

УДК 519.725

DOI [https://doi.org/10.24144/2616-7700.2023.42\(1\).18-23](https://doi.org/10.24144/2616-7700.2023.42(1).18-23)М. Ю. Бортош¹, М. В. Химинець²

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 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 $C_3 \times D_8$

Бінарні коди Голя вивчалися довгий період і було встановлено багато різних конструкцій для їх побудови, а також з'ясовано багато властивостей цих кодів. У статті розглянуто побудову розширених бінарних кодів Голя за головними ідеалами (ліви́ми) групою алгеброю $\mathbb{F}_2(C_3 \times D_8)$ групи $C_3 \times D_8$ порядку 24 над полем з двох елементів \mathbb{F}_2 . Розглядається дія регулярного зображення $v \rightarrow \sigma(v)$ на елементах v групової алгебри. Рядки матриці $\sigma(v)$ породжують лінійний бінарний код $C(v)$. У попередніх дослідженнях з'ясовано кількість всіх елементів v групової алгебри \mathbb{F}_2G скінченних груп $(C_6 \times C_2) \rtimes C_2$ та D_{24} таких, що бінарний код $C(v)$ є розширеним бінарним кодом Голя. Раніше таким способом розширений бінарний код Голя будувався за одним елементом $v \in \mathbb{F}_2G$, що $v = v^*$. В результаті числових обчислень знайдено всі 12 288 елементів $v \in \mathbb{F}_2(C_3 \times D_8)$, за якими можна побудувати розширений бінарний код Голя, серед яких 128 задовольняє умову $v = v^*$.

Ключові слова: групова алгебра, коди Голя, розширені бінарні коди, самодуальні коди, коди над полями.

1. Вступ. У багатьох роботах [1, 3–10] досліджувалися різні підходи побудови і властивості бінарних [23, 12, 7]-кодів та розширених [24, 12, 8]-кодів Голя. [23, 12, 7]-код є добре відомим кодом, має низку властивостей і широке застосування як у загальній математиці, так і в теорії кодування. Хоча розширені бінарні коди Голя не володіють усіма властивостями таких кодів, вони демонструють інші важливі риси. Вперше ці коди були розглянуті Марселем Дж. Е. Голеем у роботі [1] у 1949 році. Математична значимість коду Голя далеко виходить за рамки його властивості виправлення помилок. Розширений бінарний код Голя пов'язаний з групою Матґе M_{24} . Крім того, даний код є головним елементом у побудові 24-вимірної решітки Ліча. Поняття решітки Ліча було відкрито у зв'язку з упакуванням сфер в n -вимірний простір. Він забезпечує найкраще ґратчасте пакування в \mathbb{R}^{24} , розташування одиничних сфер в \mathbb{R}^{24} так, що їхні центри утворюють решітку.

У статті ми розглядатимемо тільки розширені бінарні коди Голя. Для групи $(C_6 \times C_2) \rtimes C_2$ (C_n — циклічна група порядку n) та групи Діедра D_{24} раніше була з'ясована точна кількість всіх елементів, за якими будуються розширені бінарні коди Голя за головним ідеалом групових алгебр даних скінченних груп. У даній роботі розглядаємо таку ж задачу для групи $G = C_3 \times D_8$.

Розглянемо побудову розширених бінарних кодів Голея використовуючи конструкцію запропоновану Т. Харлі у роботі [2]. Нехай $G = \{g_1, g_2, \dots, g_n\}$ — скінченна група порядку n і нехай $v = \sum_{i=1}^n \alpha_{g_i} g_i \in \mathbb{F}_2 G$ ($\alpha_{g_i} \in \mathbb{F}_2$). Для елемента $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \dots + \alpha_{g_n} g_n \in \mathbb{F}_2 G$ позначимо $v^* = \alpha_{g_1} g_1^{-1} + \alpha_{g_2} g_2^{-1} + \dots + \alpha_{g_n} g_n^{-1} \in \mathbb{F}_2 G$. Розглянемо матрицю $\sigma(v) \in M(n, \mathbb{F}_2)$ вигляду

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

Легко бачити, що $\sigma(v)^T = \sigma(v^*)$. Для заданого елемента $v \in \mathbb{F}_2 G$ визначимо $C(v)$, як бінарний код породжений рядками матриці $\sigma(v)$. Розглянемо простір \mathbb{F}_2^n , в якому вводиться скалярний добуток $[v, w] = \sum_{i=1}^n v_i w_i$. $C(v)$ є підпростором простору \mathbb{F}_2^n . Бінарний код C називається *самоортогональним*, якщо $C \subset C^\perp$ і *самодуальним* — якщо $C = C^\perp$, де $C^\perp = \{v \in \mathbb{F}_2^n \mid [v, w] = 0, w \in C\}$. Зрозуміло, що код $C(v)$ самоортогональний, якщо $\sigma(v)\sigma(v)^T = 0$. Відомо [12], що розширений бінарний код Голея самодуальний.

Теорема 1 ([11]). *Нехай G скінченна група порядку 24 з елементом v групової алгебри $\mathbb{F}_2 G$. Якщо*

- 1) $v = v^*$,
- 2) $v^2 = 0$,
- 3) $\text{rank}(\sigma(v)) = 12$,

тоді код $C(v)$ самодуальний.

У [2–4, 11] встановлено, що з 15 неізоморфних груп 24-го порядку, для груп D_{24} , S_4 , $(C_6 \times C_2) \rtimes C_2$, $C_3 \times D_8$, $C_2 \times A_4$ розширений бінарний код Голея будується за достатніми умовами самодуальності коду наведені в теоремі 1. Далі скористаємося таким очевидним критерієм.

Теорема 2 ([5]). *Нехай G скінченна група порядку 24 з елементом v групової алгебри $\mathbb{F}_2 G$. Код $C(v)$ самодуальний тоді і тільки тоді, коли*

- 1) $vv^* = 0$,
- 2) $\text{rank}(\sigma(v)) = 12$.

2. Побудова кодів за групою $G = C_3 \times D_8$.

Лема 1. *Нехай $G = \langle x, y, z \mid x^3 = 1, y^4 = 1, z^2 = 1, xy = yx, xz = zx, yzyz = 1 \rangle$, $v = \sum_{i=0}^3 ((\alpha_{i+1} + \alpha_{i+13}z)y^i + (\alpha_{i+5} + \alpha_{i+17}z)y^i x + (\alpha_{i+9} + \alpha_{i+21}z)y^i x^2)$. Якщо код $C(v)$ самодуальний, тоді*

- 1) $\sum_{i=1}^{24} \alpha_i = 0$,
- 2) $(\alpha_1 + \alpha_3 + \alpha_5 + \alpha_7 + \alpha_9 + \alpha_{11})(\alpha_2 + \alpha_4 + \alpha_6 + \alpha_8 + \alpha_{10} + \alpha_{12}) + (\alpha_{13} + \alpha_{15} + \alpha_{17} + \alpha_{19} + \alpha_{21} + \alpha_{23})(\alpha_{14} + \alpha_{16} + \alpha_{18} + \alpha_{20} + \alpha_{22} + \alpha_{24}) = 0$,
- 3) $(\alpha_1 + \alpha_3 + \alpha_2 + \alpha_4)(\alpha_{17} + \alpha_{18} + \alpha_{19} + \alpha_{20} + \alpha_{21} + \alpha_{22} + \alpha_{23} + \alpha_{24}) + (\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8)(\alpha_{13} + \alpha_{14} + \alpha_{15} + \alpha_{16} + \alpha_{21} + \alpha_{22} + \alpha_{23} + \alpha_{24}) + (\alpha_9 + \alpha_{10} + \alpha_{11} + \alpha_{12})(\alpha_{13} + \alpha_{14} + \alpha_{15} + \alpha_{16} + \alpha_{17} + \alpha_{18} + \alpha_{19} + \alpha_{20}) = 0$,

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

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

$$\gamma_7 = (\alpha_1 + \alpha_5)(\alpha_{11} + \alpha_3) + (\alpha_1 + \alpha_9)(\alpha_3 + \alpha_7) + (\alpha_2 + \alpha_6)(\alpha_{12} + \alpha_4) + (\alpha_2 + \alpha_{10})(\alpha_4 + \\ + \alpha_8) + (\alpha_{13} + \alpha_{17})(\alpha_{23} + \alpha_{15}) + (\alpha_{13} + \alpha_{21})(\alpha_{15} + \alpha_{19}) + (\alpha_{14} + \alpha_{18})(\alpha_{24} + \alpha_{16}) + (\alpha_{14} + \\ + \alpha_{22})(\alpha_{16} + \alpha_{20}),$$

$$\gamma_8 = \alpha_1(\alpha_{10} + \alpha_8) + \alpha_2(\alpha_{11} + \alpha_5) + \alpha_3(\alpha_{12} + \alpha_6) + \alpha_4(\alpha_9 + \alpha_7) + \alpha_{13}(\alpha_{24} + \alpha_{18}) + \\ + \alpha_{14}(\alpha_{21} + \alpha_{19}) + \alpha_{15}(\alpha_{22} + \alpha_{20}) + \alpha_{16}(\alpha_{23} + \alpha_{17}) + \alpha_9\alpha_6 + \alpha_{10}\alpha_7 + \alpha_{11}\alpha_8 + \alpha_{12}\alpha_5 + \\ + \alpha_{17}\alpha_{22} + \alpha_{18}\alpha_{23} + \alpha_{19}\alpha_{24} + \alpha_{20}\alpha_{21},$$

$$\gamma_9 = \alpha_1(\alpha_{23} + \alpha_{19}) + \alpha_2(\alpha_{24} + \alpha_{20}) + \alpha_3(\alpha_{21} + \alpha_{17}) + \alpha_4(\alpha_{22} + \alpha_{18}) + \alpha_5(\alpha_{15} + \alpha_{23}) + \\ + \alpha_6(\alpha_{16} + \alpha_{24}) + \alpha_7(\alpha_{13} + \alpha_{21}) + \alpha_8(\alpha_{14} + \alpha_{22}) + \alpha_9(\alpha_{19} + \alpha_{15}) + \alpha_{10}(\alpha_{20} + \alpha_{16}) + \\ + \alpha_{11}(\alpha_{17} + \alpha_{13}) + \alpha_{12}(\alpha_{18} + \alpha_{14}),$$

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

Звідси отримаємо,

$$\gamma_2 + \gamma_6 + \gamma_8 = (\alpha_1 + \alpha_3 + \alpha_5 + \alpha_7 + \alpha_9 + \alpha_{11})(\alpha_2 + \alpha_4 + \alpha_6 + \alpha_8 + \alpha_{10} + \alpha_{12}) + (\alpha_{13} + \\ + \alpha_{15} + \alpha_{17} + \alpha_{19} + \alpha_{21} + \alpha_{23})(\alpha_{14} + \alpha_{16} + \alpha_{18} + \alpha_{20} + \alpha_{22} + \alpha_{24}).$$

$$\gamma_3 + \gamma_4 + \gamma_9 + \gamma_{10} = (\alpha_1 + \alpha_3 + \alpha_2 + \alpha_4)(\alpha_{22} + \alpha_{18} + \alpha_{20} + \alpha_{24} + \alpha_{23} + \alpha_{19} + \alpha_{21} + \\ + \alpha_{17}) + (\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8)(\alpha_{14} + \alpha_{22} + \alpha_{16} + \alpha_{24} + \alpha_{15} + \alpha_{23} + \alpha_{13} + \alpha_{21}) + (\alpha_9 + \alpha_{10} + \\ + \alpha_{11} + \alpha_{12})(\alpha_{18} + \alpha_{14} + \alpha_{20} + \alpha_{16} + \alpha_{19} + \alpha_{15} + \alpha_{17} + \alpha_{13}).$$

Якщо код $C(v)$ самодуальний, то за умовою 1 теореми 2 виконуються умови: $vv^* = 0$ і $\sigma(v)\sigma(v)^T = \sigma(vv^*) = 0$. Таким чином, $\gamma_i = 0$ ($i = 1, \dots, 10$). Тоді $\gamma_1 = 0$, $\gamma_2 + \gamma_6 + \gamma_8 = 0$, $\gamma_3 + \gamma_4 + \gamma_9 + \gamma_{10} = 0$, $\gamma_5 = 0$, $\gamma_7 = 0$. Звідси отримуємо відповідно рівняння наведені у висновку леми.

Одним зі знайдених елементів є, наприклад, $v = y^3x^2 + z + zy + zx + zyx + zx^2 + zy^2x^2 + zy^3x^2$. Для нього $v^* = yx + z + zy + zx^2 + zyx^2 + zx + zy^2x + zy^3x \neq v$. В таблиці подано добутки всіх доданків з v на доданки з v^* .

Таблиця 1.

Таблиця добутків доданків з v на доданки з v^*

	yx	z	zy	zx^2	zyx^2	zx	zy^2x	zy^3x
y^3x^2	1	zyx^2	zy^2x^2	zyx	zy^2x	zy	zy^3	z
z	zyx	1	y	x^2	yx^2	x	y^2x	y^3x
zy	zy^2x	y^3	1	y^3x^2	x^2	y^3x	yx	y^2x
zx	zyx^2	x	yx	1	y	x^2	y^2x^2	y^3x^2
zyx	zy^2x^2	y^3x	x	y^3	1	y^3x^2	yx^2	y^2x^2
zx^2	zy	x^2	yx^2	x	yx	1	y^2	y^3
zy^2x^2	zy^3	y^2x^2	y^3x^2	y^2x	y^3x	y^2	1	y
zy^3x^2	z	yx^2	y^2x^2	yx	y^2x	y	y^3	1

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

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

Обчислення в системі комп'ютерної алгебри GAP показують, що $\text{rank}(\sigma(v)) = 12$, а мінімальна відстань Хемінга коду $C(v)$ рівна 8. Таким чином, $C(v)$ є розширеним бінарним кодом Голя.

3. Числові результати. Групова алгебра $\mathbb{F}_2(C_3 \times D_8)$ складається, очевидно, з $2^{24} = 16\,777\,216$ елементів v . В результаті обчислень отримуємо кількість елементів $v \in \mathbb{F}_2(C_3 \times D_8)$, що $C(v)$ — розширений бінарний код Голя. Подаємо ці результати разом з кількістю тих же елементів при умові $v = v^*$.

Таблиця 2.

Кількість елементів з групової алгебри $\mathbb{F}_2(C_3 \times D_8)$

Мінімальна відстань Хемінга $C(v)$	2	4	6	8
Кількість елементів v , що $v = v^*$	128	1 216	128	128
Кількість елементів v	7 680	92 160	12 288	12 288

Таким чином, існує рівно 12 288 елементів $v \in \mathbb{F}_2(C_3 \times D_8)$, що $C(v)$ є розширеним бінарним кодом Голя.

4. Висновки та перспективи подальших досліджень. У статті досліджено конструкції розширених бінарних кодів Голя за груповою алгеброю \mathbb{F}_2G групи $G = C_3 \times D_8$. Знайдено 12 288 елементів $v \in \mathbb{F}_2(C_3 \times D_8)$, що $C(v)$ є розширеним бінарним кодом Голя. В подальших дослідженнях, крім вже розглянутих $(C_6 \times C_2) \rtimes C_2$, D_{24} , $C_3 \times D_8$, можна буде розглянути інші групи порядку 24, наприклад групи $C_2 \times A_4$ та S_4 .

Автори щиро вдячні професору Тилищаку О. А. за цінні поради при обговоренні результатів.

Список використаної літератури

1. Golay M. J. Notes on digital coding. *Proc. I.R.E.* 1949. Vol. 37, No. 6. 657 pp.
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. Vol. 55, No. 2, P. 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. Vol. 86, No. 9. P. 2115–2138. DOI: <https://doi.org/10.1007/s10623-017-0440-7>.
5. Бортош М. Ю., Тилищак О. А. Розширені бінарні коди Голя за груповою алгеброю однієї групи. *Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ.* 2020. Вип. 1, № 36. С. 65–72.
6. Бортош М. Ю., Тилищак О. А., Химинець М. В. Розширені бінарні коди Голя за груповою алгеброю групи діедра. *Науковий вісник Ужгородського університету. Серія «Математика і інформатика».* 2022. Вип. 40, № 1, С. 27–32.

7. Pless V. On the uniqueness of the Golay codes. *J. Combin. Theory*. 1968. Vol. 5, No. 3. P. 215–228.
8. Peng X. H., Farrell P. G. On construction of the (24, 12, 8) Golay codes. *IEEE Trans. Inform. Theory*. 2006. Vol. 8, No. 52. P. 3669–3675.
9. Curtis R. T. Error-correction and the binary Golay code. *London Mathematical Society*. 2016. Vol. 150, No. 1, P. 51–58.
10. McLoughlin I. Dihedral codes. 2009. URL: <http://hdl.handle.net/10379/6401>
11. McLoughlin I., Hurley T. A group ring construction of the extended binary Golay code. *IEEE Trans. Inform. Theory*. 2008. Vol. 9, No. 54. P. 4381–4383.
12. Huffman W. C., Pless V. Fundamentals of error-correcting codes. Cambridge University : Press, Cambridge, 2003. 646 pp.

Bortos M. Yu., Khymynets M. V. Extended binary Golay codes by a group algebra of the group $C_3 \times D_8$.

Binary Golay codes have been studied for a prolonged period of time and many different structures of their construction have been established as well as a certain amount of their properties has been revealed. In the article the construction of extended binary Golay has been considered according to the principle ideals (left) of the group algebra $\mathbb{F}_2(C_3 \times D_8)$ of the group $C_3 \times D_8$ of order 24 over a field of two elements \mathbb{F}_2 . The action of the regular representation $v \rightarrow \sigma(v)$ on the elements v of the group algebra is considered. The rows of the matrix $\sigma(v)$ generate a linear binary code $C(v)$. In preceding studies, the number of all elements v of the group algebra \mathbb{F}_2G of finite groups $(C_6 \times C_2) \rtimes C_2$ and D_{24} such that the binary code $C(v)$ is an extended binary Golay code was established. Previously, in this way the extended binary Golay code was built on one element $v \in \mathbb{F}_2G$, which $v = v^*$. As a result of numerical calculations, all the 12 288 elements of $v \in \mathbb{F}_2(C_3 \times D_8)$ were found, on which the extended binary Golay codes can be constructed. Among them 128 satisfy the condition $v = v^*$.

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

References

1. Golay, M. J. (1949). Notes on digital coding. *Proc. I.R.E.*, 37(6), 657.
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. Bortos, M. Yu., Tylyshchak, A. A., & Khymynets, M. V. (2022). Extended binary Golay codes by a group algebra of dihedral group. *Scientific Bulletin of Uzhhorod University. Series of Mathematics and Informatics*, 40(1), 27–32.
7. Pless, V. (1968). On the uniqueness of the Golay codes. *J. Combin. Theory*, 5(3), 215–228.
8. Peng, X. H., & Farrell, P. G. (2006). On construction of the (24, 12, 8) Golay codes. *IEEE Trans. Inform. Theory*, 8(52), 3669–3675.
9. Curtis, R. T. (2016). Error-correction and the binary Golay code. *London Mathematical Society*, 150(1), 51–58.
10. McLoughlin, I., & Hurley, T. (2008). A group ring construction of the extended binary Golay code. *IEEE Trans. Inform. Theory*, 9(54), 4381–4383.
11. McLoughlin, I. (2009). Dihedral codes. Retrieved from <http://hdl.handle.net/10379/6401>
12. Huffman, W. C., & Pless, V. (2003). *Fundamentals of error-correcting codes*. Cambridge University Press: Cambridge.

Одержано 28.04.2023