в получената до този момент сума. Сега заменяме $4 + 4$ с $3 + 5$ и получаваме множество въпрос, за което $a \in B$ и $b \notin B$. Случаите $a = 2$ и $a = 1$ са аналогични.

Остана да докажем, че не съществуват две различни двойки от стълбове, имащи равни сборове. Достатъчно е да покажем, че за произволни $a, b, c, d \in A$, $a < b < c < d$ съществува множество въпрос B, за което $|B \cap \{a, b, c, d\}|$ е нечетно. Отново прилагаме лакомия алгоритъм за представяне на $S - b - c - d$ като сбор на елементи от $A \backslash \{a, b, c, d\}$. Ако алгоритъмът е успешен, имаме $|B \cap \{a, b, c, d\}| = 3$, т.е. намираме търсеното множество. Нека $a \geq 3$, $b - a \geq 2$, $c - b \geq 2$ и $d - c \geq 2$. За $x \in \{a, b, c, d\}$ имаме $x = 1 + (x - 1)$ и $1, x - 1 \notin \{a, b, c, d\}$, което означава, че алгоритъмът е успешен.

Останалите случаи се разглеждат отделно. Например, нека $a = 2$, $b - a \geq 2$, $c - b = 1$ и $d - c \geq 2$. Тъй като $b = 1 + (b - 1)$, $d = 1 + (d - 1)$ алгоритъма е неуспешен само ако в даден момент сборът се допълва само с a или c. Нека първо числото е c. Понеже при $c \geq 7$ имаме $c = 3 + (c - 3)$, където $\{a, b\} \cap \{3, c - 3\} = \emptyset$, то алгоритъма е успешен при $c \geq 7$. Остава да разгледаме случаите $c = 6$ или $c = 5$. Ако $d - c \geq 3$ заместваме $b + 2c = 5 + 2.6 = 17$ с

$7+8+1+4$ (при $c=6$) и $b+2c=4+2.5=14$ с $6+7+1$ (при $c=6$). И в двата случая алгоритъмът е успешен. Ако $d-c=1$ имаме $\{a,b,c,d\}=\{2,5,6,8\}$ или $\{a,b,c,d\}=\{2,4,5,7\}$. И в двата случая от $S \leq 2^{2n-1}-2^{n-1}+1$ следва, че $d+1$ не е избран от алгоритъма. Тъй като $b+2c=17=1+3+4+9$ в първия случай и $b+2c=4+2.5=6+8$ за втория, алгоритъма е успешен.

Сега да допуснем, че алгоритъм спира при $a=2$. Да забележим, че $c-2 \neq 2$ и $c-2 \neq b$. Ако заместим c с 2 и $c-2$ отново намираме множество въпрос B, за което $|B \cap \{a,b,c,d\}|=3$. □

4.2.5 Търсене с грешни отговори

В тази част са представени резултати, получени в [14], [15] и [50].

Да разгледаме описаната по-горе (A,w,S) задача за неадаптивно търсене при теглова функция $w(i)=i$. Нека неизвестният елемент се избира от крайно множество $\mathcal{A}$ с M елемента. Без ограничение можем да считаме, че

$$\mathcal{A}=\{1,2,3,\ldots,M\}.$$

Да допуснем, че в получените отговори е разрешен един неверен. Да означим въпросите, с които можем да намерим неизвестния елемент с $B_1,B_2,\ldots,B_k$.

За всеки елемент x от множеството $\mathcal{A}$ получените k отговора ще представляват стълб x от характеристичната матрица (когато няма грешен отговор) или ще се отличават само в една позиция от същия този стълб (когато имаме грешен отговор). За да можем да определим неизвестния елемент x, всеки два стълба трябва да се различават в поне 3 позиции. Това означава, че двоичния код, образуван от стълбовете на характеристичната матрица, има дължина $n=k$, минимално разстояние $d=3$ и мощност M, т.е. това е един двоичен $(n,M,d \geq 3)$ код. Скаларното произведение на всеки ред на G с $(1,2,3,\ldots,M)$ е равно на S. Матрица с горните свойства ще наричаме *подходяща матрица с тегло* S.

Пример 4.2.5. Ще решим горната задача за $M = 16$, т.е. $A = \{1, 2, 3, \ldots 16\}$. Тъй като минималното n за което съществува двоичен $(n, 16, 3)$ код е $n = 7$, всяка подходяща матрица G с минимален брой редове е матрица 7×16. Съществуват два нееквивалентни $(7, 16, 3)$ кода - линейния съвършен $[7, 4, 3]$ код на Хеминг и неговия съседен клас.

Първо ще конструираме подходящи матрици като използваме $[7, 4, 3]$ кода на Хеминг. Тегловното разпределение за този код се дава с $A_0 = 1, A_3 = 7, A_4 = 7, A_7 = 1$. Ако стълбовете в подходяща матрица G са подредени в нарастващ (съответно намаляващ) ред на техните тегла, то $\mathrm{wt}(G)$ е максималното (съответно минималното) възможно. Директно се проверява, че матрицата

$$\left(\begin{array}{cccccccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
\hline
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}\right)$$

е подходяща с тегло 57. Тогава матрицата $\overline{G_1}$ е също подходяща с тегло 79.

Следователно най-малката (съответно най-голямата) стойност на S, за която съществува подходяща матрица е $S = 57$ (съответно $S = 79$). Трябва да определим за кои стойности на $S \in [57, 79]$ съществува подходяща матрица с тегло S. Да припомним, че ако G е подходяща, то $\overline{G}$ е също подходяща и $S_G + S_{\overline{G}} = 136$. Достатъчно е да проверим само стойностите на S от 57 до средата на интервала $[57, 79]$. Матрицата

$$\left(\begin{array}{cccccccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
\hline
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0
\end{array}\right)$$

е подходяща с тегло $S = 60$. Всички вектори с тегла 3 и 4 са комбинирани в комбинация $V\overline{V}$, където V е вектор с тегло 4. Като разменим местата на вектора $\mathbf{1}$ с произволна двойка $V\overline{V}$, получената матрица е подходяща, като S се уеличава с 1.

Разменяйки местата на вектора $\mathbf{1}$ със следващите двойки $V\overline{V}$ и накрая с вектора $\mathbf{0}$, получаваме подходящи матрици за всяко $S \in [61, 68]$. Следователно за всяко $S \in [60, 76]$ съществува подходяща матрица с тегло S, като вече намерихме и подходящи матрици за $S = 57$ и $S = 79$.

Лесно се намира подходяща матрица с тегло $S = 58$. Не е трудно да се докаже, че не съществува подходяща матрица с тегло $S = 59$.

Съседен клас на кода на Хеминг има тегловно разпределетние $A_1 = 1$, $A_2 = A_5 = 3$, $A_3 = A_4 = 4$ и $A_6 = 1$. В този случай границите за S са съответно 81 и 55. Както при използване на кода на Хеминг, можем да намерим подходящи матрици с тегла 55, 56 и 59:

$$\left(\begin{array}{cccccccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
\hline
1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1
\end{array}\right)$$

$$\left(\begin{array}{cccccccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
\hline
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}\right)$$

$$\left(\begin{array}{cccccccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
\hline
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}\right)$$

Следователно за всяко $S \in [55, 81]$ съществува подходяща матрица с тегло S.

В следващата теорема се доказва съществуването на подходяща матрица при използване на цикличен код с нечетна дължина.

Теорема 4.2.11. Нека C е двоичен цикличен $(n, M = 2^k, 3)$ код, който съдържа вектора съставен от единици. Съществува подходяща матрица $n \times M$ с тегло $\dfrac{\sum_{i=1}^{M} i.\mathrm{wt}(v_i)}{n}$ където $v_1, v_2, \ldots, v_M$ са кодовите думи от C и $\mathrm{wt}(v_i) \leq \mathrm{wt}(v_{i+1})$, $i = 1, 2, \ldots, M-1$.

Доказателство. Нека $n = 2t + 1$ и с G_i за $i = 0, 1, \ldots, t$ да означим матрицата с редове всички кодови думи с тегло i. Да разгледаме матрицата

$$G = G_0 G_1 \ldots G_{t-1} G_t \overline{G_t G_{t-1}} \ldots \overline{G_1 G_0}.$$

Тъй като G_i и $\overline{G_i}$ прибавят еднакво число към скаларното произведение на всеки ред с вектора $(1, 2, \ldots, M)$, то G е подходяща матрица. Теглото на тази матрица е равно на $\dfrac{\sum_{i=1}^{M} i.\mathrm{wt}(v_i)}{n}$, където $v_1, v_2, \ldots, v_M$ са кодовите думи на C и $\mathrm{wt}(v_i) \leq \mathrm{wt}(v_{i+1})$, $i = 1, 2, \ldots, M-1$ □

При $M = 2^{2^r - r - 1}$ минималното n, за което съществува $(n, M, 3)$ код е $n = 2^r - 1$. Следователно за да конструираме подходяща матрица трябва да използваме съвършен двоичен код с параметри $(n = 2^r - 1, M = 2^{2^r - r - 1}, 3)$. Тъй като кодът на Хеминг е с такива параметри и удовлетворява условията на Теорема 4.2.11, то за всяко r можем да намерим подходящи граници за S. Да означим тези граници с S_{min} и S_{max}.

Както видяхме в Пример 4.2.5 за $M = 16$ с използването на съседен клас на кода на Хеминг можем да получим по-добри граници за подходящите числа S.

Оказва се, че при използване на код на Хеминг с дължина $n = 2^t - 1$ при t четно число всяко S от интервала $[S_{min}, S_{max}]$ е подходящо [50].

Теорема 4.2.12. За двоичния кода на Хеминг с дължина $n = 2^t - 1$, t четно число, всички числа от интервала $[S_{min}, S_{max}]$ са подходящи.

4.3 Една двумерна задача за търсене

В тази част е представен резултат, получен в [53]. Ще разгледаме една двумерна задача за търсене, предложена от Katona [30]. Това е задача за адаптивно търсене на неизвестен единичен квадрат в даден правоъгълник. Първо ще дадем формално описание на задачата. Множеството

$$\mathcal{A}(m,n) = \{(i,j) \mid i,j \in \mathbf{Z}, 1 \leq i \leq m, 1 \leq j \leq n\}$$

се нарича правоъгълник с размери $m \times n$. Когато $m = n$ казваме, че е е даден квадрат с размерност n.

За два елемента $\mathbf{a} = (a_1, a_2) \in \mathcal{A}(m,n)$ и $\mathbf{b} = (b_1, b_2) \in \mathcal{A}(m,n)$ записваме $\mathbf{a} \leq \mathbf{b}$ тогава и само тогава, когато $a_1 \leq b_1$ и $a_2 \leq b_2$. Както в класическата задача за търсене нека е избран елемент $\mathbf{x} = (x_1, x_2) \in \mathcal{A}(m,n)$, който не ни е известен.

Искаме да намерим неизвестния елемент $\mathbf{x}$ с минималния брой въпроси от вида: Вярно ли е, че $\mathbf{x} \leq \mathbf{a}$?

Задаването на въпрос е еквивалентно на посочването на елемент $\mathbf{a}$ на $\mathcal{A}(m,n)$. Разглеждаме адаптивно търсене, което означава, че всеки въпрос се задава след като е получен отговора на предишния.

Да означим с $t(m,n)$ минималният брой въпроси, необходими за намиране на $\mathbf{x}$. Първо ще докажем две важни неравенства [72],[53].

Лема 4.3.1. Изпълнени са неравенствата

$$\lceil \log_2 m + \log_2 n \rceil \leq t(m,n) \leq \lceil \log_2 m \rceil + \lceil \log_2 n \rceil.$$

Доказателство. Тъй като правоъгълника $\mathcal{A}(m,n)$ има mn елемента, то според Лема 4.1.1 за намирането на неизвестния елемент са необходими поне $\lceil \log_2 mn \rceil = \lceil \log_2 m + \log_2 n \rceil$ въпроса. Следователно

$$\lceil \log_2 m + \log_2 n \rceil \leq t(m,n).$$

От друга страна, решавайки едномерната задача можем да определим в кой от „редовете“ на правоъгълника $\mathcal{A}(m,n)$ се намира неизвестния елемент с $\lceil \log m \rceil$ въпроса. След това, отново решавайки едномерната задача, можем да намерим неизвестния елемент с $\lceil \log n \rceil$ въпроса. Следователно

$$t(m,n) \leq \lceil \log_2 m \rceil + \lceil \log_2 n \rceil. \qquad \square$$

Лесно се доказва, че $\lceil \log m + \log n \rceil + \varepsilon = \lceil \log m \rceil + \lceil \log n \rceil$, където $\varepsilon = 0$ или 1.

Когато $\varepsilon = 0$ имаме $\lceil \log m + \log n \rceil = \lceil \log m \rceil + \lceil \log n \rceil$ и тогава задачата за определяне на $t(m,n)$ е решена. Когато $\varepsilon = 1$ за $t(m,n)$ има две възможности и в този случай задачата за определяне на $t(m,n)$ се оказва нетривиална.

Дефиниция 4.3.1. Правоъгълник $\mathcal{A}(m,n)$ се нарича *разрешим* ако съществува алгоритъм, чрез който неизвестният елемент $\mathbf{x}$ от $\mathcal{A}(m,n)$ може да бъде намерен с $\lceil \log m + \log n \rceil$ въпроса. В противен случай правоъгълникът се нарича *неразрешим*.

Преди да изложим основните резултати ще представим някои елементарни твърдения.

Лема 4.3.2. Ако $m_1, n_1, m_2, n_2 \in \mathbb{N}$ и $m_1 \leq n_1$, $m_2 \leq n_2$, то $t(m_1,n_1) \leq t(m_2,n_2)$.

Лема 4.3.3. За произволни $j,k,m,n \in \mathbb{N}$ е изпълнено неравенството

$$t(2^j m, 2^k n) \leq j + k + t(m,n).$$

В частност, ако $\mathcal{A}(m,n)$ е разрешим, то $\mathcal{A}(2^j m, 2^k n)$ е също разрешим.

Лема 4.3.4. За естествено число $m = 2^t - 1$ правоъгълникът $\mathcal{A}(m,n)$ е разрешим за всяко n.

Доказателство. Ще извършим доказателството с индукция по n. При $n = 1$ твърдението е очевидно. Нека $n = 2^l + A > 1$, $0 < A < 2^l$ и $\mathcal{A}(m, n')$ е разрешим за всяко $n' < n$. Можем да допуснем, че $mn \leq 2^{t+1}$, защото в противен случай двете граници от Лема 4.3.1 съвпадат и няма какво да доказваме.

Задаваме последователни въпроси от дадения вид докато не получим отговор „да“.

$$\mathbf{q}_\alpha = \left(\sum_{i=1}^{\alpha} 2^{t-i}, 2^i \right), \alpha = 1, 2, \ldots, t.$$

Ако на някои от въпросите е отговорено с да, прилагаме алгоритъма от Лема 4.3.1 за намиране на $\mathbf{x}$, когато страните на правоъгълника са степени на двойката.

Ака отговорите на всички въпроси $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_t$ са „не“, то неизвестният елемент $\mathbf{x}$ се съдържа в правоъгълник с размери $m \times A$. Според индукционното допускане този правоъгълник е разрешим. Остава да забележим, че

$$mA = mn - m2^l \leq 2^{t+1} - 2^l(2^t - 1) = 2^l$$

и следователно $\mathbf{x}$ може да бъде намерен с $t + 1$ въпроса. Това означава, че $\mathcal{A}(m, n)$ е разрешим. □

Теорема 4.3.1. Ако $m = \frac{2^{st}-1}{2^s-1}$ за $s, t \in \mathbb{N}$, то за произволно $n \in \mathbb{N}$ правоъгълникът $\mathcal{A}(m, n)$ е разрешим.

Доказателство. Ще докажем твърдението с индукция по n. Очевидно $\mathcal{A}(m, 1)$ е разрешим. Нека $n = 2^l + A > 1$, $0 < A < 2^l$ и $\mathcal{A}(m, n')$ е разрешим за всяко $n' < n$. Можем да допуснем, че $mn \leq 2^{s(t-1)l++1}$. Когато $n \leq 2^s - 1$ твърдението следва от Лема 4.3.4 и Лема 4.3.2.

Нека $n > 2^s - 1$ (т.е. $l > s > 1$). Ако $A \leq 2^{l-1} + 2^{l-2} + \cdots + 2^{l-s+1}$, то $2^{s(t-1)+l} < mn < 2^{s(t-1)+l+l}$. От Лема 4.3.3 сега следва, че правоъгълникът

$\mathcal{A}(m, 2^{l-s-1}(2^s-1))$ е разрешим. Сега от Лема 4.3.2 следва, че $\mathcal{A}(m,n)$ е също разрешим.

Остава да разгледаме случая $A > 2^{l-1} + 2^{l-2} + \cdots + 2^{l-s+1}$. Задаваме следните st въпроса докато не получим отговор "да„.

$$\mathbf{q}_{\alpha s+\beta} = \left(\sum_{i=0}^{\alpha} 2^{s(t-i-1)}, \sum_{j=1}^{\beta} 2^{s(l-j+1)} \right),$$

$alpha = 0, 1, \ldots, t-1$ и $\beta = 1, 2, \ldots, s$. Да допуснем, че отговорът на въпроса $\mathbf{q}_{\alpha_0 s+\beta_0}$ е "да„.

Това означава, че $\mathbf{x}$ се съдържа в правоъгълник с размери $2^{s(t-\alpha_0-1)} \times 2^{l-\beta_0+1}$ и следователн оможе да бъде намерен с $s(t-\alpha_0-1)+l-\beta_0+1$ въпроса. Тогава общият брои въпроси е $s(t-1)+l+1$ и правоъгълникът е разрешим.

Ако отговорът на всички въпроси е "не„, то $\mathbf{x}$ се съдържа в правоъгълник с размери $m \times n'$, където $n' = n - 2^{l-s+1}(2^s-1)$, който според индукционната хипотеза е разрешим. Остава да пресметнем броя на използваните въпроси. Тъй като

$$mn' = mn - m2^{l-s+1}(2^s-1) \leq 2^{s(t-1)+l+1} - 2^{l-s+1}(2^{st}-1) = 2^{l-s+1},$$

то $\mathbf{x}$ може да бъде намерен с $st + (l-s+1) = s(tt-1)+l+1$ въпроса. Това означава, че разглежданият правоъгълник е разрешим. □

В тази част ще докажем, че за подходящи стойности на m съществуват безбройно много стойности на n, за които правоъгълник $\mathcal{A}(m,n)$ е неразрешим.

Дефиниция 4.3.2. Нека $\mathcal{A}(m,n)$ е правоъгълник, за който $\lceil \log m + \log n \rceil \neq \lceil \log m \rceil + \lceil \log n \rceil$. Под *недостиг* на $\mathcal{A}(m,n)$ разбираме числото

$$d(m,n) = 2^{\lceil \log_2 mn \rceil} - mn.$$

Нека неизвестния елемент е $\mathbf{x}$ и сме задали въпросите $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_s$. Нека отговорите на тези въпроси са $i_1, i_2, \ldots, i_s,\ i_j \in \{0,1\}$(0 означава не, а 1 означава да). С $S^{i_1,i_2,\ldots,i_s}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_s}$ означаваме множеството от онези елементи на $\mathcal{A}(m,n)$, за които отговорите на въпроси $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_s$ са точно $i_1, i_2, \ldots, i_s$. Ясно е, че ако $\mathcal{A}(m,n)$ е разрешим, то за $\mathbf{q}_1 = (\alpha_1, \alpha_2)$ е изпълнено

$$\alpha_1\alpha_2 = |S_1^{\mathbf{q}_1}| \leq 2^{\lceil \log_2 mn \rceil - 1}$$

$$mn - \alpha_1\alpha_2 = |S_0^{\mathbf{q}_1}| \leq 2^{\lceil \log_2 mn \rceil - 1}.$$

Следователно $2^{\lceil \log_2 mn \rceil - 1} - d(m,n) \leq \alpha_1\alpha_2 \leq 2^{\lceil \log_2 mn \rceil - 1}$.

Като използваме естествените ограничения $1 \leq \alpha_1 \leq m$ и $1 \leq \alpha_2 \leq nm$, можем да намерим всички начални въпроси чрез разглеждане на разлагането на прости множители на числата

$$2^{\lceil \log_2 mn \rceil - 1} - d(m,n), 2^{\lceil \log_2 mn \rceil - 1} - d(m,n) + 1, \ldots, 2^{\lceil \log_2 mn \rceil - 1}.$$

Както по-горе можем да дефинираме *недостиг* за множеството $S^{i_1,i_2,\ldots,i_s}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_s}$, като

$$d^{i_1,i_2,\ldots,i_s}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_s} = 2^{\lceil \log_2 mn \rceil - s} - |S^{i_1,i_2,\ldots,i_s}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_s}|.$$

От очевидното равенство

$$S^{i_1,i_2,\ldots,i_{s-1}}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_{s-1}} = S^{i_1,i_2,\ldots,i_{s-1},0}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_{s-1},\mathbf{q}_s} \cup S^{i_1,i_2,\ldots,i_{s-1},1}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_{s-1},\mathbf{q}_s}$$

получаваме

$$d^{i_1,i_2,\ldots,i_{s-1}}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_{s-1}} = d^{i_1,i_2,\ldots,i_{s-1},0}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_{s-1},\mathbf{q}_s} + d^{i_1,i_2,\ldots,i_{s-1},1}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_{s-1},\mathbf{q}_s}.$$

В частност имаме $d^0_{\mathbf{q}_1} + d^1_{\mathbf{q}_1} = d(m,n)$. Следователно всеки алгоритъм, който намира неизвестния елемент $\mathbf{x} \in \mathcal{A}(m,n)$ за $\lceil \log_2 mn \rceil$ въпроса, трябва да има неотрицателен *недостиг* за всяко множество $S^{i_1,i_2,\ldots,i_s}_{\mathbf{q}_1,\mathbf{q}_2,\ldots,\mathbf{q}_s}$, за всяко $s \leq \lceil \log_2 mn \rceil$ и всяка s-орка от нули и единици $(i_1, i_2, \ldots, i_s)$.

Лема 4.3.5. Нека $m = 2^{l_1} + A$, $n = 2^{l_2} + B$, $A < 2^{l_1}$, $B < 2^{l_2}$ и първите два въпроса са $\mathbf{q}_1 = (2^{l_1}, 2^{l_2})$, $\mathbf{q}_2 = (\alpha_1, \alpha_2)$, като $\alpha_1 > 2^{l_1}$ и $\alpha_2 > 2^{l_2}$. Тогава

$$|S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| \neq 2^{l_1+l_2-1}.$$

Доказателство. За допуснем, че $|S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| = 2^{l_1+l_2-1}$. Да забележим, че α_1 и α_2 не са степени на двойката и следователно всяко от тях има нечетен делител. От друга страна е изпълнено равенството

$$\alpha_1\alpha_2 = |S^1_{\mathbf{q}_1} \cup S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| = 3.2^{l_1+l_2-1}.$$

Това означава, че в $\alpha_1\alpha_2$ има най-много един нечетен делител, което е противоречие. □

Следващата теорема определя един безкраен клас от неразрешими правоъгълници.

Теорема 4.3.2. Нека $m = 2^{l_1} + A$, $2^{l_1-2} + 2^{l_1-3} \leq A < 2^{l_1-1}$ е нечетно число и

$$k = \text{НОК}\left\{r_u | \frac{m}{2} < u \leq m, u - \text{ odd }\right\}, \tag{4.1}$$

където r_u и r са редовете на 2 съответно в $\mathbb{Z}^\star_u$ и $\mathbb{Z}^\star_m$. Тогава правоъгълникът $\mathcal{A}(m,n)$ за $n = \frac{2^{\alpha kr-1}}{m}$ е неразрешим за всяко $\alpha \in \mathbb{N}$.

Доказателство. Първият въпрос $\mathbf{q}_1 = (\alpha_1, \alpha_2)$ трябва да изпълнява условието $\alpha_1\alpha_2 = 2^{\alpha kr-1}$ или $\alpha_1\alpha_2 = 2^{\alpha kr-1} - 1$. Тъй като α_1 е нечетно и $\frac{m}{2} < \alpha_1 \leq m$. От $2^{\alpha kr-1} \equiv 1 \pmod{\alpha_1}$ следва, че $\alpha kr \equiv 1 \pmod{r_{\alpha_1}}$, което е невъзможно поради 4.1.

Следователно за първия въпрос $\mathbf{q}_1 = (\alpha_1, \alpha_2)$ имаме $\alpha_1\alpha_2 = 2^{\alpha kr-1}$. Ако $n = 2^{l_2} + B$ от условието за A имаме $2^{l_2-2} \leq B < 2^{l_2-1}$, $\alpha kr - 1 = l_1 + l_2$, $\alpha_1 = 2^{l_1}$ и $\alpha_2 = 2^{l_2}$.

Да разгледаме вторият въпрос $\mathbf{q_2} = (\beta_1, \beta_2)$. Имаме $|S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| = 2^{\alpha kr-2} - 1$ или $|S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| = 2^{\alpha kr-2}$, откъдето $\beta_1 > 2^{l_1}$ и $\beta_2 > 2^{l_2}$. Според Лема 4.3.5 имаме $|S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| \neq 2^{\alpha kr-2}$ и следователно

$$|S^1_{\mathbf{q}_1} \cup S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| = 2^{\alpha kr-1} + 2^{\alpha kr-2} - 1 = \beta_1\beta_2.$$

Това означава, че

$$3.2^{\alpha kr-2} \equiv 1 \pmod{\beta_1},$$

където $(\beta_1, 2) = (\beta_1, 3) = 1$ и $\frac{m}{2} < \beta_1 \leq m$. Ако $3 \notin \langle 2 \rangle$ в $\mathbb{Z}^\star_{\beta_1}$, то горното сравнение е невъзможно. Да допуснем, че

$$2^s \equiv 3 \pmod{\beta_1}, 0 < s < r_{\beta_1}. \tag{4.2}$$

Тогава $2^{\alpha kr+s-2} \equiv 1 \pmod{\beta_1}$. Следователно r_{β_1} дели $s-2$, което е възможно само при $s-2$. Това е противоречие с 4.2. □

4.3.1 Намиране на най-малкия неразрешим правоъгълник

Ще намерим най-малкия неразрешим правоъгълник, т.е. неразрешим правоъгълник $\mathcal{A}(m, n)$, за който произведението mn е минимално.

Лема 4.3.6. Най-малкият неразрешим правоъгълник е $\mathcal{A}(11, 93)$. Това е единственият неразрешим правоъгълник с мощност, по-малка от 1024.

Доказателство. Да разгледаме правоъгълник $\mathcal{A}(m, n)$, $m \leq n$, за който $2^{l-1} < mn \leq 2^l$. Директно се проверява, че ако нито едно от числата m и n не е от вида $\frac{2^k(2^{st}-1)}{2^s-1}$ за s положително, k и t неотрицателни цели числа,

имаме следните възможности:

$$
\begin{array}{lllll}
(A) & m = 11, & n = 11, & l = 7 \\
(B) & m = 11, & n \leq 23, & l = 8 \\
(C) & m = 13, & n \leq 19, & l = 8 \\
(D) & m = 11, & n \leq 46, & l = 9 \\
(E) & m = 13, & n \leq 39, & l = 9 \\
(F) & m = 19, & n \leq 26, & l = 9 \\
(G) & m = 22, & n \leq 23, & l = 9 \\
(H) & m = 11, & n \leq 93, & l = 10 \\
(I) & m = 19, & n \leq 53, & l = 10 \\
(J) & m = 27, & n \leq 37, & l = 10 \\
(K) & m = 29, & n \leq 35, & l = 10
\end{array}
$$

Случай (A) е разгледан в [72], като е доказано, че $\mathcal{A}(11, 11)$ е неразрешим.

За всеки от правоъгълниците $\mathcal{A}(11, 23)$, $\mathcal{A}(13, 19)$, $\mathcal{A}(13, 39)$, $\mathcal{A}(19, 53)$, $\mathcal{A}(27, 37)$ и $\mathcal{A}(29, 35)$ лесно може да се намери алгоритъм за намирането на неизвестния елемент, от който следва, че съответният правоъгълник е разрешим. Това доказва, че всеки от правоъгълниците в случаите $(B) - (G)$ и $(I) - (K)$ е разрешим.

Ще докажем, че $\mathcal{A}(11, 93)$ е неразрешим.

Нека първият въпрос е $\mathbf{q}_1 = (\alpha_1, \alpha_2)$, където $\alpha_1\alpha_2 = 511$ или 512. Следователно имаме две възможности:

$$(i)\alpha_1 = 8, \alpha_2 = 64;$$

$$(ii)\alpha_1 = 7, \alpha_2 = 73.$$

Нека вторият въпрос е $\mathbf{q}_2 = (\beta_1, \beta_2)$.

(i) $|S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| = 255$ или 256. Следователно $\beta_1 > \alpha_1$ и $\beta_2 > \alpha_2$. От Лема 4.3.5 следва, че $|S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| = 255$ и $|S^{0,0}_{\mathbf{q}_1,\mathbf{q}_2}| = 256$. Оттук получаваме, че е изпълнено

$1023 - \beta_1\beta_2 = 256$ за $8 < \beta_1 \leq 11$ и $64 < \beta_2 \leq 93$. Тъй като такива β_1 и β_2 не съществуват, случай (i) е невъзможен.

(ii) Трябва да е изпълнено $|S^{0,1}_{\mathbf{q}_1,\mathbf{q}_2}| = 256$ и единствената възможност е $\beta_1 = 11$ и $\beta_2 = 64$. Нека $\mathbf{q}_3 = (\gamma_1, \gamma_2)$ е третият въпрос. Тогава имаме $|S^{0,0,0}_{\mathbf{q}_1,\mathbf{q}_2\mathbf{q}_3}| = 128$. Това е възможно само когато $\gamma_1 > 7$ и $\gamma_2 > 73$. Следователно

$$128 = 29.11 - \gamma_1(\gamma_2 - 64),$$

откъдето $\gamma_1(\gamma_2 - 64) = 191$, което е невъзможно.

Да отбележим, че правоъгълникът $\mathcal{A}(11, 92)$ е разрешим понеже $92 = 4.23$ и $\mathcal{A}(11, 23)$ е разрешим. □

4.3.2 Намиране на най-малкия неразрешим квадрат

В [72] е доказано, че квадратите $\mathcal{A}(5, 5)$, $\mathcal{A}(11, 11)$ и $\mathcal{A}(45, 45)$ са разрешими. Този факт, заедно с Лема 4.3.2 и Лема 4.3.3 дават, че всички квадрати $\mathcal{A}(n, n)$ за $n \leq 180$ са разрешими. Следователно първият нерешен случай е $\mathcal{A}(181, 181)$.

Теорема 4.3.3. Квадратът $\mathcal{A}(181, 181)$ е неразрешим.

Доказателство. Като използваме, че $d(181, 181) = 7$ можем да намерим всички възможности за първите два въпроса. Получаваме следните 13 въз-

можности:

$$
\begin{aligned}
&1A) \quad \mathbf{q}_1 = (140, 117) \quad \mathbf{q}_2 = (128, 181)\\
&1B) \quad \mathbf{q}_1 = (140, 117) \quad \mathbf{q}_2 = (130, 180)\\
&2A) \quad \mathbf{q}_1 = (156, 105) \quad \mathbf{q}_2 = (117, 175)\\
&2B) \quad \mathbf{q}_1 = (156, 105) \quad \mathbf{q}_2 = (126, 170)\\
&2C) \quad \mathbf{q}_1 = (156, 105) \quad \mathbf{q}_2 = (128, 169)\\
&2D) \quad \mathbf{q}_1 = (156, 105) \quad \mathbf{q}_2 = (130, 168)\\
&3A) \quad \mathbf{q}_1 = (159, 103) \quad \mathbf{q}_2 = (128, 167)\\
&4A) \quad \mathbf{q}_1 = (180, 91) \quad \mathbf{q}_2 = (91, 181)\\
&4B) \quad \mathbf{q}_1 = (180, 91) \quad \mathbf{q}_2 = (105, 169)\\
&4C) \quad \mathbf{q}_1 = (181, 91) \quad \mathbf{q}_2 = (117, 161)\\
&4D) \quad \mathbf{q}_1 = (181, 91) \quad \mathbf{q}_2 = (126, 156)\\
&4E) \quad \mathbf{q}_1 = (181, 91) \quad \mathbf{q}_2 = (128, 155)\\
&4F) \quad \mathbf{q}_1 = (181, 91) \quad \mathbf{q}_2 = (130, 154)
\end{aligned}
$$

Ще разгледаме някои от случаите.

3A) Имаме $e^{0,0}_{\mathbf{q}_1,\mathbf{q}_2} = 0$, което означава, че $|S^{0,0,i}_{\mathbf{q}_1,\mathbf{q}_2\mathbf{q}_3}| = 2^{12}$ за $i = 0, 1$. За да определим възможностите за третия въпрос да разделим множеството $S^{0,0}_{\mathbf{q}_1,\mathbf{q}_2}$ по следния начин:

$$S^{0,0}_{\mathbf{q}_1,\mathbf{q}_2} = \cup_{i=1}^{6} \mathcal{T}_i,$$

където множествата $\mathcal{T}_i$ за $i = 1, 2, \ldots, 6$ са дефинирани последния начин:

$$
\begin{aligned}
\mathcal{T}_1 &= \{(a, b) | 128 < a \leq 181; 0 < b \leq 103\}\\
\mathcal{T}_2 &= \{(a, b) | 128 < a \leq 159; 103 < b \leq 167\}\\
\mathcal{T}_3 &= \{(a, b) | 159 < a \leq 181; 103 < b \leq 167\}\\
\mathcal{T}_4 &= \{(a, b) | 0 < a \leq 128; 167 < b \leq 181\}\\
\mathcal{T}_5 &= \{(a, b) | 128 < a \leq 159; 167 < b \leq 181\}\\
\mathcal{T}_6 &= \{(a, b) | 159 < a \leq 181; 167 < b \leq 181\}.
\end{aligned}
$$

Въпрос $\mathbf{q}_3$ не може да бъде в $\mathcal{T}_1$, $\mathcal{T}_2$ или $\mathcal{T}_4$, защото $|S^{0,0,1}_{\mathbf{q}_1,\mathbf{q}_2\mathbf{q}_3}| \leq |\mathcal{T}_i| < 2^{12}$ за $i = 1, 2, 4$.

Също така $\mathbf{q}_3$ не може да бъде в $\mathcal{T}_5$ поради Лема 4.3.5. Ако $\mathbf{q}_3 \in \mathcal{T}_6$, то имаме

$$181^2 - \alpha_1\alpha_2 = 2^{12},$$

което уравнение няма решение за $159 < \alpha_1 \leq 181$ и $167 < \alpha_2 \leq 181$.

Ако $\mathbf{q}_3 \in \mathcal{T}_3$, то имаме

$$|S^{0,0,1}_{\mathbf{q}_1,\mathbf{q}_2\mathbf{q}_3}| = (\alpha_1 - 159)\alpha_2 + (\alpha_2 - 103)32 = 2^{12}$$

което уравнение няма решение за $159 < \alpha_1 \leq 181$ и $103 < \alpha_2 \leq 167$.

2B) Имаме $e^{0,0}_{\mathbf{q}_1,\mathbf{q}_2} = 1$, което означава, че $|S^{0,0,i}_{\mathbf{q}_1,\mathbf{q}_2\mathbf{q}_3}| = 2^{12} - 1$ ила на 2^{12} за $i = 0, 1$. Както в случай 3A) разделяме множеството $S^{0,0}_{\mathbf{q}_1,\mathbf{q}_2}$ за $i = 0, 1$, на същите 6 множества. Проверявайки всяко от тях, както в предишния случай, намираме, че единствената възможност е $\mathbf{q}_3 = (171, 161)$. Лесно се проверява, че $|e^{0,0,0}_{\mathbf{q}_1,\mathbf{q}_2\mathbf{q}_3}| = 0$ и какъвто и да е четвъртия въпрос $\mathbf{q}_4 = (\beta_1, \beta_2)$, трябва да имаме $|\, S^{0,0,0,i}_{\mathbf{q}_1,\mathbf{q}_2\mathbf{q}_3,\mathbf{q}_4} \,| = 2^{11}$ за $i = 0, 1$. Първо да забележим, че $126 < \beta_1 \leq 181$ и $170 < \beta_2 \leq 181$. Директна проверка показва, че не съществува четвърти въпрос $\mathbf{q}_4$, за който $|\, S^{0,0,0,1}_{\mathbf{q}_1,\mathbf{q}_2\mathbf{q}_3,\mathbf{q}_4} \,| = 2^{11}$.

Останалите случаи се доказват по аналогичен начин. □

Теорема 4.3.3 определя най-малкия неразрешим квадрат. Не е известно дали съществуват безбройно много неразрешими квадрати.

Библиография

[1] T. Baicheva and E. Kolev, Binary Codes of Length Eight, Minimum Distance Three and Twenty Codewords, Proc. of the International Workshop on Optimal Codes, June 9-15, Sozopol, Bulgaria, 1998, 5-8.

[2] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko and N. J. A. Sloane and W. D. Smith, Bounds for binary code of length less than 25 , *IEEE Trans. Inform. Theory*, 24, 1978, 81-93.

[3] M. R. Best, Binary codes with a minimum distance of four *IEEE Trans. Inform. Theory*, 26, 1980, 738-742.

[4] A. Blokhuis and C. W. H. Lam, More coverings by rook domains, *J. Comnin. Theory, Ser. A* 36, 1984, 240-244.

[5] D. Brink, The inverse Football pool problem, *Journal of Integer Sequences* 14, article 11.8.8

[6] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, A new table of constant weight codes , *IEEE Trans. Inform. Theory*, 36, 1990, 1334-1380.

[7] W. A. Carnielli, On covering and coloring problems by rook domains,*Discrete Mathematics,* 57, 1985, 9-16.

[8] W. Chen and I. S. Honkala, Lower bounds for q-ary covering codes, *IEEE Trans. Infrom. Theory,* 36, 1990, 664-671.

[9] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering codes*, Amsterdam, The Netherlands: North-Holland, 1997.

[10] G. D. Cohen, M. G. Karpovsky, H. F. Matson, Jr., and J. R. Schatz, Covering radius – survey and recent results, *IEEE Trans. Inform. Theory* 32, 1985, 328-343.

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

[12] G. D. Cohen, S. N. Litsyn, A. C. Lobstein and H. F. Mattson, Jr, Covering Radius 1985-1994, *Applicable Algebra in Engineering, Comunication and Computing,* vol.8, No.3, 1997, 173-239.

[13] J. Czyzowicz, D. Mundici and A. Pelc, Ulam's Searching Game With Lies , *J. Combin. Theory Ser. A* 52 1989, 62-76.

[14] N. Dichev, E. Kolev, Nonadaptive search with a lie, *Ninth International Workshop, Algebraic and Combinatorial Coding theory*, June 19-25, Kranevo, Bulgaria, 2004, 120-124.

[15] N. Dichev, E. Kolev, Search with a lie, *International congress MASSEE 2003* September 15-21, Bulgaria, 2003.

[16] B. Elspas, A conjecture on binary nongroup codes,*IEEE Trans. Inform. Theory*, 11, 1965, 599-600.

[17] T. Etzion and G. Greenberg, Construction for perfect mixed codes and other covering codes, *IEEE Trans. Inform. Theory* 39, 1993, 209-214.

[18] R. I. Graham, N. J. A. Sloane, On the covering radius of codes, *IEEE Trans. Inform. Theory* 31(3), 1985, 385-401.

[19] H. O. Hämäläinen, S.Rankinen, Upper bounds for football pool problems and mixed covering codes, *J. Combin. Theory Ser.A*, 56, 1991, 84-95.

[20] H. Hämäläinen, I. Honkala, S. Litsyn, P. Östergård, Football Pools – A Game for Mathematicians, *The American Mathematical Monthly*, 102(7), 1995.

[21] I. S. Honkala, Modified bounds for covering codes, *IEEE Trans. Inform. Theory* 34, 1988, 1343-1344.

[22] I. S. Honkala, Lower bounds for binary covering codes, *IEEE, Trans. Inform. Theory,* 34 (2), 1988, 326-329.

[23] I. S. Honkala, Modified bounds for covering codes, *IEEE Trans. Inform. Theory,* 37(2), 1991, 352-365.

[24] I. Honkala, Lower bounds for binary covering codes, *IEEE Trans. Inform. theory*, 34, 1988, 326-329.

[25] R. Hill, A first course in Coding Theory, *Clarendon press*, Oxford, 1986.

[26] R. Hill and J. P. Karim, Searching With lies: the Ulam Problem, *Discrete Mathematics,* 106-107, 1992, 273-283.

[27] D. Julin, Two improved block codes, *IEEE Trans. Inform. Theory* 11, 1965, 459.

[28] M. Kaikkonen, Codes from affine permutation groups, *Des. Codes Cryptogr.,*15, 1999, 183-184.

[29] H. J. I. Kamps and J. H. van Lint, A covering Problem, *Colloq. Math. Soc. Janos Bolyai; Hung. Combin. Theory and Appl.,* Balantonfüred, Hungary, 1969, 679-685.

[30] G. O. H. Katona, Renýi and the combinatorial search problems, *Periodica Math. Hungar*

[31] G. Kéri, On the covering radius of small codes, *Journal Studia Scientiarum Mathematicarum Hungarica*, 40(1-2), 2003, 242-256.

[32] G. Kéri, P. R. J. Östergård, Further results on the covering radius of small codes, *Discrete Mathematics*, Volume 307, Issue 1, 6 January 2007, pp. 69Ц77.

[33] S. Kapralov, Enumeration of some Dyson sets, *Twelfth International Workshop on Algebraic and Combinatorial Coding Theory*, September 5-11, 2010, Akademgorodok, Novosibirsk, Russia pp. 178-181.

[34] Y. Klein, S. Litsyn and A. Vardy, Two new bounds on the size of binary codes with a minimum distance of 3 , *Des. Codes Cryptogr.,* 6, 1995, 219-227.

[35] E. Kolev, An Improved Upper Bound on $A_2(10,3)$, *Fifth International Workshop on Algebraic and Combinatorial Coding theory*, Pskov, Russia, September 6-12, 1998, 155-157.

[36] E. Kolev, R. Hill, An Improved Lower Bound on the covering number $K_2(9,1)$, *Discrete Mathematics* 197/198, 1999, 483-489.

[37] E. Kolev, Mixed Covering Codes with Two Binary and Four Ternary Coordinates, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lecture Notes in Computer Science, vol. 948, 1995, 312-322

[38] E. Kolev, A $(9;56)1$ binary code does not exist, *CR Acad. Bulg. Sci.*, 51(11-12), 1998, 25Ц28.

[39] E. Kolev, Codes over GF(3) of Length 5, 27 Codewords and Covering Radius 1, *Journal of Combinatorial Designs*, 1(4), 1993, 265-275.

[40] E. Kolev, Nonadaptive Search with Sets of Given Sum, *Eight International Workshop Algebraic and Combinatorial Coding theory*, September 8-14, Tsarskoe Selo, Russia, 2002, 159-161.

[41] E. Kolev, Equivalent Codes and Backtrack Search, *Swedish-Bulgarian Government IT Security Conference Information Security in the 21th Century: Global Convergence*, September 18-24, Bansko, Bulgaria, 1999, 23-26.

[42] E. Kolev, On nonadaptive search problem, *Serdica Math. J.* 29, 2003, 361-376.

[43] E. Kolev, Nonadaptive Search Problem with Sets of Equal Sum, *Central European Journal of Mathematics*, 1(3), 2003, 272-283.

[44] E. Kolev, A search problem and cyclic codes of odd length, *Fourth International Workshop, Optimal Codes and related topics*, June 17-23, Pamporovo, Bulgaria, 2005, 201-204.

[45] E. Kolev, Nonadaptive Search Problem in Weighted Set, *Eight International Workshop, Algebraic and Combinatorial Coding Theory*, September 3-9, Zvenigorod, Russia, 2006, 147-150.

[46] E. Kolev, Nonadaptive search problem in sets with four weights, *Fifth International Workshop Optimal Codes and related Topics*, June 16-22, White Lagoon, Bulgaria, 2007, 132-135.

[47] E. Kolev, Nonadaptive search for two elements with sets of equal sum, *Fifth International Workshop, Optimal Codes and related topics*, June 16-22, Varna, Bulgaria, 2009.

[48] E. Kolev, How to have a wrong bet in football pools, *CR Acad. Bulg. Sci.*, 66(3) 2013, 315-320.

[49] E. Kolev, I. Langev, On Some Mixed Covering Codes of Small Length, *Lecture Notes in Computer Science,* Springer-Verlag, 781, 1994, 38-50.

[50] E. Kolev, Proper integers for search with a lie, *Thirteenth International Workshop Algebraic and Combinatorial Coding Theory*, June 15-21, Pomorie, Bulgaria, 2012, 188-191.

[51] E. Kolev, T. Baicheva, About the inverse football pool problem for 9 games, *Seventh International Workshop, Optimal Codes and related topics*, September 6-12, Albena, Bulgaria, 2013.

[52] E. Kolev, T. Baicheva, Minimal coverings of $\{0,1,2\}^n$ with spheres of radius n, accepted for publication in *Utilitas Mathematica*.

[53] I. Landgev, E. Kolev, On a Two Dimensional Search Problem, *Serdica Math. J.*, 21(3), 1995, 219-230.

[54] J. H. van Lint, Jr., G. J. M. van Wee, Generalized bounds on binary/ternary mixed packing and covering codes, *J. Combin. Theory Ser.A* 57, 1991, 130-134.

[55] S. Litsyn and A. Vardy, The uniquenes of Best code ,*IEEE Trans. Inform. Theory*, 40, 1994, 1693-1698.

[56] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* Amsterdam, The Netherlands: North-Holland, 1977.

[57] B. D. McKay, nauty users's guide (version 1.5), *Comp. Sci. Dept. Australian Nat. Univ. Tech. Rep.* TR-CS-90-02, 1990.

[58] P. R. J. Östergård, New multiple covering codes by tabu search, *Australasian Journal of Combinatorics,* 12, 1995, 145-155.

[59] P. R. J. Östergård, A combinatorial proof for the football pool problem for six matches, *Journal of Combinatorial Theory, A* 76, 1996, 160-163.

[60] P. R. J. Östergård, Constructing covering codes by tabu search, *Journal of Combinatorial designs,* 5, 1997, 71-80.

[61] P. R. G. Östergård, T. Baicheva, E. Kolev, Optimal Binary One-Error-Correcting Codes of Length 10 Have 72 Codewords, *IEEE Trans on Inf. Theory,* 45(4), 1999, 1229-1231.

[62] P. R. J. Östergård, A coloring problem in Hamming spaces, *Europ. J. Combinatorics,* 18, 1997, 303-309.

[63] P. R. J. Östergård, On the structure of optimal error-correcting codes, *Discrete Mathematics,* 179, 1998, 285-287.

[64] P. R. J. Östergård and T. Riihonen, A covering problem for tori, *Ann. Comb.*, 7, 2003, 357-363.

[65] P. R. J. Östergård, Construction of mixed covering codes, *Research Report A18, Digital Systems Laboratory, Helsinki University of Technology*, 1991

[66] P. R. J. Östergård, New upper bounds for binary|ternary mixed covering codes, *Research Report A22, Digital Systems Laboratory, Helsinki University of Technology*, 1993

[67] P. R. J. Östergård, A new binary code of length 10 and covering radius 1, *IEEE Trans. Inform. Theory,* 37(6), 1991, 179-1805

[68] P. R. J. Östergård, Upper bounds for q-ary covering codes, *IEEE Trans. Inform. Theory,* 37(3), 1991, 660-664.

[69] P. R. J. Östergård, A new table of binary/ternary mixed covering codes, *Designs, codes and cryptography,* 11, 1997, 151-178.

[70] P. R. J. Östergård, Blass, U., On the size of optimal binary codes of length 9 and covering radius 1, *IEEE - Information Theory,* 47(6), 2001, 2556-2557,

[71] T. Riihonen, How to gamble 0 correct in football pools, *Helsinki university of thechnology,* 2002. Available at http://users.tkk.fi/priihone/tuotokset.html

[72] M. Ruszinko, On a 2 and 3-dimensional search problem,*Proc. of the Sixth Joint Swedish – Russian Workshop on Inf. Theory,* Mölle, Swede, Aug. 21-27, 1993, 437-440.

[73] N. J. A. Sloane, The on-line encyclopedia of integer sequences, htpp://www.research.att.com/njas/sequences/

[74] J. Spencer, Guess a Number-With Lying, *Math. Mag.* 57, 1984, 105-108.

[75] N. Wax, On upper bounds for error-detecting and error-correcting codes of finite length, *IRE Trans. Infrom. Theory,* 5, 1959, 168-174.

[76] G. J. M. van Wee, Improved sphere bounds on the covering radius of codes, *J. Combin. Theory Ser.A*, 1991, 117-129.

[77] G. J. M. van Wee, On the non-existence of certain perfect mixed codes, *Discrete Mathematics,* 87, 1991, 323-326.

[78] L. T. Wille, Improved binary code coverings by simulated annealing, *Congressus Numerantium*, 73, 1990, 53-58.

[79] L. T. Wille, New binary covering codes obtained by simulated annealing, *IEEE Trans.Inf.Theory*, 42, 1996, 300-302.

[80] L. T. Wille, The football pool problem for 6 matches: A new upper bound obtained by simulated annealing, *J. Combin. Theory Ser. A*, 45, 1987, 171-177.

[81] S. K. Zaremba, Covering problems concerning abelian groups, *J. London Math. Soc.*, 27, 1952, 242-246.

Публикации по дисертацията

[P1] E. Kolev, I. Langev, On Some Mixed Covering Codes of Small Length, *Lecture Notes in Computer Science,* Springer-Verlag, 781, 1994, 38-50.

[P2] I. Landgev, E. Kolev, On a Two Dimensional Search Problem, *Serdica Math. J.*, 21(3), 1995, 219-230.

[P3] E. Kolev, Mixed Covering Codes with Two Binary and Four Ternary Coordinates, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lecture Notes in Computer Science, vol. 948, 1995, 312-322

[P4] T. Baicheva and E. Kolev, Binary Codes of Length Eight, Minimum Distance Three and Twenty Codewords, Proc. of the International Workshop on Optimal Codes, June 9-15, Sozopol, Bulgaria, 1998, 5-8.

[P5] E. Kolev, A $(9; 56)1$ Binary Code does not Exist, *CR Acad. Bulg. Sci.*, 51(11-12), 1998, 25-28.

[P6] E. Kolev, An improved upper bound on $A_2(10, 3)$, *Fifth International Workshop on Algebraic and Combinatorial Coding theory*, Pskov, Russia, September 6-12, 1998, 155-157.

[P7] E. Kolev, R. Hill, An improved lower bound on the covering number $K_2(9, 1)$, *Discrete Mathematics* 197/198, 1999, 483-489.

[P8] P. G. Östergård, T. Baicheva, E. Kolev, Optimal Binary One-Error-Correcting Codes of Length 10 Have 72 Codewords, *IEEE Trans. Inf. Theory,* 45(4), 1999, 1229-1231.

[P9] E. Kolev, Equivalent Codes and Backtrack Search, *Swedish-Bulgarian Government IT Security Conference Information Security in the 21th Century: Global Convergence*, September 18-24, Bansko, Bulgaria, 1999, 23-26.

[P10] E. Kolev, Nonadaptive search with sets of given sum, *Eight International Workshop Algebraic and Combinatorial Coding theory*, September 8-14, Tsarskoe Selo, Russia, 2002, 159-161.

[P11] E. Kolev, On nonadaptive search problem, *Serdica Math. J.* 29, 2003, 361-376.

[P12] E. Kolev, Nonadaptive Search Problem with Sets of Equal Sum, *Central European Journal of Mathematics*, 1(3), 2003, 272-283.

[P13] N. Dichev, E. Kolev, Search with a lie, *International congress MASSEE 2003* September 15-21, Bulgaria, 2003,

[P14] N. Dichev, E. Kolev, Nonadaptive search with a lie, *Ninth International Workshop, Algebraic and Combinatorial Coding theory*, June 19-25, Kranevo, Bulgaria, 2004, 120-124.

[P15] E. Kolev, A search problem and cyclic codes of odd length, *Fourth International Workshop, Optimal Codes and related topics*, June 17-23, Pamporovo, Bulgaria, 2005, 201-204.

[P16] E. Kolev, Nonadaptive Search Problem in Weighted Set, *Eight International Workshop, Algebraic and Combinatorial Coding Theory*, September 3-9, Zvenigorod, Russia, 2006, 147-150.

[P17] E. Kolev, Nonadaptive search problem in sets with four weights, *Fifth International Workshop Optimal Codes and related Topics*, June 16-22, White Lagoon, Bulgaria, 2007, 132-135.

[P18] E. Kolev, Nonadaptive search for two elements with sets of equal sum, *Fifth International Workshop, Optimal Codes and related topics*, June 16-22, Varna, Bulgaria, 2009.

[P19] E. Kolev, Proper integers for search with a lie, *Thirteenth International Workshop Algebraic and Combinatorial Coding Theory*, June 15-21, Pomorie, Bulgaria, 2012, 188-191.

[P20] E. Kolev, How to have a wrong bet in football pools, *CR Acad. Bulg. Sci.*, 66(3) 2013, 315-320.

[P21] E. Kolev, T. Baicheva, About the inverse football pool problem for 9 games, *Seventh International Workshop, Optimal Codes and related topics*, September 6-12, Albena, Bulgaria, 2013.

[P22] E. Kolev, T. Baicheva, Minimal coverings of $\{0,1,2\}^n$ with spheres of radius n, accepted for publication in *Utilitas Mathematica*.

Списък на цитирания

1. E. Kolev, I. Langev, On Some Mixed Covering Codes of Small Length, *Lecture Notes in Computer Science,* Springer-Verlag, 781, 1994, 38-50.

   1 P. R. J. Östergård, H. Hämäläinen, A new table of binary|ternary mixed covering codes, *Designs, codes and cryptography*, 11(2), 1997, 151-178.

   2 G. D. Cohen, S. N. Litsyn, A. C. Lobstein, N. F. Matson, Jr., Covering Radius 1984-1995, *Department Informatique, Ecole Nationale Supérieure des Télécommunications, 94 D025.*

   3 G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, Covering codes, North Holland Mathematical library, North Holland, 1997.

   4 G. D. Cohen, S. N. Litsyn, A. C. Lobstein, N. F. Matson, Jr., Covering Radius 1984-1995, *Applicable Algebra in Engineering, Communication and Computing,* 8, 1977, 173-239.

   5 V. Pless, W. C. Huffman, Handbook on coding theory.

   6 R. A. Brualdi, S. Litsyn, V. Pless, Covering codes, Handbook on coding theory, North-Holland 1998, 755-826.

   7 G. Kéri, On the covering radius of small codes, *Journal Studia Scientiarum Mathematicarum Hungarica*, 40(1-2), 2003, 242-256.

   8 G. Kéri, P. R. J. Östergård, Further results on the covering radius of small codes, *Discrete Mathematics*, Volume 307, Issue 1, 6 January 2007, pp. 69-77.

2. I. Landgev, E. Kolev, On a Two Dimensional Search Problem, *Serdica Math. J.*, 21(3), 1995, 219-230.

   1 Miklós Ruszinkó, Gabor Tárdos, On a search problem in multidimensional grids, *Journal of Statistical Planning and Inference*, 59(1), 1997, 101-109.

3. E. Kolev, Mixed Covering Codes with Two Binary and Four Ternary Coordinates, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lecture Notes in Computer Science, vol. 948, 1995, 312-322

    1 G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, Covering codes, North Holland Mathematical library, North Holland, 1997.

4. T. Baicheva, E. Kolev, Binary Codes of Length Eight, Minimum Distance Three and Twenty Codewords, Proc. of the International Workshop on Optimal Codes, June 9-15, Sozopol, Bulgaria, 1998, 5-8.

    1 Petteri Kaski, P. G. Östergård, Classification algorithms for codes and designs, Springer, book, 2006

    2 Rix, James Gregory, Hypercube coloring and the structure of binary codes, *Master of Science Thesis*, University of British Colombia, 2008.

    3 D. Sverdlov, Coloring Hamming graphs, Diplomatbeit vorgelegt, Technishen Universität Berlin, 2009.

    4 D. S. Krotov, P.R.J. Östergärd, O. Pottonen, On Optimal Binary One-Error-Correcting Codes of Lengths 2^m-4 and 2^m-3, *IEEE Transactions on Inf. Theory*, 57(10), 2011, 6771 - 6779.

5. E. Kolev, A $(9; 56)1$ Binary Code does not Exist, *CR Acad. Bulg. Sci.*, 51(11-12), 1998, 25-28.

    1 P.R.J. Östergård, P.R.J. Blass, U. , On the size of optimal binary codes of length 9 and covering radius 1 *IEEE - Information Theory* 47(6), 2001, 2556-2557.

6. E. Kolev, An improved upper bound on $A_2(10, 3)$, *Fifth International Workshop on Algebraic and Combinatorial Coding theory*, Pskov, Russia, September 6-12, 1998, 155-157.

7. E. Kolev, R. Hill, An improved lower bound on the covering number $K_2(9,1)$, *Discrete Mathematics* 197/198, 1999, 483-489.

8. P. G. Östergård, T. Baicheva, E. Kolev, Optimal Binary One-Error-Correcting Codes of Length 10 Have 72 Codewords, *IEEE Trans. Inf. Theory,* 45(4), 1999, 1229-1231.

1 J. H. Conway, N. J. A. Sloane, *Sphere packings, lattices and groups,* Springer Verlag, 1998.

2 P. Simons, Extending the Stable Model Semantics with More Expressive Rules, *Lecture Notes in Computer Science*, Vol. 1730, pp. 305-316, 1999.

3 Г. Богданова, *Граници за оптимални кодове,* Докторска дисертация, 2000 г.

4 P. Simons, *Extending and implementing the stable model semantics*, Research report 58, Helsinki University of Technology, Helsinki, Finland, 2000.

5 K. Kapralov, Optimal quaternary two-error-correcting codes of length 7 have 32 codewords, *Mathematics and Education in Mathemaitics*, pp. 179-183, 2000.

6 G. Bogdanova, S. Kapralov, Bounds for codes over small alphabets, *Mathematics and education in Mathematics,* pp. 149-154, 2000.

7 K. Kapralov, The nonexistence of ternary $(10, 15, 7)$ codes, *Proc. of Intern. Workshop ACCT,* Bansko, Bulgaria, pp. 189-192, 2000.

8 P. Simons, *Extending and implementing the stable model semantics*, Dissertation of the degree Doctor of Technology, Helsinki University of Technology, 2000.

9 E. Agrell, A. Vardy and K. Zeger, A table of upper bounds for binary codes, *IEEE Trans. on Inf. Theory,* vol. 47, pp. 3004-3006, 2001.

10 Petteri Kaski, Isomorph-free exhaustive generation of combinatorial designs, *Research report A70*, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, December, 2001.

11 I. Bouyukliev, Maximal cliques in graphs and some new upper bounds for constant-weight codes, *Proc. of International Workshops on Groups and Graphs,* Varna, Bulgaria, pp. 19-22, 2002.

12 M. Letourneau and S. Houghten, *Optimal Ternary (10,7) Codes,* Technical Report # CS-02-10, Department of Computer Science, Brock University, St. Catharines, Ontario, Canada, September, 2002.

13 M. Letourneau and S. Houghten, *Optimal Ternary (11,7) and (14,10) Codes,* Technical Report # CS-02-20, Department of Computer Science, Brock University, St. Catharines, Ontario, Canada, September, 2002.

14 A. Trachtenberg and A. Vardy, Full-rank tilings of F_2^8 do not exist, *SIAM Journal of Discrete Mathematics*, 16(3), pp. 390-392, 2003.

15 Ст. Капралов, *Граници, конструкции и клрасификация на оптимални кодове,* Дисертация за присъждане на научната степен „Доктор на математическите науки “, 2004.

16 Juergen Bierbrauer, *Introduction to Coding Theory*, Publisher: Chapman& Hall/CRC, 2004.

17 S.K. Houghten, D. Ashlock and J. Lennarz Bounds on Optimal Edit Metric Codes, *Technical Report # CS-05-07*, Brock University, July, 2005.

18 Petteri Kaski, *Algorithms for Classification of Combinatorial Objects*, Ph. D. Helsinki University Schools of Technology, June, 2005.

19 Bojja Neelima and Rahman Syed Mustafizur, *Upper bounds for block codes*, Master's Thesis, Department of Sygnals and Systems, Chalmers

University of Technology, Göteborg, Sweden, 2005 (Report Number EX037/2005).

20 S.K. Houghten, D. Ashlock and J. Lennarz Construction of Optimal Edit Metric Codes, *IEEE Information Theory Workshop*, Chengdu, 22-26 Oct. 2006, pp. 259-263. ISBN: 1-4244-0067-8.

21 Jay Baga, Adrian Heinz and Mahbubul Majumder, An Algorithm for Graceful Labelings of Cycles, *Congressus Numerantium*, 186 (2007), pp. 57-63.

22 M. Ghebleh, L. A. Goddyn, E. S. Mahmoodian and M. Verdian-Rizi, Silver Cubes, *Graphs and Combinatorics*, vol. 24, No 5, 2008, pp. 429-442,

23 J. Rix, *Hypercube coloring and the structure of binary codes*, Master's Thesis, The University of British Colombia, July, 2008.

24 Jacqueline Smith and D. Chris Rayner, Search Enhancements for $A(n, d)$, *CMPUT 674 Project Report*, December 10, 2008.

25 I. Chuang, A. Cross, G. Smith, J. Smolin and Bei Zeng, Codeword stabilized quantum codes: Algorithm and structure, *Journal of Math. Phys.* vol. 50, Issue 4, 2009.

26 Bei Zeng, *Quantum operations and codes beyond the Stabilizer-Clifford framework*, Ph. D. Thesis, Massachusetts Institute of Technology, 2009.

27 Olli Pottonen, *Perfect binary codes: classification and properties*, Ph. D. Helsinki University of Technology, 2009.

28 Nicolas Bitouzé, Alexandre Graell I Amat, Eirik Rosnes, Error Correcting Coding for a Non-symmetric Ternary Channel, *IEEE Trans. Inform. Theory,* vol. 56, issue 11, November 2010, pp. 5715-5729.

29 D. Brink, The inverse football pool problem, *Journal of integer sequences,* Vol. 14, Article 11.8.8, 2011.

30 Marcus Greferath, Jens Zumbragel, On the algebraic representation of certain optimal non-linear binary codes, *arXiv:1109.4770v2*, 2012.

31 Xiang, Jingen, *Scalable Scientific Computing Algorithms Using MapReduce*, Thesis, University of Waterloo, 2013.

32 I. Bouyukliev, V. Monev, M. Dzhumalieva-Stoeva, About parallelization of an algorithm for the maximum clique problem, *Seventh International Workshop, Optimal Codes and related topics*, September 6-12, Albena, Bulgaria, 2013, 53-58.

9. E. Kolev, Equivalent Codes and Backtrack Search, *Swedish-Bulgarian Government IT Security Conference Information Security in the 21th Century: Global Convergence*, September 18-24, Bansko, Bulgaria, 1999, 23-26.

10. E. Kolev, Nonadaptive search with sets of given sum, *Eight International Workshop Algebraic and Combinatorial Coding theory*, September 8-14, Tsarskoe Selo, Russia, 2002, 159-161.

11. E. Kolev, On nonadaptive search problem, *Serdica Math. J.* 29, 2003, 361-376.

12. E. Kolev, Nonadaptive Search Problem with Sets of Equal Sum, *Central European Journal of Mathematics*, 1(3), 2003, 272-283.

13. N. Dichev, E. Kolev, Search with a lie, *International congress MASSEE 2003* September 15-21, Bulgaria, 2003.

14. N. Dichev, E. Kolev, Nonadaptive search with a lie, *Ninth International Workshop, Algebraic and Combinatorial Coding theory*, June 19-25, Kranevo, Bulgaria, 2004, 120-124.

15. E. Kolev, A search problem and cyclic codes of odd length, *Fourth International Workshop, Optimal Codes and related topics*, June 17-23, Pamporovo,

Bulgaria, 2005, 201-204.

16. E. Kolev, Nonadaptive Search Problem in Weighted Set, *Eight International Workshop, Algebraic and Combinatorial Coding Theory*, September 3-9, Zvenigorod, Russia, 2006, 147-150.

17. E. Kolev, Nonadaptive search problem in sets with four weights, *Fifth International Workshop Optimal Codes and related Topics*, June 16-22, White Lagoon, Bulgaria, 2007, 132-135.

18. E. Kolev, Nonadaptive search for two elements with sets of equal sum, *Fifth International Workshop, Optimal Codes and related topics*, June 16-22, Varna, Bulgaria, 2009.

19. E. Kolev, Proper integers for search with a lie, *Thirteenth International Workshop Algebraic and Combinatorial Coding Theory*, June 15-21, Pomorie, Bulgaria, 2012, 188-191.

20. E. Kolev, How to have a wrong bet in football pools, *CR Acad. Bulg. Sci.*, 66(3) 2013, 315-320.

21. E. Kolev, T. Baicheva, About the inverse football pool problem for 9 games, *Seventh International Workshop, Optimal Codes and related topics*, September 6-12, Albena, Bulgaria, 2013.

22. E. Kolev, T. Baicheva, Minimal coverings of $\{0,1,2\}^n$ with spheres of radius n, accepted for publication in *Utilitas Mathematica*.