Домашна работа 2

Увод в теория на кодирането

Кристиян Стоименов
ф.н 3MI0400121, ФМИ

Май 2023

Задача 1

Да се напише векторът, който съответства на булевата функция $f = 1 + v_3 + v_1 v_2$

- ако f е функция на три променливи
- ако f е функция на четири променливи

Решение:

Ако f е функция на три промеливи:

Откриваме стойностите за f като заместим v_1, v_2 и v_3 в полинома, вземайки стойности от всеки един от редовете. Решението е написано на Таблица 1.

Стойност	v_1	v_2	v_3	f
0	0	0	0	1
1	0	0	1	0
2	0	1	0	1
3	0	1	1	0
4	1	0	0	1
5	1	0	1	0
6	1	1	0	0
7	1	1	1	1

Таблица 1: *Стойности на* $f(v_1, v_2, v_3) = 1 + v_3 + v_1 v_2$

Ако f е функция на четири промеливи:

Тъй като v_4 не участва в полинома, то неговата стойност няма отражение върху функционалната стойност. Поради тази причина, няма нужда отново да смятаме $f(v_1, v_2, v_3, *)$. Решението е написано на Таблица 2.

Задача 2

Да се намери полинома на Жегалкин, съответстващ на f, зададена със Таблица 3.

Решение:

Стойност	v_1	v_2	v_3	v_4	f
0	0	0	0	0	1
1	0	0	0	1	1
2	0	0	1	0	0
3	0	0	1	1	0
4	0	1	0	0	1
5	0	1	0	1	1
6	0	1	1	0	0
7	0	1	1	1	0

Стойност	x_1	x_2	x_3	x_4	f
8	1	0	0	0	1
9	1	0	0	1	1
10	1	0	0	0	0
11	1	0	1	1	0
12	1	1	1	0	0
13	1	1	0	1	0
14	1	1	1	0	1
15	1	1	1	1	1

Таблица 2: *Стойности на* $f(v_1, v_2, v_3, v_4) = 1 + v_3 + v_1 v_2$

Стойност	x_1	x_2	x_3	x_4	f
0	0	0	0	0	1
1	0	0	0	1	1
2	0	0	1	0	0
3	0	0	1	1	1
4	0	1	0	0	0
5	0	1	0	1	0
6	0	1	1	0	0
7	0	1	1	1	0

Стойност	x_1	x_2	x_3	x_4	f
8	1	0	0	0	1
9	1	0	0	1	0
10	1	0	1	0	1
11	1	0	1	1	1
12	1	1	0	0	0
13	1	1	0	1	1
14	1	1	1	0	1
15	1	1	1	1	1

Таблица 3: *Функцията* f*, чието представяне чрез полином се търси в Задача .*

Представяме функцията f като функция с един по-малко аргумент и други две функции f_0 и f_1. Извършваме аналгични действия, докато не стигнем до функция на една променлива, чиято стойност можем да определим непострествено - това са функциите f_{***}.

$$
\begin{aligned}
f &= (1 + x_1) f_0 + x_1 f_1 \\
f_0 &= (1 + x_2) f_{00} + x_2 f_{01} \\
f_1 &= (1 + x_2) f_{10} + x_2 f_{11} \\
f_{00} &= (1 + x_3) f_{000} + x_3 f_{001} \\
f_{01} &= (1 + x_3) f_{010} + x_3 f_{011} \\
f_{10} &= (1 + x_3) f_{100} + x_3 f_{101} \\
f_{11} &= (1 + x_3) f_{110} + x_3 f_{111}
\end{aligned}
$$

$$
\begin{aligned}
f_{000} &= 1 \\
f_{001} &= x_4 \\
f_{010} &= 0 \\
f_{011} &= 0 \\
f_{100} &= 1 + x_4 \\
f_{101} &= 1 \\
f_{110} &= x_4 \\
f_{111} &= 1
\end{aligned}
$$

Сега "се връщаме нагоре за да получим полином за функцията f.

$$
\begin{aligned}
f_{00} &= (1+x_3)f_{000} + x_3 f_{001} = (1+x_3) + x_3x_4 = 1 + x_3x_4 + x_3\\
f_{01} &= (1+x_3)f_{010} + x_3 f_{011} = (1+x_3).0 + x_3.0 = 0\\
f_{10} &= (1+x_3)f_{100} + x_3 f_{101} = (1+x_3)(1+x_4) + x_3 = 1 + x_3x_4 + x_4\\
f_{11} &= (1+x_3)f_{110} + x_3 f_{111} = (1+x_3)x_4 + x_3 = x_3x_4 + x_3 + x_4
\end{aligned}
$$

$$
\begin{aligned}
f_0 &= (1+x_2)f_{00} + x_2 f_{01} = (1+x_2)(1+x_3x_4+x_3) + x_2.0 = 1 + x_3x_4 + x_3 + x_2 + x_2x_3x_4 + x_2x_3\\
f_1 &= (1+x_2)f_{10} + x_2 f_{11} = (1+x_2)(1+x_3x_4+x_4) + x_2(x_3x_4+x_3+x_4) = 1 + x_3x_4 + x_2x_3 + x_4 + x_2
\end{aligned}
$$

$$
\begin{aligned}
f &= (1+x_1)f_0 + x_1 f_1 = (1+x_1)(1+x_3x_4+x_3+x_2+x_2x_3x_4+x_2x_3) + x_1(1+x_2x_3+x_3x_4+x_2+x_4) =\\
&= 1 + x_1x_2x_3x_4 + x_2x_3x_4 + x_1x_4 + x_1x_3 + x_2x_3 + x_3x_4 + x_2 + x_3
\end{aligned}
$$

Задача 3

Да се опишат параметрите на всички RM кодове на пет промеливи и да се посочи количеството грешки, които могат да поправят.

Решение:

Щом разглеждаме код на пет промеливи, то той ще съдържа всички двоични вектори с дължина $2^5 = 32$ (т. е $m = 5$). Също така най-високата възможна степен за едночлен, и респективно за полиноми, е 5. Тогава трябва да изследваме $RM(r, 5)$, където $0 \leq r \leq 5$.

Дължината на кодовите думи е фиксирана: 2^5. При зададено r от посочения интервал размерността k пресмятаме като

$$k = \sum_{i=0}^{r} \binom{m}{i}$$

За минималното разстояние знаем, че се получава като $d = 2^{m-r}$. Количеството грешки, които открива коът е $\leq 2^{m-r} - 1$, а количеството на тези, които поправя -

$$t \leq \lfloor \frac{2^{m-r} - 1}{2} \rfloor$$

Обобщено получаваме

Код	**Параметри**	**Граница за t**
$RM(0,5)$	$[32, 1, 32]$	$t \leq 15$
$RM(1,5)$	$[32, 6, 16]$	$t \leq 7$
$RM(2,5)$	$[32, 16, 8]$	$t \leq 3$
$RM(3,5)$	$[32, 26, 4]$	$t \leq 1$
$RM(4,5)$	$[32, 31, 2]$	$t \leq 0$
$RM(5,5)$	$[32, 32, 1]$	$t \leq 0$

Таблица 4: *Описание на кодове* $RM(r, 5)$*, където* $0 \leq r \leq 5$

.

Задача 4

Да се напише пораждащата матрица на кода $RM(1,4)$ и да се декодират следните вектори чрез декодера на Рид:

- $y = 1000010111100101$
- $z = 1001011001101001$
- $t = 1110111011101110$

Решение:

Размерността на кода е

$$k = \sum_{i=0}^{1} \binom{4}{i} = \binom{4}{0} + \binom{4}{1} = 5,$$

а дължината на всеки вектор от него е

$$2^4 = 16.$$

В пораждащата матрица трябва да включим двоичните вектои, съответстващи на едночлени от степени 0 и 1 ($<= r$, където $r = 1$).

Степен 0

x_1	x_2	x_3	x_4	f
$*$	$*$	$*$	$*$	1

Степен 1

x_1	x_2	x_3	x_4	$f = x_1$
0	$*$	$*$	$*$	0
1	$*$	$*$	$*$	1

Аналогично прилагаме и за $f = x_2$, $f = x_3$ и $f = x_4$, за да получим още четири вектора. Накрая, получените вектори подреждаме в матрица, за да получим пораждащата:

$$G = \underbrace{\begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix}}_{5 \times 16}$$

Декодираме получена дума y, търсейки изпратения информационен вектор $a = (a_1, a_2, a_3, a_4, a_5)$. Връзката между двете е чрез пораждащата матрица:

$$\begin{aligned} y = a.G = (a_1, \quad & a_1 + a_5, \quad a_1 + a_4, \quad a_1 + a_4 + a_5, \\ & a_1 + a_3, \quad a_1 + a_3 + a_5, \quad a_1 + a_3 + a_4, \quad a_1 + a_3 + a_4 + a_5, \\ & a_1 + a_2, \quad a_1 + a_2 + a_5, \quad a_1 + a_2 + a_4, \quad a_1 + a_2 + a_4 + a_5, \\ & a_1 + a_2 + a_3, \quad a_1 + a_2 + a_3 + a_5, \quad a_1 + a_2 + a_3 + a_4, \quad a_1 + a_2 + a_3 + a_4 + a_5) \end{aligned}$$

Ако полученият вектор $y = (y_1, y_2, \ldots, y_{16})$, то можем да получим следните равенства:

$$y_1 = a_1$$

$$
\begin{aligned}
y_9 &= a_1 + a_2 = y_1 + a_2 \Rightarrow a_2 = y_1 + y_9 \\
y_{10} &= a_1 + a_2 + a_5 = a_2 + (a_1 + a_5) = y_2 + a_2 \Rightarrow a_2 = y_2 + y_{10} \\
y_{11} &= a_1 + a_2 + a_4 = a_2 + (a_1 + a_4) = a_2 + y_3 \Rightarrow a_2 = y_3 + y_{11} \\
y_{12} &= a_1 + a_2 + a_4 + a_5 = a_2 + (a_1 + a_4 + a_5) = a_2 + y_4 \Rightarrow a_2 = y_4 + y_{12} \\
y_{13} &= a_1 + a_2 + a_3 = a_2 + (a_1 + a_3) = a_2 + y_5 \Rightarrow a_2 = y_5 + y_{13} \\
y_{14} &= a_1 + a_2 + a_3 + a_5 = a_2 + (a_1 + a_3 + a_5) = a_2 + y_6 \Rightarrow a_2 = y_6 + y_{14} \\
y_{15} &= a_1 + a_2 + a_3 + a_4 = a_2 + (a_1 + a_3 + a_4) = a_2 + y_7 \Rightarrow a_2 = y_7 + y_{15} \\
y_{16} &= a_1 + a_2 + a_3 + a_4 + a_5 = a_2 + (a_1 + a_3 + a_4 + a_5) = a_2 + y_8 \Rightarrow a_2 = y_8 + y_{16}
\end{aligned}
$$

$$
\begin{aligned}
y_5 &= a_3 + a_1 = a_3 + y_1 \Rightarrow a_3 = y_1 + y_5 \\
y_6 &= a_3 + (a_1 + a_5) = a_3 + y_2 \Rightarrow a_3 = y_2 + y_6 \\
y_7 &= a_3 + (a_1 + a_4) = a_3 + y_3 \Rightarrow a_3 = y_3 + y_7 \\
y_8 &= a_3 + (a_1 + a_3 + a_5) = a_3 + y_4 \Rightarrow a_3 = y_4 + y_8 \\
y_{13} &= a_3 + (a_1 + a_2) = a_3 + y_9 \Rightarrow a_3 = y_9 + y_{13} \\
y_{14} &= a_3 + (a_1 + a_2 + a_5) = a_3 + y_{10} \Rightarrow a_3 = y_{10} + y_{14} \\
y_{15} &= a_3 + (a_1 + a_2 + a_4) = a_3 + y_{11} \Rightarrow a_3 = y_{11} + y_{15} \\
y_{16} &= a_3 + (a_1 + a_2 + a_4 + a_5) = a_3 + y_{12} \Rightarrow a_3 = y_{12} + y_{16}
\end{aligned}
$$

$$
\begin{aligned}
y_3 &= a_4 + a_1 = a_4 + y_1 \Rightarrow a_4 = y_1 + y_3 \\
y_4 &= a_4 + (a_1 + a_5) = a_4 + y_2 \Rightarrow a_4 = y_2 + y_4 \\
y_7 &= a_4 + (a_1 + a_3) = a_4 + y_5 \Rightarrow a_4 = y_5 + y_7 \\
y_8 &= a_4 + (a_1 + a_3 + a_5) = a_4 + y_6 \Rightarrow a_4 = y_6 + y_8 \\
y_{11} &= a_4 + (a_1 + a_2) = a_4 + y_9 \Rightarrow a_4 = y_9 + y_{11} \\
y_{12} &= a_4 + (a_1 + a_2 + a_5) = a_4 + y_{10} \Rightarrow a_4 = y_{10} + y_{11} \\
y_{15} &= a_4 + (a_1 + a_2 + a_3) = a_4 + y_{13} \Rightarrow a_4 = y_{13} + y_{15} \\
y_{16} &= a_4 + (a_1 + a_2 + a_3 + a_5) = a_4 + y_{14} \Rightarrow a_4 = y_{14} + y_{16}
\end{aligned}
$$

$$
\begin{aligned}
y_2 &= a_5 + a_1 = a_5 + y_1 \Rightarrow a_5 = y_1 + y_2 \\
y_4 &= a_5 + (a_1 + a_4) = a_5 + y_3 \Rightarrow a_5 = y_3 + y_4 \\
y_6 &= a_5 + (a_1 + a_3) = a_5 + y_5 \Rightarrow a_5 = y_5 + y_6 \\
y_8 &= a_5 + (a_1 + a_3 + a_4) = a_5 + y_7 \Rightarrow a_5 = y_7 + y_8 \\
y_{10} &= a_5 + (a_1 + a_2) = a_5 + y_9 \Rightarrow a_5 = y_9 + y_{10} \\
y_{12} &= a_5 + (a_1 + a_2 + a_4) = a_5 + y_{11} \Rightarrow a_5 = y_{11} + y_{12} \\
y_{14} &= a_5 + (a_1 + a_2 + a_3) = a_5 + y_{13} \Rightarrow a_5 = y_{13} + y_{14} \\
y_{16} &= a_5 + (a_1 + a_2 + a_3 + a_4) = a_5 + y_{15} \Rightarrow a_5 = y_{15} + y_{16}
\end{aligned}
$$

Обобщено:

$$\begin{aligned}
&a_1 = y_1\\
&a_2 = y_1 + y_9 = y_2 + y_{10} = y_3 + y_{11} = y_4 + y_{12} = y_5 + y_{13} = y_6 + y_{14} = y_7 + y_{15} = y_8 + y_{16}\\
&a_3 = y_1 + y_5 = y_2 + y_6 = y_3 + y_7 = y_4 + y_8 = y_9 + y_{13} = y_{10} + y_{14} = y_{11} + y_{15} = y_{12} + y_{16}\\
&a_4 = y_1 + y_3 = y_2 + y_4 = y_5 + y_7 = y_6 + y_8 = y_9 + y_{11} = y_{10} + y_{12} = y_{13} + y_{15} = y_{14} + y_{16}\\
&a_5 = y_1 + y_2 = y_3 + y_4 = y_5 + y_6 = y_7 + y_8 = y_9 + y_{10} = y_{11} + y_{12} = y_{13} + y_{14} = y_{15} + y_{16}
\end{aligned}$$

Нека получената кодова дума за декодиране е $y = (1000010111100101)$. Тогава пресмятаме всички възможни стойности за всеки един от битовете на информационния вектор, за да получим

Бит	**Брой на "0"**	**Брой на "1"**	**Стойност**
a_1	-	-	1
a_2	6	2	0
a_3	2	6	1
a_4	6	2	0
a_5	2	6	1

Таблица 5: *Декодиране на* $y = (1000010111100101)$

Окончателно получаваме, че думата y се декодира до 10101.

Нека сега получената кодова дума за декодиране е $z = (1001011001101001)$. Тогава пресмятаме по сходен начин

Бит	**Брой на "0"**	**Брой на "1"**	**Стойност**
a_1	-	-	1
a_2	0	8	1
a_3	0	8	1
a_4	0	8	0
a_5	0	8	1

Таблица 6: *Декодиране на* $z = (1001011001101001)$

Окончателно получаваме, че думата z се декодира до 11111.

Нека накрая получената кодова дума да бъде $t = (1110111011101110)$. Тогава пресмятаме по сходен начин

Бит	**Брой на "0"**	**Брой на "1"**	**Стойност**
a_1	-	-	1
a_2	8	0	0
a_3	8	0	0
a_4	4	4	-
a_5	4	4	-

Таблица 7: *Декодиране на* $t = (1110111011101110)$

Така можем да заключим, че t не се декодира недвусмислено.

Задача 5

Да се декодират следните вектори чрез постъпково мажоритарно декодиране, приложено върху $RM(1,3)$ код:

- $y = 10111010$
- $z = 10011001$
- $t = 01110111$

Решение:

При $RM(1,3)$ се интересуваме от точките на афинната геометрия $AG(3,2)$, които са $P_0 = (000)$, $P_1 = (001)$, $P_2 = (010)$, $P_3 = (011)$, $P_4 = (100)$, $P_5 = (101)$, $P_6 = (110)$, $P_7 = (111)$.

Нека разглеждаме получените вектори като характеристични вектори на подмножество от точки от афинната геометрия $AG(3,2)$.

$$M_y = \{P_0, P_2, P_3, P_4, P_6\} \subset AG(3,2),$$
$$M_z = \{P_0, P_3, P_4, P_7\} \subset AG(3,2),$$
$$M_t = \{P_1, P_2, P_3, P_5, P_6, P_7\} \subset AG(3,2)$$

Разглеждаме всички равнини (двумерни подпространства на $AG(3,2)$) и тяхната четност при пресичане с тези подмножества от точки M като ги подреждаме в таблица.

Разглеждаме всички прави, зададени чрез две от точките P и техните четности, определени от четностите на равнините, в които се срещат. Представяме ги сходно на това равнините и техните четности.

Накрая разглеждаме и четностите на точките в съответните подмножества.

За изпратени кодови думи получаваме съответно

$$a_y = (),$$
$$a_z = (),$$
$$a_t = ().$$

Споменатите таблици се намират на следващата страница.

Равнина	M_y	M_z	M_t
P_0, P_1, P_2, P_3	1	0	1
P_0, P_1, P_2, P_4	1	0	0
P_0, P_1, P_2, P_5	0	1	1
P_0, P_1, P_2, P_6	1	1	1
P_0, P_1, P_2, P_7	0	0	1
P_0, P_1, P_3, P_4	1	1	0
P_0, P_1, P_3, P_5	0	0	1
P_0, P_1, P_3, P_6	1	0	1
P_0, P_1, P_3, P_7	0	1	1
P_0, P_1, P_4, P_5	0	0	0
P_0, P_1, P_4, P_6	1	0	0
P_0, P_1, P_4, P_7	0	1	0
P_0, P_1, P_5, P_6	0	1	1
P_0, P_1, P_5, P_7	1	0	1
P_0, P_1, P_6, P_7	0	0	1
P_0, P_2, P_3, P_4	0	1	0
P_0, P_2, P_3, P_5	1	0	1
P_0, P_2, P_3, P_6	0	0	1
P_0, P_2, P_3, P_7	1	1	1
P_0, P_2, P_4, P_5	1	0	0
P_0, P_2, P_4, P_6	0	0	0
P_0, P_2, P_4, P_7	1	1	0
P_0, P_2, P_5, P_6	1	1	1
P_0, P_2, P_5, P_7	0	0	1
P_0, P_2, P_6, P_7	1	0	1
P_0, P_3, P_4, P_5	1	1	0
P_0, P_3, P_4, P_6	0	1	0
P_0, P_3, P_4, P_7	1	0	0
P_0, P_3, P_5, P_6	1	0	1
P_0, P_3, P_5, P_7	0	1	1
P_0, P_3, P_6, P_7	1	1	1
P_0, P_4, P_5, P_6	1	0	0
P_0, P_4, P_5, P_7	0	1	0
P_0, P_4, P_6, P_7	1	1	0
P_0, P_5, P_6, P_7	0	0	1

Равнина	M_y	M_z	M_t
P_1, P_2, P_3, P_4	1	0	1
P_1, P_2, P_3, P_5	0	1	0
P_1, P_2, P_3, P_6	1	1	0
P_1, P_2, P_3, P_7	0	0	0
P_1, P_2, P_4, P_5	0	1	1
P_1, P_2, P_4, P_6	1	1	1
P_1, P_2, P_4, P_7	0	0	1
P_1, P_2, P_5, P_6	0	0	0
P_1, P_2, P_5, P_7	1	1	0
P_1, P_2, P_6, P_7	0	1	0
P_1, P_3, P_4, P_5	0	0	1
P_1, P_3, P_4, P_6	1	0	1
P_1, P_3, P_4, P_7	0	1	1
P_1, P_3, P_5, P_6	0	1	0
P_1, P_3, P_5, P_7	1	0	0
P_1, P_3, P_6, P_7	0	0	0
P_1, P_4, P_5, P_6	0	1	1
P_1, P_4, P_5, P_7	1	0	1
P_1, P_4, P_6, P_7	0	0	1
P_1, P_5, P_6, P_7	1	1	0
P_2, P_3, P_4, P_5	1	0	1
P_2, P_3, P_4, P_6	0	0	1
P_2, P_3, P_4, P_7	1	1	1
P_2, P_3, P_5, P_6	1	1	0
P_2, P_3, P_5, P_7	0	0	0
P_2, P_3, P_6, P_7	1	0	0
P_2, P_4, P_5, P_6	1	1	1
P_2, P_4, P_5, P_7	0	0	1
P_2, P_4, P_6, P_7	1	0	1
P_2, P_5, P_6, P_7	0	1	0
P_3, P_4, P_5, P_6	1	0	1
P_3, P_4, P_5, P_7	0	1	1
P_3, P_4, P_6, P_7	1	1	1
P_3, P_5, P_6, P_7	0	0	0
P_4, P_5, P_6, P_7	0	0	1

Права	M_y	M_z	M_t
P_0, P_1	0	0	1
P_0, P_2	1	0	1
P_0, P_3	1	1	1
P_0, P_4	1	1	0
P_0, P_5	0	0	1
P_0, P_6	1	0	1
P_0, P_7	0	1	1
P_1, P_2	0	1	1
P_1, P_3	0	0	1
P_1, P_4	0	0	1
P_1, P_5	0	1	1
P_1, P_6	0	1	1
P_1, P_7	0	0	1
P_2, P_3	1	0	1
P_2, P_4	1	0	1
P_2, P_5	0	1	1
P_2, P_6	1	1	1
P_2, P_7	0	0	1
P_3, P_4	1	1	1
P_3, P_5	0	0	1
P_3, P_6	1	0	1
P_3, P_7	0	1	1
P_4, P_5	0	0	1
P_4, P_6	1	0	1
P_4, P_7	0	1	1
P_5, P_6	0	1	1
P_5, P_7	0	0	1
P_6, P_7	0	0	1

Точка	M_y	M_z	M_t
P_0	0	0	1
P_1	1	0	1
P_2	1	1	1
P_3	1	1	0
P_4	0	0	1
P_5	1	0	1
P_6	0	1	1
P_7	0	1	1

Таблица 8: *Подпространсва на $AG(3,2)$ и техните четности спрямо множествата от точки зададени от подадените кодови вектори.*