УДК 519.725
DOI 10.24144/2616-7700.2022.1(40).27-32

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

[1] ДВНЗ «Ужгородський національний університет»,
доцент кафедри алгебри та диференціальних рівнянь,
кандидат фізико-математичних наук
maria.bortos@uzhnu.edu.ua
ORCID: https://orcid.org/0000-0002-1648-1350

[2] Закарпатський угорський інститут ім. Ференца Ракоці II,
професор кафедри математики та інформатики,
доктор фізико-математичних наук
alxtlk@gmail.com
ORCID: https://orcid.org/0000-0001-7828-3416

[3] ДВНЗ «Ужгородський національний університет»,
аспірант кафедри алгебри та диференціальних рівнянь,
myroslava.khymynets1@uzhnu.edu.ua
ORCID: https://orcid.org/0000-0001-6363-421X

РОЗШИРЕНІ БІНАРНІ КОДИ ГОЛЕЯ ЗА ГРУПОВОЮ АЛГЕБРОЮ ГРУПИ ДІЕДРА

Для побудови лінійних бінарних самодуальних кодів було встановлено багато різних конструкцій. У статті розглядаємо побудову розширених бінарних кодів Голея за головними ідеалами (лівими) груповою алгеброю $\mathbb{F}_2D_{24}$ групи діедра D_{24} порядку 24 над полем з двох елементів $\mathbb{F}_2$. Розроблено алгоритм відшукання та знайдено програмним шляхом всі елементи $v \in \mathbb{F}_2D_{24}$, які породжують головні ідеали, що визначають розширених бінарних кодів Голея. Раніше таким способом розширений бінарний код Голея будувався за одним елементом $v \in \mathbb{F}_2D_{24}$, що $v = v^*$. Було знайдено всі 36 864 елементів $v \in \mathbb{F}_2D_{24}$ за якими можна побудувати розширений бінарний код Голея та з'ясовано, що 768 з них задовольняє умову $v = v^*$.

Ключові слова: групова алгебра, розширені бінарні коди, коди Голея, самодуальні коди, коди над полями, група діедра.

1. Вступ. В 1967 р. С. Д. Бермана [1] (див. також [8]) запропонував піонерський підхід в побудові кодів, який розглядає односторонні ідеали в групових алгебрах скінченних груп над скінченними полями, як коди над тими ж полями. Більшість відомих на той час кодів з оптимальними параметрами вкладалися в запропоновану схему. І. МакЛоглін та Т. Харлі в [2, 6] використовуючи таку ж конструкцію побудував розширений бінарний код Голея, як головний ідеал породжений деяким елементом v групової алгебри групи діедра $G = D_{24}$ порядку 24 над полем $\mathbb{F}_2$ з двох елементів. Для інших груп G порядку 24 розширені бінарні коди Голея за головним ідеалом їх групових алгебр будувалися в [3–5]. Зокрема, було з'ясовано для яких груп така побудова можлива, а для групи $(C_6 \times C_2) \rtimes C_2$ (C_n — циклічна група порядку n) була з'ясована точна кількість всіх таких елементів v за якими будуються розширені бінарні коди Голея розглядуваним способом. В статті розглядаємо аналогічну задачу для групи $G = D_{24}$.

Опишемо використовувану конструкцію та означимо розширені бінарні коди Голея. Нехай $G = \{g_1, g_2, \ldots, g_n\}$ — скінченна група порядку n. Нехай $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \ldots + \alpha_{g_n}g_n \in \mathbb{F}_2G$ ($\alpha_i \in \mathbb{F}_2$). Визначимо матрицю $\sigma(v) \in M(n, \mathbb{F}_2)$

вигляду

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

Для заданого елемента $v \in \mathbb{F}_2G$ визначаємо бінарний код: $C(v)$, як підпростір простору $\mathbb{F}_2^n$ породжений рядками матриці $\sigma(v)$. В просторі $\mathbb{F}_2^n$ вводиться скалярний добуток $[(v_1,\dots,v_1),(w_1,\dots,w_1)] = \sum_{i=1}^{n} v_i w_i$ і відповідне *ортогональне доповнення* $C^{\perp} = \{v \in \mathbb{F}_2^n | [v,w] = 0, w \in C\}$. Бінарний код C називається *самоортогональним*, якщо $C \subset C^{\perp}$ і *самодуальним* — якщо $C = C^{\perp}$. Зрозуміло, що код $C(v)$ самоортогональний, якщо $\sigma(v)\sigma(v)^T = 0$. Для елемента $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \ldots + \alpha_{g_n}g_n \in \mathbb{F}_2G$ позначимо $v^* = \alpha_{g_1}g_1^{-1} + \alpha_{g_2}g_2^{-1} + \ldots + \alpha_{g_n}g_n^{-1} \in \mathbb{F}_2G$. Легко бачити, що $\sigma(v)^T = \sigma(v^*)$.

Розглядаючи лінійний код над полем з двох елементів, використовуватимемо термін $[n,k,d]$-*код* для позначення лінійних бінарних кодів, де n — довжина кодових слів, k — розмірність підпростору кодових слів і d — мінімальна відстань Хемінга коду. Легко бачити, що відстань Хемінга між довільними кодовими словами бінарного самодуального коду парна. *Розширений бінарний код Голея* визначається, як будь-який бінарний лінійний [24,12,8]-код. Відомо [7], що розширений бінарний код Голея самодуальний.

Теорема 1 ([6]). *Нехай G скінченна група порядку 24 з елементом v групової алгебри $\mathbb{F}_2G$. Якщо*

1) $v = v^*$,

2) $v^2 = 0$,

3) $\operatorname{rank}(\sigma(v)) = 12$,

тоді код $C(v)$ самодуальний.

У [2–4, 6] встановлено, що з 15 неізоморфних груп 24-го порядку для яких будується розширений бінарний код Голея D_{24}, S_4, $(C_6 \times C_2) \rtimes C_2$, $C_3 \times D_8$, $C_2 \times A_4$ він будується за достатніми властивостями самодуальності коду наведені в теореми 1. Теорема 2 дає достатню умову, щоб код $C(v)$ був розширеним бінарним кодом Голея Скористаємося таким очевидним критерієм.

Теорема 2. *Нехай G скінченна група порядку 24 з елементом v групової алгебри $\mathbb{F}_2G$. Код $C(v)$ самодуальний тоді і тільки тоді, коли*

1) $vv^* = 0$,

2) $\operatorname{rank}(\sigma(v)) = 12$.

2. Побудова кодів за групою $G = D_{24}$.

Лема 1. *Нехай $G = D_{24} = \langle x, y \,|\, x^{12} = 1, y^2 = 1, y^{-1}xy = x^{-1}\rangle$, $v = \sum_{i=0}^{11} \alpha_{i+1}x^i + \alpha_{i+13}x^i y$. Якщо код $C(v)$ самодуальний, тоді $\sum_{i=1}^{24} \alpha_i = 0$,*

$$(\alpha_1+\alpha_3+\alpha_5+\alpha_7+\alpha_9+\alpha_{11})(\alpha_2+\alpha_4+\alpha_6+\alpha_8+\alpha_{10}+\alpha_{12}) +$$

$$(\alpha_{13}+\alpha_{15}+\alpha_{17}+\alpha_{19}+\alpha_{21}+\alpha_{23})(\alpha_{14}+\alpha_{16}+\alpha_{18}+\alpha_{20}+\alpha_{22}+\alpha_{24}) = 0,$$

$$(\alpha_1+\alpha_5)(\alpha_3+\alpha_7) + (\alpha_1+\alpha_9)(\alpha_7+\alpha_{11}) + (\alpha_2+\alpha_6)(\alpha_4+\alpha_8) +$$

$$(\alpha_2+\alpha_{10})(\alpha_8+\alpha_{12})+(\alpha_{13}+\alpha_{17})(\alpha_{15}+\alpha_{19})+(\alpha_{13}+\alpha_{21})(\alpha_{19}+\alpha_{23})+$$
$$(\alpha_{14}+\alpha_{18})(\alpha_{16}+\alpha_{20})+(\alpha_{14}+\alpha_{22})(\alpha_{20}+\alpha_{24})=0,$$
$$\alpha_1+(\alpha_1+\alpha_5)(\alpha_1+\alpha_9)+\alpha_2+(\alpha_2+\alpha_6)(\alpha_2+\alpha_{10})+\alpha_3+(\alpha_3+\alpha_7)(\alpha_3+\alpha_{11})+\alpha_4+$$
$$(\alpha_4+\alpha_8)(\alpha_4+\alpha_{12})+\alpha_{13}+(\alpha_{13}+\alpha_{17})(\alpha_{13}+\alpha_{21})+\alpha_{14}+(\alpha_{14}+\alpha_{18})(\alpha_{14}+\alpha_{22})+\alpha_{15}+$$
$$(\alpha_{15}+\alpha_{19})(\alpha_{15}+\alpha_{23})+\alpha_{16}+(\alpha_{16}+\alpha_{20})(\alpha_{16}+\alpha_{24})=0.$$

Доведення. Обчислення в групі $G=D_{24}$ показують, що $\sigma(v)$ має вигляд:

$$\begin{pmatrix}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24}\\
\alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23}\\
\alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22}\\
\alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21}\\
\alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20}\\
\alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19}\\
\alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18}\\
\alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17}\\
\alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16}\\
\alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15}\\
\alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14}\\
\alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13}\\
\alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2\\
\alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3\\
\alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4\\
\alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5\\
\alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6\\
\alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7\\
\alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8\\
\alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9\\
\alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10}\\
\alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11}\\
\alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12}\\
\alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1
\end{pmatrix}.$$

Тоді матриця $\sigma(v)\sigma(v)^T=\sigma(vv^*)$ набуває вигляду:

$$\begin{pmatrix}
\gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_3\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \gamma_2\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & 0 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1
\end{pmatrix},$$

де $\gamma_1=\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5+\alpha_6+\alpha_7+\alpha_8+\alpha_9+\alpha_{10}+\alpha_{11}+\alpha_{12}+\alpha_{13}+\alpha_{14}+$
$+\alpha_{15}+\alpha_{16}+\alpha_{17}+\alpha_{18}+\alpha_{19}+\alpha_{20}+\alpha_{21}+\alpha_{22}+\alpha_{23}+\alpha_{24}$;

$\gamma_2=(\alpha_1+\alpha_3)(\alpha_4+\alpha_2)+(\alpha_1+\alpha_5)(\alpha_6+\alpha_4)+(\alpha_1+\alpha_7)(\alpha_8+\alpha_6)+(\alpha_1+\alpha_9)\cdot$
$\cdot(\alpha_{10}+\alpha_8)+(\alpha_1+\alpha_{11})(\alpha_{12}+\alpha_{10})+(\alpha_{13}+\alpha_{15})(\alpha_{16}+\alpha_{14})+(\alpha_{13}+\alpha_{17})(\alpha_{18}+\alpha_{16})+$
$+(\alpha_{13}+\alpha_{19})(\alpha_{20}+\alpha_{18})+(\alpha_{13}+\alpha_{21})(\alpha_{22}+\alpha_{20})+(\alpha_{13}+\alpha_{23})(\alpha_{24}+\alpha_{22})$,

або $\gamma_2=\alpha_1(\alpha_{12}+\alpha_2)+\alpha_3(\alpha_2+\alpha_4)+\alpha_5(\alpha_4+\alpha_6)+\alpha_7(\alpha_6+\alpha_8)+\alpha_9(\alpha_8+\alpha_{10})+$
$\alpha_{11}(\alpha_{10}+\alpha_{12})+\alpha_{13}(\alpha_{24}+\alpha_{14})+\alpha_{15}(\alpha_{14}+\alpha_{16})+\alpha_{17}(\alpha_{16}+\alpha_{18})+\alpha_{19}(\alpha_{18}+\alpha_{20})+$
$\alpha_{21}(\alpha_{20}+\alpha_{22})+\alpha_{23}(\alpha_{22}+\alpha_{24})$;

$\gamma_3 = (\alpha_1 + \alpha_5)(\alpha_3 + \alpha_7) + (\alpha_1 + \alpha_9)(\alpha_7 + \alpha_{11}) + (\alpha_2 + \alpha_6)(\alpha_4 + \alpha_8) + (\alpha_2 + \alpha_{10}) \cdot$
$\cdot (\alpha_8 + \alpha_{12}) + (\alpha_{13} + \alpha_{17})(\alpha_{15} + \alpha_{19}) + (\alpha_{13} + \alpha_{21})(\alpha_{19} + \alpha_{23}) + (\alpha_{14} + \alpha_{18})(\alpha_{16} +$
$+ \alpha_{20}) + (\alpha_{14} + \alpha_{22})(\alpha_{20} + \alpha_{24})$,

або $\gamma_3 = \alpha_1(\alpha_{11} + \alpha_3) + \alpha_2(\alpha_{12} + \alpha_4) + \alpha_5(\alpha_3 + \alpha_7) + \alpha_6(\alpha_4 + \alpha_8) + \alpha_9(\alpha_7 + \alpha_{11}) +$
$\alpha_{10}(\alpha_8 + \alpha_{12}) + \alpha_{13}(\alpha_{23} + \alpha_{15}) + \alpha_{14}(\alpha_{24} + \alpha_{16}) + \alpha_{17}(\alpha_{15} + \alpha_{19}) + \alpha_{18}(\alpha_{16} + \alpha_{20}) +$
$\alpha_{21}(\alpha_{19} + \alpha_{23}) + \alpha_{22}(\alpha_{20} + \alpha_{24})$;

$\gamma_4 = (\alpha_1 + \alpha_7)(\alpha_4 + \alpha_{10}) + (\alpha_2 + \alpha_8)(\alpha_5 + \alpha_{11}) + (\alpha_3 + \alpha_9)(\alpha_6 + \alpha_{12}) + (\alpha_{13} + \alpha_{19}) \cdot$
$\cdot (\alpha_{16} + \alpha_{22}) + (\alpha_{15} + \alpha_{21})(\alpha_{18} + \alpha_{24}) + (\alpha_{17} + \alpha_{23})(\alpha_{14} + \alpha_{20})$;

$\gamma_5 = \alpha_1 + (\alpha_1 + \alpha_5)(\alpha_1 + \alpha_9) + \alpha_2 + (\alpha_2 + \alpha_6)(\alpha_2 + \alpha_{10}) + \alpha_3 + (\alpha_3 + \alpha_7)(\alpha_3 + \alpha_{11}) +$
$+ \alpha_4 + (\alpha_4 + \alpha_8)(\alpha_4 + \alpha_{12}) + \alpha_{13} + (\alpha_{13} + \alpha_{17})(\alpha_{13} + \alpha_{21}) + \alpha_{14} + (\alpha_{14} + \alpha_{18})(\alpha_{14} +$
$+ \alpha_{22}) + \alpha_{15} + (\alpha_{15} + \alpha_{19})(\alpha_{15} + \alpha_{23}) + \alpha_{16} + (\alpha_{16} + \alpha_{20})(\alpha_{16} + \alpha_{24})$,

або $\gamma_5 = \alpha_1(\alpha_9 + \alpha_5) + \alpha_2(\alpha_{10} + \alpha_6) + \alpha_3(\alpha_{11} + \alpha_7) + \alpha_4(\alpha_8 + \alpha_{12}) + \alpha_{24}(\alpha_{20} + \alpha_{16}) +$
$\alpha_{23}(\alpha_{19} + \alpha_{15}) + \alpha_{22}(\alpha_{18} + \alpha_{14}) + \alpha_{17}(\alpha_{21} + \alpha_{13}) + \alpha_9\alpha_5 + \alpha_{10}\alpha_6 + \alpha_{11}\alpha_7 + \alpha_{12}\alpha_8 +$
$\alpha_{18}\alpha_{14} + \alpha_{19}\alpha_{15} + \alpha_{20}\alpha_{16} + \alpha_{13}\alpha_{21}$;

$\gamma_6 = (\alpha_1 + \alpha_{11})(\alpha_6 + \alpha_4) + (\alpha_1 + \alpha_9)(\alpha_4 + \alpha_2) + (\alpha_1 + \alpha_7)(\alpha_2 + \alpha_{12}) + (\alpha_{21} + \alpha_5) \cdot$
$\cdot (\alpha_{12} + \alpha_{10}) + (\alpha_1 + \alpha_3)(\alpha_{10} + \alpha_8) + (\alpha_{13} + \alpha_{23})(\alpha_{18} + \alpha_{16}) + (\alpha_{13} + \alpha_{21})(\alpha_{16} +$
$+ \alpha_{14}) + (\alpha_{13} + \alpha_{19})(\alpha_{14} + \alpha_{24}) + (\alpha_{13} + \alpha_{17})(\alpha_{24} + \alpha_{22}) + (\alpha_{13} + \alpha_{15})(\alpha_{22} + \alpha_{20})$;

або $\gamma_6 = \alpha_1(\alpha_6 + \alpha_8) + \alpha_2(\alpha_7 + \alpha_9) + \alpha_3(\alpha_8 + \alpha_{10}) + \alpha_4(\alpha_9 + \alpha_{11}) + \alpha_5(\alpha_{10} + \alpha_{12}) +$
$\alpha_{20}(\alpha_{13} + \alpha_{15}) + \alpha_{21}(\alpha_{14} + \alpha_{16}) + \alpha_{22}(\alpha_{15} + \alpha_{17}) + \alpha_{23}(\alpha_{16} + \alpha_{18}) + \alpha_{24}(\alpha_{17} + \alpha_{19}) +$
$a_6a_{11} + a_7a_{12} + a_{13}a_{18} + a_{14}a_{19}$.

Звідси отримаємо,

$\gamma_2 + \gamma_4 + \gamma_6 = (\alpha_1 + \alpha_3 + \alpha_5 + \alpha_7 + \alpha_9 + \alpha_{11})(\alpha_2 + \alpha_4 + \alpha_6 + \alpha_8 + \alpha_{10} + \alpha_{12}) + (\alpha_{13} +$
$+ \alpha_{15} + \alpha_{17} + \alpha_{19} + \alpha_{21} + \alpha_{23})(\alpha_{14} + \alpha_{16} + \alpha_{18} + \alpha_{20} + \alpha_{22} + \alpha_{24})$.

Якщо код $C(v)$ самодуальний, то за умовою 1 теореми 2 виконуються умови: $vv^* = 0$ і $\sigma(v)\sigma(v)^T = \sigma(vv^*) = 0$ а, отже, $\gamma_i = 0$ $(i = 1, \ldots, 6)$. Тоді $\gamma_1 = 0$, $\gamma_2 + \gamma_4 + \gamma_6 = 0$, $\gamma_3 = 0$, $\gamma_5 = 0$. Звідси отримуємо відповідно рівняння наведені у висновку леми.

Одним з знайдених елементів є, наприклад, $v = x^2 + x^4 + x^6 + x^9 + x^{11} + x^3y +$
$+ x^9y + x^{11}y$. Для нього $v^* = x^{10} + x^8 + x^6 + x^3 + x + x^3y + x^9y + x^{11}y \neq v$. В таблиці подано добутки всіх доданків з v на доданки з v^*.

Таблиця 1.

Таблиця добутків доданків з v на доданки з v^*

	x^{10}	x^8	x^6	x^3	x	x^3y	x^9y	$x^{11}y$
x^2	1	x^{10}	x^8	x^5	x^3	x^5y	$x^{11}y$	xy
x^4	x^2	1	x^{10}	x^7	x^5	x^7y	xy	x^3y
x^6	x^4	x^2	1	x^9	x^7	x^9y	x^3y	x^5y
x^9	x^7	x^5	x^3	1	x^{10}	y	x^6y	x^8y
x^{11}	x^9	x^7	x^5	x^2	1	x^2y	x^8y	$x^{10}y$
x^3y	x^5y	x^7y	x^9y	y	x^2y	1	x^6	x^4
x^9y	$x^{11}y$	xy	x^3y	x^6y	x^8y	x^6	1	x^{10}
$x^{11}y$	xy	x^3y	x^5y	x^8y	$x^{10}y$	x^8	x^2	1

Таким чином, $vv^* = 0$. З вигляду v одержимо, що

$$\sigma(v) = \begin{pmatrix}
0&0&1&0&1&0&1&0&0&1&0&1&0&0&0&1&0&0&0&0&0&1&0&1\\
1&0&0&1&0&1&0&1&0&0&1&0&1&0&0&0&1&0&0&0&0&0&1&0\\
0&1&0&0&1&0&1&0&1&0&0&1&0&1&0&0&0&1&0&0&0&0&0&1\\
1&0&1&0&0&1&0&1&0&1&0&0&1&0&1&0&0&0&1&0&0&0&0&0\\
0&1&0&1&0&0&1&0&1&0&1&0&0&1&0&1&0&0&0&1&0&0&0&0\\
0&0&1&0&1&0&0&1&0&1&0&1&0&0&1&0&1&0&0&0&1&0&0&0\\
1&0&0&1&0&1&0&0&1&0&1&0&0&0&0&1&0&1&0&0&0&1&0&0\\
0&1&0&0&1&0&1&0&0&1&0&1&0&0&0&0&1&0&1&0&0&0&1&0\\
1&0&1&0&0&1&0&1&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&1\\
0&1&0&1&0&0&1&0&1&0&0&1&1&0&0&0&0&0&1&0&1&0&0&0\\
1&0&1&0&1&0&0&1&0&1&0&0&0&1&0&0&0&0&0&1&0&1&0&0\\
0&1&0&1&0&1&0&0&1&0&1&0&0&0&1&0&0&0&0&0&1&0&1&0\\
0&1&0&1&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1&0\\
0&0&1&0&1&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1\\
0&0&0&1&0&1&0&0&0&0&0&1&1&0&0&1&0&1&0&0&1&0&1&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0&1&0&0&1&0&1&0&0&1&0&1\\
0&1&0&0&0&1&0&1&0&0&0&0&1&0&1&0&0&1&0&1&0&0&1&0\\
0&0&1&0&0&0&1&0&1&0&0&0&0&1&0&1&0&0&1&0&1&0&0&1\\
0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1&0&0&1&0&1&0&0\\
0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1&0&0&1&0&1&0\\
0&0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1&0&0&1&0&1\\
1&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1&0&0&1&0\\
0&1&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1&0&0&1\\
1&0&1&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&1&0&1&0&0
\end{pmatrix}.$$

Звичайно важко дати теоретичне обґрунтування, але обчислення в системі комп'ютерної алгебри GAP показують, що $\operatorname{rank}(\sigma(v)) = 12$, а мінімальна відстань Хемінга коду $C(v)$ рівна 8. Тобто $C(v)$ є розширений бінарний код Голея.

3. Числові результати. Групова алгебра $\mathbb{F}_2D_{24}$ складається, очевидно, з $2^{24} = 16\ 777\ 216$ елементів v. В результаті обчислень одержуємо кількість елементів $v \in \mathbb{F}_2D_{24}$, що $C(v)$ — розширений бінарний код Голея. Подаємо ці результати для порівняння з кількістю тих же елементів при умові $v = v^*$.

Таблиця 2.

Кількість елементів з групової алгебри $\mathbb{F}_2D_{24}$

Мінімальна відстань Хемінга $C(v)$	2	4	6	8
Кількість елементів v, що $v = v^*$	640	8 704	768	768
Кількість елементів v	19 200	287 232	36 864	36 864

Таким чином, існує рівно 36 864 елементів $v \in \mathbb{F}_2D_{24}$, що $C(v)$ є розширеним бінарним кодом Голея.

4. Висновки та перспективи подальших досліджень. Ця стаття присвячена дослідженню конструкцій розширених бінарних кодів Голея за груповою алгеброю $\mathbb{F}_2G$ групи $G = D_{24}$. Знайдено 36 864 елементів $v \in \mathbb{F}_2D_{24}$, що $C(v)$ є розширеним бінарним кодом Голея. В подальших дослідженнях крім вже розглянутих $(C_6 \times C_2) \rtimes C_2$, D_{24} можна буде розглянути інші групи порядку 24 або групи вищих порядків для отримання кодів більшої довжини.

Автори щиро вдячні професору Бондаренку В. М. за корисні поради та змістовні дискусії при підготовці роботи.

Список використаної літератури

1. Берман С. Д. К теории групповых кодов. *Кибернетика.* 1967. № 1. С. 31–39.
2. Hurley T. Group Rings and Rings of Matrices. *Int. Jour. Pure and Appl. Math.* 2006. Vol. 31. No. 3. P. 319–335.
3. Bernhardt F., Landrock P., Manz O.: The extended Golay codes considered as ideals. J. Comb. Theory Ser. A. 1990. 55(2), 235–246.
4. 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). P. 2115–2138. DOI: 10.1007/s10623-017-0440-7.

5. Бортош М. Ю., Тилищак О. А. Розширені бінарні коди Голея за груповою алгеброю однієї групи. Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. 2020. Вип. 1(36). С. 65–72.
6. McLoughlin I., Hurley T. A group ring construction of the extended binary Golay code. *IEEE Trans. Inform. Theory*. 2008. 9(54). P. 4381–4383.
7. Huffman W. C., Pless V. Fundamentals of error-correcting codes. *Cambridge University*. Press, Cambridge. 2003.
8. Zimmerman K. H. Beiträge zur algebraischen Codierungstheorie mittels modularer Darstellungstheorie. *Bayreuther Math. Schr.* 1994. P. 48.

Bortos M. Yu., Tylyshchak A. A., Khymynets M. V. Extended binary Golay codes by a group algebra of dihedral group.

Many different structures for construction linear binary self-dual codes were established. In the paper we consider the construction of extended binary Golay codes according to the principle ideals (left) of the group algebra $\mathbb{F}_2D_{24}$ of the dihedral group D_{24} of order 24 over a field of two elements $\mathbb{F}_2$. A search algorithm has been developed and all elements $v \in \mathbb{F}_2D_{24}$, which generate the principle ideals that define extended binary Golay codes, have been found programmatically. Previously, in this way the extended binary Golay code was built on one element $v \in \mathbb{F}_2D_{24}$, which $v = v^*$. All 36 864 elements $v \in \mathbb{F}_2D_{24}$ were found, on which the define extended binary Golay codes can be constructed, and it was found that 768 of them satisfy the condition $v = v^*$.–

Keywords: group algebra, extended binary codes, Golay codes, self-dual codes, codes over fields, dihedral group.

References

1. Berman, S. D. (1967). K teoryy hrupovykh kodov [On theory of group codes]. *Kybernetyka, 1*, 31–39. [in Russian].
2. Hurley, T. (2006). Group Rings and Rings of Matrices. *Int. Jour. Pure and Appl. Math, 31(3)*, 319–335.
3. Bernhardt, F. Landrock, P., & Manz, O. (1990). The extended Golay codes considered as ideals. *J. Combin. Theory Ser. A, 55(2)*, 235–246.
4. Dougherty, S. T., Gildea, J., Taylor, R., & Tylyshchak, A. (2018). Group rings, G-codes and constructions of self-dual and formally self-dual codes. *Designs, Codes and Cryptography, 86(9)*, 2115–2138. https://doi.org/10.1007/s10623-017-0440-7.
5. Bortos, M. Yu., & Tylyshchak, A. A. (2020). Extended binary Golay codes by a group algebra of one group. *Scientific Bulletin of Uzhhorod University. Ser. Of Mathematics and Informatics, 1(36)*, 65–72.
6. McLoughlin, I., & Hurley, T. (2008). A group ring construction of the extended binary Golay code. *IEEE Trans. Inform. Theory, 9(54)*, 4381–4383.
7. Huffman, W. C., & Pless, V. (2003). Fundamentals of error-correcting codes. *Cambridge University Press*, Cambridge.
8. Zimmerman, K. H. (1994). Contribution to algebraic coding theory by means of modular representation theory. *Bayreuther Math. Schr. 48.* [in Germany].

Одержано 15.04.2022