УДК 519.725
DOI https://doi.org/10.24144/2616-7700.2020.1(36).65-72

М. Ю. Бортош[1], О. А. Тилищак[2]

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

[2] ДВНЗ «Ужгородський національний університет»,
доцент кафедри алгебри,
кандидат фізико-математичних наук
alxtlk@gmail.com
ORCID: https://orcid.org/0000-0001-7828-3416

РОЗШИРЕНІ БІНАРНІ КОДИ ГОЛЕЯ ЗА ГРУПОВОЮ АЛГЕБРОЮ ОДНІЄЇ ГРУПИ

Розширені бінарні коди Голея є прикладом екстремальних бінарних самодуальних кодів типу II (лінійних бінарних самодуальних кодів з відстаню Хемінга між довільними кодовими словами кратною 4, що має найбільшу можливу мінімальну відстань Хемінга серед таких кодів з фіксованою розмірністю простору кодових слів та їх довжиною). Такі коди вивчалися довгий період і було встановлено багато різних конструкцій для побудови цих кодів. Крім того, розширені бінарні коди Голея можна легко одержати з бінарних кодів Голея і навпаки. А останні є досконалими і разом з бінарними кодами Хемінга дають всі можливі параметри нетривіальних бінарних досконалих кодів.

У статті розглядається конструкція лінійних бінарних кодів, зокрема, розширених бінарних кодів Голея за груповою алгеброю $\mathbb{F}_2G$ скінченної групи $G = (C_6 \times C_2) \rtimes C_2$ порядку $n = 24$ над полем з двох елементів $\mathbb{F}_2$. Розширений бінарний код Голея визначається як будь-який бінарний лінійний код, для якого довжина кодових слів рівна 24, розмірність підпростору кодових слів – 12, а мінімальна відстань Хемінга коду – 8, тобто будь-який лінійний бінарний [24,12,8]-код. При дослідженні даних кодів застосовуємо елементи теорії зображень, зокрема розглядаємо регулярне зображення $v \to \sigma(v)$ алгебри $\mathbb{F}_2G$. Для даного елемента v визначаємо бінарний код $C(v)$, як підпростір простору $\mathbb{F}_2^n$ породжений рядками матриці $\sigma(v)$. Було використано критерія самодуальних кодів $C(v)$ для довільної скінченної групи G порядку 24 та знайдено легко вивірювані необхідні умови самодуальності бінарного коду $C(v)$ для елементів v групової алгеброю $\mathbb{F}_2G$ групи $G = (C_6 \times C_2) \rtimes C_2$. В результаті числових обчислень, що передбачає перевірку знайдених необхідних умов, отримаємо кількість елементів $v \in \mathbb{F}_2G$, що $C(v)$ є самодуальним кодом. Кількісні результати подані для порівняння з кількістю тих же елементів при умові $v = v^*$. Раніше в такому вигляді розширені бінарні коди Голея були знайдені тільки для елементів v, що $v = v^*$. При обчисленнях отримано всі 27 648 елементів v групової алгебри $\mathbb{F}_2G$, що $C(v)$ є розширеним бінарним кодом Голея.

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

1. Вступ. Розглянемо конструкцію лінійних бінарних кодів запропоновану Т. Харлі в [1]. Метод реалізовує піонерський підхід С. Д. Бермана [2] (див. також [11]), що розглядає односторонні ідеали в групових алгебрах скінченних груп над скінченними полями, як коди над тими ж полями.

Нехай $\mathbb{F}_2$ — поле з двох елементів, $G = \{g_1, g_2, \ldots, g_n\}$ — 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

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

Відображення $v \to \sigma(v)$ розглядається в теорії зображень скінченних груп над полями, як *регулярне зображення* алгебри $\mathbb{F}_2G$, що відповідає такому порядку $g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}$ елементів групи G. 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. Бінарний самодуальний код, для якого відстань Хемінга між довільними кодовими словами кратна 4 називається бінарним самодуальним кодом *типу II*, а в іншому випадку бінарним самодуальним кодом *типу I*. Верхня межа мінімальної відстані бінарних самодуальних кодів була знайдена в [3].

Теорема 1. *Нехай $d_I(n)$ і $d_{II}(n)$ мінімальна відстань бінарного коду довжини n типу I і II, відповідно. Тоді*

$$d_{II}(n) \leq 4\left[\frac{n}{24}\right] + 4$$

і

$$d_I(n) \leq \begin{cases} 4\left[\frac{n}{24}\right] + 4 & \text{if } n \not\equiv 22 \pmod{24}, \\ 4\left[\frac{n}{24}\right] + 6 & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

Тут $[x]$ позначає цілу частину числа x.

Бінарний самодуальний код типу I і II, мінімальна відстань якого досягає вказаних в теоремі крайніх значень, називається *екстремальним*. Прикладами екстремальних бінарних самодуальних кодів типу II є розширені бінарні коди Голея (див. [8]), які вперше було розглянуто Марселем Дж. Е. Голеєм в статті [4] в 1949 році. З тих пір такі коди вивчали багато разів і були встановлені багато різних конструкцій для побудови цих кодів в [5–7]. *Розширений бінарний код Голея* визначається, як будь-який бінарний лінійний [24,12,8]-код.

У [9] розширений бінарний код Голея було побудовано у вигляді $C(v)$ для деякого елемента v з групової алгебри $\mathbb{F}_2S_4$, де S_4 — симетрична група порядку 24. У [7] аналогічний результат одержано для групи D_{24} діедра порядку 24. При побудові використовувалася таке твердження.

Теорема 2 ([7]). *Нехай G скінченна група порядку 24 з елементом v групової алгебри $\mathbb{F}_2G$. Якщо*

1) $v = v^*$,

2) $v^2 = 0$,

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

тоді код $C(v)$ самодуальний.

У [10] встановлено, що з 15 неізоморфних груп 24-го порядку таким способом можна побудувати код також для груп $(C_6 \times C_2) \rtimes C_2$, $C_3 \times D_8$, $C_2 \times A_4$. Теорема 2 дає достатню умову, щоб код $C(v)$ був розширеним бінарним кодом Голея для елемента v групової алгебри $\mathbb{F}_2G$ групи G порядку 24. В [10] показано, що для решти груп 24-го порядку розширений бінарний код Голея за теоремою 2 побудувати не можна. Скористаємося таким очевидним критерієм.

Теорема 3. *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) $\mathrm{rank}(\sigma(v)) = 12$.

В статті знаходяться всі елементи v групової алгебри $\mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$, що $C(v)$ є розширеним бінарним кодом Голея.

2. Побудова кодів за групою $G = (C_6 \times C_2) \rtimes C_2$.

Лема 1. *Нехай $G = (C_6 \times C_2) \rtimes C_2 = \langle x, y, z \,|\, x^3 = 1, y^4 = 1, z^2 = 1, yz = zy^3, xy = yx^2, xz = zx\rangle$,*

$$v = \sum_{i=0}^{3} (\alpha_{i+1} + \alpha_{i+5}x + \alpha_{i+9}x^2)y^i + (\alpha_{i+13} + \alpha_{i+17}x + \alpha_{i+21}x^2)y^i z.$$

Якщо код $C(v)$ самодуальний, тоді $\sum_{i=1}^{24} \alpha_i = 0$,

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

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

$$(\alpha_1+\alpha_3+\alpha_5+\alpha_7)(\alpha_{13}+\alpha_{15}+\alpha_{21}+\alpha_{23})+(\alpha_1+\alpha_3+\alpha_9+\alpha_{11})(\alpha_{13}+\alpha_{15}+\alpha_{17}+\alpha_{19})+$$

$$(\alpha_2+\alpha_4+\alpha_6+\alpha_8)(\alpha_{14}+\alpha_{16}+\alpha_{22}+\alpha_{24})+(\alpha_2+\alpha_4+\alpha_{10}+\alpha_{12})(\alpha_{14}+\alpha_{16}+\alpha_{18}+\alpha_{20}) = 0.$$

$$(\alpha_1+\alpha_5)(\alpha_{23}+\alpha_{15})+(\alpha_1+\alpha_9)(\alpha_{15}+\alpha_{19})+(\alpha_2+\alpha_6)(\alpha_{22}+\alpha_{14})+(\alpha_2+\alpha_{10})(\alpha_{14}+\alpha_{18})+$$

$$(\alpha_3 + \alpha_7)(\alpha_{21} + \alpha_{13}) + (\alpha_3 + \alpha_{11})(\alpha_{13} + \alpha_{17}) + (\alpha_4 + \alpha_8)(\alpha_{24} + \alpha_{16}) +$$

$$(\alpha_4 + \alpha_{12})(\alpha_{16} + \alpha_{20}) = 0,$$

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

$$(\alpha_4+\alpha_8)(\alpha_4+\alpha_{12})+\alpha_{13}+(\alpha_{13}+\alpha_{17})(\alpha_{13}+\alpha_{21})+\alpha_{14}+(\alpha_{14}+\alpha_{18})(\alpha_{14}+\alpha_{22})+\alpha_{15}+$$

$$(\alpha_{15} + \alpha_{19})(\alpha_{15} + \alpha_{23}) + \alpha_{16} + (\alpha_{16} + \alpha_{20})(\alpha_{16} + \alpha_{24}) = 0.$$

Доведення. Обчислення в групі $G = (C_6 \times C_2) \rtimes C_2$ 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_4 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{19} \\
\alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{22} \\
\alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{17} \\
\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_5 & \alpha_6 & \alpha_7 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{23} \\
\alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{18} \\
\alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{21} \\
\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_{12} & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{15} \\
\alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{14} \\
\alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{13} \\
\alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_{10} \\
\alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 \\
\alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_{12} \\
\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_{21} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 \\
\alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_{11} \\
\alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_7 & \alpha_6 & \alpha_5 & \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_{17} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 \\
\alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 \\
\alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 \\
\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}.$$

Безпосередні обчислення показують, що матриця $\sigma(v)\sigma(v)^T = \sigma(vv^*)$ набуває вигляду:

$$\begin{pmatrix}
\gamma_1 & \gamma_2 & 0 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_6 & \gamma_5 & \gamma_6 & 0 & 0 & 0 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 \\
\gamma_2 & \gamma_1 & \gamma_2 & 0 & \gamma_6 & \gamma_3 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & 0 & 0 & 0 & 0 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 \\
0 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & \gamma_3 & \gamma_6 & 0 & 0 & 0 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 \\
\gamma_2 & 0 & \gamma_2 & \gamma_1 & \gamma_6 & \gamma_5 & \gamma_6 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & 0 & 0 & 0 & 0 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 \\
\gamma_3 & \gamma_6 & \gamma_5 & \gamma_6 & \gamma_1 & \gamma_2 & 0 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_7 & 0 & \gamma_8 & 0 & 0 & 0 & 0 & 0 & \gamma_7 & 0 & \gamma_8 & 0 \\
\gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_2 & \gamma_1 & \gamma_2 & 0 & \gamma_6 & \gamma_3 & \gamma_6 & \gamma_5 & 0 & \gamma_5 & 0 & \gamma_8 & 0 & 0 & 0 & 0 & 0 & \gamma_7 & 0 & \gamma_8 \\
\gamma_5 & \gamma_6 & \gamma_3 & \gamma_6 & 0 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_8 & 0 & \gamma_7 & 0 & 0 & 0 & 0 & 0 & \gamma_8 & 0 & \gamma_7 & 0 \\
\gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & 0 & \gamma_2 & \gamma_1 & \gamma_6 & \gamma_5 & \gamma_6 & \gamma_3 & 0 & \gamma_6 & 0 & \gamma_7 & 0 & 0 & 0 & 0 & 0 & \gamma_8 & 0 & \gamma_7 \\
\gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_6 & \gamma_5 & \gamma_6 & \gamma_1 & \gamma_2 & 0 & \gamma_2 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & 0 & 0 & 0 & 0 \\
\gamma_6 & \gamma_3 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_2 & \gamma_1 & \gamma_2 & 0 & 0 & 0 & \gamma_5 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & 0 & 0 \\
\gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & \gamma_3 & \gamma_6 & 0 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & 0 & 0 & 0 & 0 \\
\gamma_6 & \gamma_5 & \gamma_6 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & 0 & \gamma_2 & \gamma_1 & 0 & \gamma_6 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_1 & \gamma_2 & 0 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_6 & \gamma_5 & \gamma_6 \\
0 & 0 & 0 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_2 & \gamma_1 & \gamma_2 & 0 & \gamma_6 & \gamma_3 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 \\
0 & 0 & 0 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & 0 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & \gamma_3 & \gamma_6 \\
0 & 0 & 0 & 0 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & \gamma_2 & 0 & \gamma_2 & \gamma_1 & \gamma_6 & \gamma_5 & \gamma_6 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 \\
\gamma_7 & 0 & \gamma_8 & 0 & 0 & 0 & 0 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_3 & \gamma_6 & \gamma_5 & \gamma_6 & \gamma_1 & \gamma_2 & 0 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 \\
0 & \gamma_7 & 0 & \gamma_8 & 0 & 0 & 0 & 0 & 0 & \gamma_7 & 0 & \gamma_8 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_2 & \gamma_1 & \gamma_2 & 0 & \gamma_6 & \gamma_3 & \gamma_6 & \gamma_5 \\
\gamma_8 & 0 & \gamma_7 & 0 & 0 & 0 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & 0 & \gamma_5 & \gamma_6 & \gamma_3 & \gamma_6 & 0 & \gamma_2 & \gamma_1 & \gamma_2 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 \\
0 & \gamma_8 & 0 & \gamma_7 & 0 & 0 & 0 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_2 & 0 & \gamma_2 & \gamma_1 & \gamma_6 & \gamma_5 & \gamma_6 & \gamma_3 \\
\gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & 0 & 0 & 0 & 0 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_6 & \gamma_1 & \gamma_2 & 0 & \gamma_2 \\
0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & 0 & 0 & 0 & \gamma_6 & \gamma_3 & \gamma_6 & \gamma_5 & \gamma_4 & \gamma_8 & \gamma_4 & \gamma_5 & \gamma_2 & \gamma_1 & \gamma_2 & 0 \\
\gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & 0 & 0 & 0 & 0 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_5 & \gamma_4 & \gamma_3 & \gamma_6 & 0 & \gamma_2 & \gamma_1 & \gamma_2 \\
0 & \gamma_8 & 0 & \gamma_7 & 0 & \gamma_8 & 0 & \gamma_7 & 0 & 0 & 0 & 0 & \gamma_6 & \gamma_5 & \gamma_6 & \gamma_3 & \gamma_4 & \gamma_7 & \gamma_4 & \gamma_3 & \gamma_2 & 0 & \gamma_2 & \gamma_1
\end{pmatrix},$$

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

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

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

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

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

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

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

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

Звідси отримаємо,

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

$\gamma_7+\gamma_8 = (\alpha_1+\alpha_3+\alpha_5+\alpha_7)(\alpha_{13}+\alpha_{15}+\alpha_{21}+\alpha_{23})+(\alpha_1+\alpha_3+\alpha_9+\alpha_{11})(\alpha_{13}+$
$+\alpha_{15}+\alpha_{17}+\alpha_{19})+(\alpha_2+\alpha_4+\alpha_6+\alpha_8)(\alpha_{14}+\alpha_{16}+\alpha_{22}+\alpha_{24})+(\alpha_2+\alpha_4+\alpha_{10}+$
$+\alpha_{12})(\alpha_{14}+\alpha_{16}+\alpha_{18}+\alpha_{20})$.

Якщо код $C(v)$ самодуальний, то за умовою 1 теореми 3 виконуються умови: $vv^* = 0$ і $\sigma(v)\sigma(v)^T = \sigma(vv^*) = 0$ а, отже, $\gamma_i = 0$ $(i = 1,\dots,8)$. Тоді $\gamma_1 = 0$, $\gamma_2+\gamma_4+\gamma_6 = 0$, $\gamma_7+\gamma_8 = 0$, $\gamma_8 = 0$, $\gamma_3 = 0$. Звідси отримуємо відповідно рівняння наведені у висновку леми.

Одним з знайдених елементів є, наприклад, $v = y^2+x^2+x^2y^2+yz+xz+xy^3z+$ $x^2y^2z+x^2y^3z$. Для нього $v^* = y^2+x+xy^2+yz+x^2z+xy^3z+xy^2z+x^2y^3z \neq v^*$. В таблиці подано добутки всіх доданків з v на доданки з v^*.

Таблиця 1. Таблиця добутків доданків з v на доданки з v^*

	y^2	x	xy^2	yz	x^2z	xy^3z	xy^2z	x^2y^3z
y^2	1	xy^2	x	y^3z	x^2y^2z	xyz	xz	x^2yz
x^2	x^2y^2	1	y^2	x^2yz	xz	y^3z	y^2z	xy^3z
x^2y^2	x^2	y^2	1	x^2y^3z	xy^2z	yz	z	xyz
yz	y^3z	x^2yz	x^2y^3z	1	xy	x^2y^2	x^2y^3	xy^2
xz	xy^2z	x^2z	x^2y^2z	xy^3	1	x^2y	x^2y^2	y
xy^3z	xyz	y^3z	yz	xy^2	x^2y^3	1	y	x^2
x^2y^2z	x^2z	y^2z	z	x^2y	xy^2	y^3	1	xy^3
x^2y^3z	x^2yz	xy^3z	xyz	x^2y^2	y^3	x	xy	1

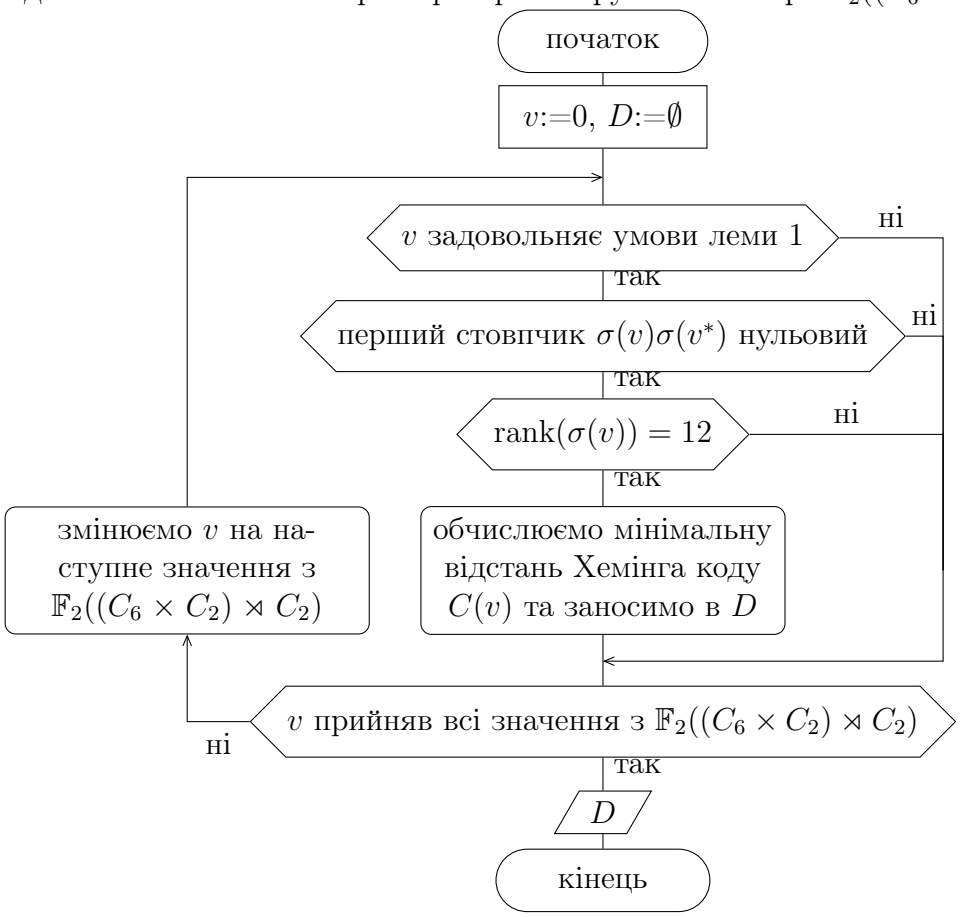
Таким чином, $vv^* = 0$. З вигляду v одержимо, що

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

Звичайно важко дати теоретичне обґрунтування, але обчислення в GAP пока-

зують, що $\mathrm{rank}(\sigma(v)) = 12$, а мінімальна відстань Хемінга коду $C(v)$ рівна 8. Тобто $C(v)$ є розширений бінарний код Голея.

3. Числові результати. Групова алгебра $\mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$ складається, очевидно, з $2^{24} = 16\ 777\ 216$ елементів v. Зрозуміло $vv^* = 0$ тоді і тільки тоді, коли $\sigma(vv^*) = 0$. Всі інші стовпчики матриці $\sigma(vv^*) = 0$ отримуються з першого деякою зміною порядку його компонент, тому $vv^* = 0$ тоді і тільки тоді, коли перший стовпчик $\sigma(vv^*) = \sigma(v)\sigma(v^*)$ нульовий. Ми організовуємо наступний порядок обчислень в GAP при переборі v з групової алгебри $\mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$.



В результаті обчислень одержуємо кількість елементів $v \in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$, що $C(v)$ — самодуальний код. Подаємо ці результати для порівняння з кількістю тих же елементів при умові $v = v^*$.

Таблиця 2. Кількість елементів з групової алгебри $\mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$

Мінімальна відстань Хемінга $C(v)$	2	4	6	8
Кількість елементів v, що $v = v^*$	416	4 192	576	576
Кількість елементів v	11 520	182 016	27 648	27 648

Таким чином, існує рівно 27 648 елементів $v \in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$, 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 $G = (C_6 \times C_2) \rtimes C_2$. Знайдено 27 648 елементів $v \in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$, що $C(v)$ є розширеним бінарним кодом Голея. В подальших дослідженнях 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. Hurley T. Group Rings and Rings of Matrices. *Int. Jour. Pure and Appl. Math.* 2006. 31, no. 3. P. 319–335.
2. Берман С. Д. К теории групповых кодов. *Кибернетика.* 1967. № 1. С. 31-39.
3. Rains E. M. Shadow Bounds for Self Dual Codes. *IEEE Trans. Inf. Theory.* 1998. vol. 44. P. 134–139.
4. Golay M. J. Notes on digital coding. Proc. I.R.E., 1949. 37(6). 657 pp.
5. Peng X. H., Farrell P. G. On construction of the $(24, 12, 8)$ Golay codes. *IEEE Trans. Inform. Theory.* 2006. 8 (52). P. 3669–3675.
6. Kanemasu M. Golay codes. *MIT Undergraduate J. Math.*. 1999. 1. P. 95–99.
7. McLoughlin I., Hurley T. A group ring construction of the extended binary Golay code. *IEEE Trans. Inform. Theory.* 2008. 9 (54). P. 4381–4383.
8. Huffman W. C., Pless V. Fundamentals of error-correcting codes. *Cambridge University.* Press, Cambridge. 2003.
9. Bernhardt F., Landrock P., Manz O. The extended Golay codes considered as ideals. *J. Combin. Theory.* 1990. Ser. A, 55, no. 2. P. 235 - 246.
10. 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.
11. Zimmerman K.-H. Beiträge zur algebraischen Codierungstheorie mittels modularer Darstellungstheorie. *Bayreuther Math. Schr.* 1994. P. 48.

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

Extended binary Golay codes are examples of extreme binary self-dual codes of Type II (linear binary self-dual codes with Hamming distance between arbitrary codewords which are multiples of 4 that has the highest possible minimum Hamming distance among such codes with a fixed dimension of codeword space and their length). These codes have been studied for a long time and many different constructions have been established to build these codes. In addition, extended binary Golay codes are easy to obtain from binary Golay codes and vice versa. The latter are perfect codes and together with binary codes they give us all possible parameters of nontrivial binary perfect codes.

In the paper the construction of linear binary codes, in particular of binary Golay codes extended by the group algebra $\mathbb{F}_2G$ of finite group $G = (C_6 \times C_2) \rtimes C_2$ of order $n = 24$ over the field of two elements $\mathbb{F}_2$ has been considered. Extended binary Golay code is defined as any binary linear code, for which the length of the codewords is 24, the dimension of the subspase of the codewords is 12 and the minimum Hamming distance of the code is 8, that is, any [24,12,8]-code. Considering these codes, we apply the elements of the presentation theory, in particular regular presentations $v \to \sigma(v)$ of algebra $\mathbb{F}_2G$. For the element v we define the binary code $C(v)$ as the subspace of $\mathbb{F}_2^n$ generated by the rows of the matrix $\sigma(v)$. The criterion of self-dual codes $C(v)$ for an arbitrary finite group G of order 24 was used and easily verified necessary conditions for binary code $C(v)$ for elements v of group algebra $\mathbb{F}_2G$ of the group $G = (C_6 \times C_2) \rtimes C_2$ to be self-dual was found. As a result of numerical calculations which involves verifying the found necessary conditions, we get the number of elements $v \in \mathbb{F}_2G$ that $C(v)$ is self-dual. Quantitative results for comparison with the number of the same elements when $v = v^*$ are presented. Previously, in this form, extended binary Golay codes were found only for elements v that $v = v^*$. As a result of calculations we obtained all 27 648 elements v of group algebra $\mathbb{F}_2G$ that $C(v)$ is extended binary Golay code.

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

References

1. Hurley, T. (2006). Group Rings and Rings of Matrices. *Int. Jour. Pure and Appl. Math, 31, no. 3*, 319–335.
2. Berman, S. D. (1967). K teoryy hrupovykh kodov [On theory of group codes]. *Kybernetyka, no. 1*, 31-39. [in Russian]
3. Rains, E. M. (1998). Shadow Bounds for Self Dual Codes. *IEEE Trans. Inf. Theory, vol. 44*, 134–139.
4. Golay, M. J. (1949). Notes on digital coding. *Proc. I.R.E., 37 (6)*, 657.
5. Peng, X. H., & Farrell, P. G. (2006). On construction of the $(24, 12, 8)$ Golay codes. *IEEE Trans. Inform. Theory, 8 (52)*, 3669–3675.
6. Kanemasu, M. (1999). Golay codes. *MIT Undergraduate J. Math., 1*, 95–99.
7. McLoughlin, I., & Hurley, T. (2008). A group ring construction of the extended binary Golay code. *IEEE Trans. Inform. Theory, 9 (54)*, 4381–4383.
8. Huffman, W. C., & Pless, V. (2003). Fundamentals of error-correcting codes. *Cambridge University Press*, Cambridge
9. Bernhardt, F. Landrock, P., & Manz, O. (1990). The extended Golay codes considered as ideals. *J. Combin. Theory Ser. A, 55, no. 2*, 235 - 246.
10. 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. DOI: 10.1007/s10623-017-0440-7.
11. Zimmerman, K. H. (1994). Contribution to algebraic coding theory by means of modular representation theory. *Bayreuther Math. Schr. 48*. [in Germany]

Одержано 30.04.2020