

ОПТИМАЛНИ РАЗДЕЛЯЩИ КОДОВЕ

OPTIMAL SUPERIMPOSED CODES

Младен Манев

Технически университет - Габрово

Abstract

This paper is a survey of results about superimposed codes and methods of construction, described in [2].

Keywords: Superimposed code; cover-free family; key distribution pattern; residual code; classification.

ВЪВЕДЕНИЕ

В настоящата работа са описани резултатите за разделящи кодове и методите за тяхното конструиране, представени в [2].

Основите на теорията на разделящите кодове са положени от Kautz и Singleton през 1964 година [5]. Различни автори изучават разделящите кодове основно от три различни гледни точки и тези три линии на проучване са почти независими една от друга. Много от резултатите са преоткривани в теория на информацията, в комбинаториката или в теория на груповото тестване. През 1985 година Erdős, Frankl и Füredi в [4] въвеждат понятието фамилия без покритие при изучаването на фамилии от крайни множества, за които никое множество не се съдържа в обединението на r от останалите множества. Това понятие може да бъде обобщено по следния начин ([8]):

Определение 1. Една фамилия $\{A_1, \dots, A_T\}$ от подмножества на множеството $[N] = \{1, \dots, N\}$ се нарича фамилия без (w, r) покритие, ако за всеки две подмножества I и J на множеството $[T] = \{1, \dots, T\}$, за които $|I| = w$, $|J| = r$ и $I \cap J = \emptyset$ е изпълнено

$$\bigcap_{i \in I} A_i \not\subset \bigcup_{j \in J} A_j.$$

Понятието фамилия без (w, r) покритие се оказва еквивалентно на въведеното през 1988 година от Mitchell и Piper понятие система за разпределение на ключове [6].

Разделящите кодове могат да се дефинират като матрици на инцидентност на системи за разпределение на ключове.

Определение 2. Двоична $N \times T$ матрица $C = (c_{ij})$ се нарича (N, T, w, r) разделящ код (superimposed code), ако за всеки две непересичащи се подмножества $W, R \subset [T]$, за които $|W| = w$ и $|R| = r$, съществува ред $i \in [N]$, за който $c_{ij} = 1$ за всички $j \in W$ и $c_{ij} = 0$ за всички $j \in R$.

Казва се още, че C е (w, r) разделящ код с дължина N и мощност T .

Разделящите кодове намират приложение при груповото тестване, както и в криптографията.

Основна задача в теорията на разделящите кодове е задачата за намиране на максималния брой стълбове $T(N, w, r)$ при зададен брой редове или минималния брой редове $N(T, w, r)$ при зададен брой стълбове, за които съществува (w, r) разделящ код с размери $N \times T$. Разделящите кодове, които имат минимална дължина или максимална мощност, се наричат оптимални. Основната задача е достатъчно да се реши само при $w \leq r$, защото $N(T, w, r) = N(T, r, w)$ и

$$T(N, w, r) =$$

$$T(N, r, w).$$

При $w = r = 1$, съгласно теоремата на Sperner, $T(N, 1, 1) = \binom{N}{\lfloor N/2 \rfloor}$ [8]. В общия случай има само някои примери за опти-

мални разделящи кодове и различни оценки за $N(T, w, r)$ и за $T(N, w, r)$.

За големи стойности на N и T е трудно да бъдат намерени точните стойности на $N(T, w, r)$ и $T(N, w, r)$. Тогава за (w, r) разделящ код C с дължина N и мощност T се дефинира неговата скорост $R(C)$ с равенството $R(C) = \frac{\log_2 T}{N}$ и се интересуваме от асимптотичното поведение на тази скорост. Граници за $R(C)$ са представени в [1] и [9].

Определение 3. Два (N, T, w, r) разделящи кода са еквивалентни, ако единият от тях може да се трансформира в другия чрез пермутация на редовете и пермутация на стълбовете. Ако $w = r$, е позволено и инвертиране на стойностите на всички участващи в кода елементи.

Когато задачата за определяне на параметрите на оптимални разделящи кодове е решена, възниква проблемът за намирането на всички нееквивалентни кодове с получените параметри. Класифицирането на оптимални разделящи кодове позволява по-лесно да бъде решена основната задача при кодове с по-големи параметри N , T , w и r .

Предмет на проведеното изследване са оптималните $(1, 2)$, $(1, 3)$, $(2, 2)$, $(2, 3)$ и $(3, 3)$ разделящи кодове с малка мощност. Използвани са пет метода за класификация на (w, r) разделящи кодове и за намиране на минималната дължина $N(T, w, r)$, за която съществува (N, T, w, r) разделящ код.

МЕТОДИ ЗА КЛАСИФИКАЦИЯ НА РАЗДЕЛЯЩИ КОДОВЕ

При първия метод разделящите кодове се построяват стълб по стълб. При него класифицирането на (w, r) разделящи кодове се базира на следното твърдение: ако познаваме всички нееквивалентни $(N, T-1, w, r)$ разделящи кодове, то всички нееквивалентни (N, T, w, r) разделящи кодове може да получим като разширим всички нееквивалентни $(N, T-1, w, r)$ разделящи кодове с по един стълб по всички възможни начини и за всяка от получените матрици проверим дали е (N, T, w, r) разделящ код.

При останалите четири метода класификацията на разделящи кодове се базира на използването на остатъчни кодове.

Определение 4. Нека C е разделящ код, а x е стълб в C . Остатъчен код спрямо стойността v в стълба x на C (означава се $Res(C, x = v)$) се нарича кода, получен по следния начин: вземат се всички редове, в които C има стойност v в стълба x , след което този стълб се премахва в избраните редове.

Остатъчните кодове $Res(C, x = 0)$ и $Res(C, x = 1)$ са съответно $(w, r-1)$ (при $r > 1$) и $(w-1, r)$ (при $w > 1$) разделящи кодове.

Вторият метод се състои в следното:

$$\begin{array}{c|c} x & \\ \hline \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \vdots \\ 1 \end{pmatrix} & \begin{pmatrix} Res(C, x=0) \\ \hline ? \end{pmatrix} \end{array}$$

1. Намираме всички нееквивалентни възможности за $Res(C, x = 0)$ или $Res(C, x = 1)$.
2. Разширяваме получените остатъчни кодове до получаване на целия разделящ код.

Третият метод може да се използва при (w, r) разделящи кодове, за които $w > 1$ и $r > 1$. Нека C е (N, T, w, r) разделящ код, а x и y са два различни стълба в C и $v_1, v_2 \in \{0, 1\}$.

Означаваме $Res(Res(C, x = v_1), y = v_2)$ с $Res(C, x = v_1, y = v_2)$. Методът се състои в следното:

$$\left(\begin{array}{cc|c} x & y & \\ \hline 0 & 1 & \text{Res}(C, x=0, y=1) \\ \vdots & \vdots & \\ 0 & 1 & \\ \hline 0 & 0 & \\ \vdots & \vdots & \\ 0 & 0 & \\ 1 & 0 & \\ \vdots & \vdots & \\ 1 & 0 & \\ 1 & 1 & \\ \vdots & \vdots & \\ 1 & 1 & \end{array} \right) \quad ?$$

1. Намираме всички нееквивалентни възможности за $\text{Res}(C, x=0, y=1)$.
2. Разширяваме получените матрици до целия разделящ код.

Четвъртият метод може да се използва при (w, r) разделящи кодове, за които $w > 1$ и $r > 1$. Нека C е (N, T, w, r) разделящ код, а x и y са два различни стълба в C . Методът се състои в следното:

$$\left(\begin{array}{cc|c} x & y & \\ \hline 0 & 1 & \text{Res}(C, x=0, y=1) \\ \vdots & \vdots & \\ 0 & 1 & \\ \hline 1 & 0 & \\ \vdots & \vdots & \text{Res}(C, x=1, y=0) \\ 1 & 0 & \\ \hline 0 & 0 & \\ \vdots & \vdots & \\ 0 & 0 & \\ 1 & 1 & \\ \vdots & \vdots & \\ 1 & 1 & \end{array} \right) \quad ?$$

1. Намираме всички нееквивалентни възможности за $\text{Res}(C, x=0, y=1)$ и $\text{Res}(C, x=1, y=0)$. Двата остатъчни кода са $(w-1, r-1)$ разделящи кодове, но може да имат различни дължини.
2. Намираме всички нееквивалентни възможности за редовете на C , които съдържат $\text{Res}(C, x=0, y=1)$ и $\text{Res}(C, x=1, y=0)$.

3. Разширяваме получените матрици до целия разделящ код.

Петият метод може да се използва при (w, r) разделящи кодове, за които $w > 2$ и $r > 2$. Нека C е (N, T, w, r) разделящ код, а x , y и z са два различни стълба в C и $v_1, v_2, v_3 \in \{0, 1\}$. Означаваме

$$\text{Res}(\text{Res}(\text{Res}(C, x=v_1), y=v_2), z=v_3)$$

с $\text{Res}(C, x=v_1, y=v_2, z=v_3)$. Методът се състои в следното:

$$\left(\begin{array}{ccc|c} x & y & z & \\ \hline 1 & 0 & 0 & \text{Res}(C, x=1, y=0, z=0) \\ \vdots & \vdots & \vdots & \\ 1 & 0 & 0 & \\ \hline 1 & 1 & 0 & \\ \vdots & \vdots & \vdots & \text{Res}(C, x=1, y=1, z=0) \\ 1 & 1 & 0 & \\ \hline 0 & 1 & 0 & \\ \vdots & \vdots & \vdots & \text{Res}(C, x=0, y=1, z=0) \\ 0 & 1 & 0 & \\ \hline 0 & 1 & 1 & \\ \vdots & \vdots & \vdots & \text{Res}(C, x=0, y=1, z=1) \\ 0 & 1 & 1 & \\ \hline 0 & 0 & 1 & \\ \vdots & \vdots & \vdots & \text{Res}(C, x=0, y=0, z=1) \\ 0 & 0 & 1 & \\ \hline 1 & 0 & 1 & \\ \vdots & \vdots & \vdots & \text{Res}(C, x=1, y=0, z=1) \\ 1 & 0 & 1 & \\ \hline 0 & 0 & 0 & \\ \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & \\ 1 & 1 & 1 & \\ \vdots & \vdots & \vdots & \\ 1 & 1 & 1 & \end{array} \right) \quad ?$$

1. Намираме всички нееквивалентни възможности за $\text{Res}(C, x=1, y=0, z=0)$, $\text{Res}(C, x=1, y=1, z=0)$, $\text{Res}(C, x=0, y=1, z=0)$, $\text{Res}(C, x=0, y=1, z=1)$, $\text{Res}(C, x=0, y=0, z=1)$ и $\text{Res}(C, x=1, y=0, z=1)$. Три от тези остатъчни кода са $(w-1, r-2)$ разделящи кодове, а другите три – $(w-2, r-1)$ разделящи кодове.

2. За всяка от получените възможности за остатъчните кодове в точка 1. намираме всички еквивалентни на нея възможности, с подредени лексикографски в нарастващ ред редове.
3. Намираме всички възможности за редовете на C , които съдържат изброените в точка 1. остатъчни кодове, като използваме получените в точка 2. разделящи кодове и налагаме условието всеки от остатъчните кодове $Res(C, x=1, z=0)$, $Res(C, y=1, z=0)$, $Res(C, x=0, y=1)$, $Res(C, x=0, z=1)$, $Res(C, y=0, z=1)$ и $Res(C, x=1, y=0)$ да бъде $(w-1, r-1)$ разделящ код.
4. Разширяваме получените в точка 3. матрици до целия разделящ код.

РЕЗУЛТАТИ

Основните резултати са свързани със създаването на алгоритми за реализиране на петте метода и разработване на компютърни програми за практическото им реализиране. Петте метода са приложени поотделно или в комбинация за изследване на оптимални разделящи кодове с различни параметри. Изследванията за еквивалентност на получаваните кодове са проведени с програмата Q-extension [3] на Илия Буюклиев.

За успешната реализация на описаните методи от особено значение е познаването на различни необходими условия, които трябва да изпълняват изследваните разделящи кодове. Една важна характеристика на всеки разделящ код е минималното разстояние по Hamming между участващите в кода стълбове. За оценяване на това разстояние в работата е използвана границата на Plotkin [7], която е в сила не само за разделящи кодове, а и за произволни двоични кодове. За разделящи кодове тази граница изглежда по следния начин:

Ако C е (N, T, w, r) разделящ код с минимално разстояние между стълбовете d , то:

$$d \leq \left\lfloor \frac{2N \left\lfloor \frac{T}{2} \right\rfloor \left\lfloor \frac{T+1}{2} \right\rfloor}{T(T-1)} \right\rfloor.$$

В дисертацията е направено уточнение на тази граница:

$$d \leq \left\lfloor \frac{2}{3} \left\lfloor \frac{3N \left\lfloor \frac{T}{2} \right\rfloor \left\lfloor \frac{T+1}{2} \right\rfloor}{T(T-1)} \right\rfloor \right\rfloor.$$

Новата граница дава или същия резултат като границата на Plotkin, или резултат, който е с 1 по-добър от него и е приложена за доказване на единствеността на $(20, 10, 2, 2)$ разделящия код.

Определени са точните стойности на функцията $N(T, w, r)$ за 13 отворени случая:

- на $N(T, 1, 2)$ при $13 \leq T \leq 20$;
- на $N(21, 1, 3)$;
- на $N(10, 2, 2)$;
- на $N(8, 2, 3)$ и $N(9, 2, 3)$;
- на $N(8, 3, 3)$.

Намерени са нови граници за $N(T, w, r)$:

- $N(13, 2, 2) \geq 24$;
- $36 \leq N(11, 2, 3) \leq 40$.

Направена е класификация на оптимални (N, T, w, r) разделящи кодове при:

- $w=1, r=2$ и $T \leq 17$;
- $w=1, r=3$ и $T \leq 20$;
- $w=2, r=2$ и $T \leq 10$;
- $w=2, r=3$ и $T \leq 8$;
- $w=3, r=3$ и $T \leq 7$.

Част от резултатите са получени самостоятелно, друга част – в съавторство с Капралов. Изследванията на $(N, T, 3, 3)$ разделящите кодове са проведени съвместно с Капралов и корейските математици Kim и Oh.

ЛИТЕРАТУРА

- [1] А. Дьячков и В. Рыков. Границы длины дизъюнктивных кодов. *Проблемы передачи информации*, 18(3):7–13, 1982.
- [2] М. Манев. Оптимални разделящи кодове. *Дисертация за присъждане на образователната и научна степен "доктор"*, 2010.
- [3] I. Bouyukliev. What is Q-extension? *Serdica Journal of Computing*, 1:115–130, 2007.
- [4] P. Erdős, P. Frankl, and Z. Füredi, Families of finite sets in which no set is covered by the union of r others. *Israel Journal of Mathematics*, 51(1-2):79–89, 1985.
- [5] W. Kautz and R. Singleton. Nonrandom binary superimposed codes. *IEEE Transactions on Information Theory*, 10(4):363–377, 1964.

- [6] C. Mitchell and F. Piper. Key storage in secure network. *Discrete Applied Mathematics*, 21(3):215–228, 1988.
- [7] M. Plotkin. Binary codes with specified minimum distance. *IRE Transactions on Information Theory*, 6(4):445–450, 1960.
- [8] E. Sperner. Ein Satz über Untermengen einer endlichen Menge. *Mathematische Zeitschrift*, 27(1):544–548, 1928.
- [9] D. Stinson, R. Wei, and L. Zhu. Some new bounds for cover-free families. *Journal of Combinatorial Theory*, 90(1):224–234, 2000.