Про розширені бінарні коди Голея за груповими алгебрами груп $C_3 \times D_8$ та $C_2 \times A_4$

М. Ю. Бортош[1], О. А. Тилищак[2], М. В. Химинець[3]

[1,3]ДВНЗ "Ужгородський національний університет", Ужгород, Україна

[2]Закарпатський угорський інститут ім. Ференца Ракоці II, Берегове, Україна

maria.bortos@uzhnu.edu.ua, alxtlk@gmail.com, khymynets.myroslava1@student.uzhnu.edu.ua

У 2006 році ірландський вчений Т. Харлі опублікував нові результати про одну із конструкцій лінійних бінарних кодів [1]. Розглянемо дану конструкцію для побудови розширених бінарних кодів Голея. Нехай $G = \{g_1, g_2, \ldots, g_n\}$ — скінченна група порядку n і $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \ldots + \alpha_{g_n} g_n \in \mathbb{F}_2 G$ ($\alpha_i \in \mathbb{F}_2$). Задамо матрицю $\sigma(v) \in M(n, \mathbb{F}_2)$ вигляду

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \ldots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \ldots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \ldots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

Визначаємо бінарний код $C(v)$, як підпростір простору $\mathbb{F}_2^n$ породжений рядками матриці $\sigma(v)$ для заданого елемента $v \in \mathbb{F}_2 G$. У просторі $\mathbb{F}_2^n$ введений скалярний добуток $[(v_1, \ldots, v_n), (w_1, \ldots, w_n)] = \sum_{i=1}^n v_i w_i$ і відповідне ортогональне доповнення $C^\perp = \{v \in \mathbb{F}_2^n | [v, w] = 0, w \in C\}$. Якщо $C \subset C^\perp$, то бінарний код C називається самоортогональним, якщо $C = C^\perp$ — самодуальним. Код $C(v)$ самоортогональний, якщо $\sigma(v)\sigma(v)^T = 0$.

Розширений бінарний код Голея визначається, як довільний бінарний лінійний [24,12,8]-код. У роботі [2] показано, що розширений бінарний код Голея є самодуальним.

Для елемента $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \ldots + \alpha_{g_n} g_n \in \mathbb{F}_2 G$ позначимо $v^* = \alpha_{g_1} g_1^{-1} + \alpha_{g_2} g_2^{-1} + \ldots + \alpha_{g_n} g_n^{-1} \in \mathbb{F}_2 G$. Відомо [3], що існує 128 елементів $v \in \mathbb{F}_2(C_3 \times D_8)$ і 384 елементів $v \in \mathbb{F}_2(C_2 \times A_4)$ таких, що $v = v^*$ і $C(v)$ — розширений бінарний код Голея.

Досліджуємо конструкцію розширених бінарних кодів Голея за груповими алгебрами $\mathbb{F}_2(C_3 \times D_8)$ та $\mathbb{F}_2(C_2 \times A_4)$. В результаті обчислень ми отримали кількість всіх елементів $v \in \mathbb{F}_2(C_3 \times D_8)$ та $v \in \mathbb{F}_2(C_2 \times A_4)$, що $C(v)$ є розширеним бінарним кодом Голея. Подаємо ці результати у наступній таблиці.

Табл. 1: Кількість елементів з групових алгебр

Мінімальна відстань Хемінга $C(v)$	2	4	6	8
Кількість елементів $v \in \mathbb{F}_2(C_3 \times D_8)$	7 680	92 160	12 288	12 288
Кількість елементів $v \in \mathbb{F}_2(C_2 \times A_4)$	10 752	96 768	18 432	18 432

Таким чином, існує 12 288 елементів $v \in \mathbb{F}_2(C_3 \times D_8)$ та 18 432 елементів $v \in \mathbb{F}_2(C_2 \times A_4)$, що $C(v)$ є розширеним бінарним кодом Голея.

В подальших дослідженнях можна буде розглянути інші групи порядку 24.

1. Hurley T. Group Rings and Rings of Matrices. Int. Jour. Pure and Appl. Math., 2006, 31, No. 3. 319 – 335.
2. Huffman W. C., Pless V. Fundamentals of error-correcting codes. Cambridge: Cambridge University Press, 2003.
3. Dougherty S. T., Gildea J., Taylor R., Tylyshchak A. Group rings, G-codes and constructions of self-dual and formally self-dual codes. Designs, Codes and Cryptography. 2018. 86 (9). 2115 – 2138. DOI:10.1007/s10623-017-0440-7.