УДК 004.492

КАЛІНОВСЬКИЙ Я.О.,
БОЯРІНОВА Ю.Є.,
ХІЦКО Я.В.,
ГОРОДЬКО Н.О.

МНОЖИННІСТЬ НЕКАНОНІЧНИХ ГІПЕРКОМПЛЕКСНИХ ЧИСЛОВИХ СИСТЕМ СКІНЧЕННОЇ ВИМІРНОСТІ

У статті розглядається спосіб отримання безлічі неканонічних гіперкомплексних систем методом переходу від нескінченновимірної гіперкомплексної системи до скінченновимірних гіперкомплексних систем різного вигляду, залежно від правил множення і методу факторизації. Системи, знайдені запропонованим методом, починаючи з третьої розмірності, є неканонічними. Отримані системи кратній розмірності можна повторно факторизувати і отримати гіперкомплексну числову систему розмірності в два рази меньше.

The subject of the article is a method of obtaining a list of non-canonical hypercomplex systems by the transition from the infinite to the finite hypercomplex number system of different types, depending on the rules of multiplication and factorization method. Systems that have been found by the proposed method, starting from the third dimension are non-canonical. The resulting systems of multiple dimensions can be re-factored to obtain hypercomplex system of dimension in half.

Вступ

Гіперкомплексна форма представлення даних є широко використовуваної для підвищення ефективності алгоритмів в різних галузях науки і техніки[1]. Найчастіше використовуються канонічні гіперкомплексні числові системи (ГЧС), такі як системи комплексних, подвійних, дуальних чисел, кватерніонів та ін [2]. У деяких задачах можна використовувати ще і різні неканонічні гіперкомплексні числові системи для того, щоб підвищити ефективність алгоритмів, або, як наприклад, в криптографічних задачах, підвищити складність злому даних зловмисником, - залежно від обраної числової системи [3-4].

Аналіз існуючих методів отримання нових гіперкомплексних числових систем

Ознака канонічності гіперкомплексної числової системи визначається добутком пар базисних елементів: якщо всі ці добутки дорівнюють одному з базисних елементів з коефіцієнтом з множини $\{-1;0;+1\}$, то така система називається канонічною. Якщо ж хоч один добуток базисних елементів є сумою двох або більшої кількості доданків і / або з коефіцієнтом, який за межами множини $\{-1;0;+1\}$, то така гіперкомплексна числова система називається неканонічною [1].

Для дослідження можливості застосування неканонічних ГЧС важливим питанням є побудова таких систем. У самому загальному випадку, побудова неканонічних ГЧС, здійснюється за допомогою перебору структурних констант при базисних елементах в комірках таблиці множення. При цьому встановлюється обмеження на діапазон значень структурних констант, наявність одиничного елемента, лінійну незалежність базисних елементів. Також, відомий метод отримання списку неканонічних ГЧС, ізоморфних конкретній системі, за допомогою перебору коефіцієнтів у системі лінійних рівнянь [4-5].

Метод факторизації нескінченновимірної гіперкомплексної числової системи

Розглянемо такий підхід отримання безлічі неканонічних гіперкомплексних систем, як перехід від нескінченновимірної гіперкомплексної системи [6] до скінчено-вимірної гіперкомплексної системи різного вигляду, залежно від правил множення і методу факторизації.

Нехай Γ - дискретна зліченна множина з нескінченним базисом $\{e_i\}, i = 1,....,n,.....$ На ньому введена операція інволюції * така, що

$$*: \Gamma \to \Gamma, \text{ для } \forall e_i \in \Gamma, e_i^* \in \Gamma. \quad (1)$$

Існує елемент базису $e_1 \in \Gamma$ такий, що

$$e_1 \cdot e_i = e_i \cdot e_1 = e_i,\ (e_i^*)^* = e_i \quad (2)$$

Операція множення (згортка) у множині проводиться за наступним правилом:

$$e_i \cdot e_j = \sum_{k=1}^{\infty} C_{ij}^k e_k \quad (3)$$

Множина є гіперкомплексною системою, яка може бути як дискретною, так і безперервною, при виконанні умов (1)-(3).

Перехід від нескінченновимірної гіперкомплексної системи до конечновимірної гіперкомплексної числової системи будемо здійснювати з врахуванням умов коммутативности і позитивності структурних констант:

$$C_{ij}^{k} \geq 0; \quad C_{ii^*}^{1} > 0; \; C_{ij}^{k} = C_{ki^*}^{j} \geq 0.$$

Сформуємо нескінченновимірну гіперкомплексну систему, від якої пізніше за допомогою факторизації по конкретній підгрупі будемо отримувати гіперкомплексні числові системи кінцевої розмірності.

Задана група $Z = \{-\infty, \infty\}$. На ній обрана деяка підгрупа автоморфізмів $V = \{-1,1\} \in Aut\,Z$, що для $\forall n \in Z$, виконуються

$$1(n) = n \in Z, -1(n) = -n \in Z.$$

Факторизуємо групу Z по підгрупі V та отримаємо множину $Z/V = \Gamma = N \cup \{0\}$. Визначимо для цієї множини правило множення базисних елементів (згортку).

Якщо для групи Z згортка має вигляд

$$\sigma_n \cdot \sigma_m = \sigma_{n+m} \quad (4)$$

або, враховуючи властивості групи Z, можна записати $n \cdot m = n + m$.

Тоді згортка для $Z/V = \Gamma$ буде мати вигляд:

$$n \cdot m = \{n,-n\} \cdot \{m,-m\} =$$
$$= (n+m) + (m-n) + (-n-m) + (n-m) =$$
$$= \{(n+m),-(n+m)\} + \{(n-m),-(n-m)\}$$

З властивостей згортки та виразу (4) вірне співвідношення:

$$\frac{1}{2}(\sigma_n \cdot \sigma_{-n}) = \sigma_n \quad (5)$$

Якщо врахувати вираз (5), отримаємо згортку:

$$\sigma_n \cdot \sigma_m = \frac{1}{2}(\sigma_n + \sigma_{-n}) \cdot \frac{1}{2}(\sigma_m + \sigma_{-m}) =$$
$$= \frac{1}{4}(\sigma_{n+m} + \sigma_{-(n+m)}) + (\sigma_{|n-m|} + \sigma_{-|n-m|}) \quad (6)$$

Тоді вигляд згортки (4) з врахуванням співвідношення (6) має вигляд:

$$\sigma_n \cdot \sigma_m = \frac{1}{2}(\sigma_{n+m} + \sigma_{|n-m|}) \quad (7)$$

Маючи нескінченновимірну гіперкомплексну систему і згортку, обираємо підгрупи, по яких будемо здійснювати факторизацію.

Можна обирати підгрупи $\{A_2, A_3, A_4, ...\}$, де

$A_2 = \{a_k : a_k = 2k, k \in \Gamma\}$,

$A_3 = \{a_k : a_k = 3k, k \in \Gamma\}$,

$A_4 = \{a_k : a_k = 4k, k \in \Gamma\}$ і т.д.

При цьом слід зазначити, что кожна така підгрупа є нескінченновімірною і число таких підгруп зліченна кількість.

(4)

Аналіз отриманих запропонованим методом гіперкомплексних числових систем

Після факторизації гіперкомплексної системи $\Gamma = N \cup \{0\}$ по підгруппі $A_2 = \{a_k : a_k = 2k, k \in \Gamma\}$ зі згорткою (7) отримаємо скінченновимірну гіперкомплексну числову систему $G_2 = \Gamma/A_2 = \{e_1, e_2\}$ другої розмірності, а саме, систему подвійних чисел, таблиця множення якої має вигляд (рис.1).

e_1	e_2
e_2	e_1

Рис.1. Таблиця множення ГЧС 2-ї вимірності

Надалі, збільшуючи розмірність, отримуємо неканонічні ГЧС.

При факторизації гіперкомплексної системы $\Gamma = N \cup \{0\}$ по підгрупі $A_3 = \{a_k : a_k = 3k, k \in \Gamma\}$ зі згорткою(7) отримаємо ГЧС $G_3 = \Gamma/A_3 = \{e_1, e_2, e_3\}$ третьої розмірності. Таблиця множення отриманої скінченновимірної гіперкомплексної числової системи буде мати вигляд (рис.2):

e_1	e_2	e_3
e_2	$\frac{1}{2}(e_1 + e_3)$	$\frac{1}{2}(e_1 + e_2)$
e_3	$\frac{1}{2}(e_1 + e_2)$	$\frac{1}{2}(e_1 + e_2)$

Рис.2. Таблиця множення ГЧС 3-ї розмірності

Після факторизації гіперкомплексної системы $\Gamma = N \cup \{0\}$ по підгрупі $A_4 = \{a_k : a_k = 4k, k \in Q\}$ зі згорткою вигляду (7) отримаємо гіперкомплексну числову систему $G_4 = \Gamma/A_4 = \{e_1, e_2, e_3, e_4\}$ четвертої розмірності (рис.3)

e_1	e_2	e_3	e_4
e_2	$\frac{1}{2}(e_1+e_3)$	$\frac{1}{2}(e_2+e_4)$	$\frac{1}{2}(e_1+e_3)$
e_3	$\frac{1}{2}(e_2+e_4)$	e_1	e_2
e_4	$\frac{1}{2}(e_1+e_3)$	e_2	$\frac{1}{2}(e_1+e_3)$

Рис.3. Таблиця множення ГЧС 4-ї розмірності

Так як в ГЧС четвертої розмірності, що отримано, є закономірність, яка полягає в наступному: $e_1 \cdot e_1 = e_1, e_3 \cdot e_3 = e_1$, то можна здійснити повторну факторизацію по підмножині $\{e_1, e_3\}$.

Повторна факторизація $G_4 / \{e_1, e_3\}$ призводить до гіперкомплексної числової системи другої розмірності з таблицею множення(рис.4).

e_1	e_2
e_2	$\frac{1}{2}(e_1+e_2)$

Рис.4. Таблиця множення неканонічної ГЧС 2-ї розмірності

Після факторизації гіперкомплексної системи $\Gamma = N \cup \{0\}$ по підгрупі $A_5 = \{a_k : a_k = 5k, k \in \Gamma\}$ з правилами множення вигляду (7) отримаємо скінченновимірну гіперкомплексну числову систему $G_5 = \Gamma / A_5 = \{e_1, e_2, e_3, e_4, e_5\}$ п‘ятої розмірності з відповідною таблицею множення (рис.5).

e_1	e_2	e_3	e_4	e_5
e_2	$\frac{1}{2}(e_1+e_3)$	$\frac{1}{2}(e_2+e_4)$	$\frac{1}{2}(e_3+e_5)$	$\frac{1}{2}(e_1+e_4)$
e_3	$\frac{1}{2}(e_2+e_4)$	$\frac{1}{2}(e_1+e_5)$	$\frac{1}{2}(e_1+e_2)$	$\frac{1}{2}(e_2+e_3)$
e_4	$\frac{1}{2}(e_3+e_5)$	$\frac{1}{2}(e_1+e_2)$	$\frac{1}{2}(e_1+e_2)$	$\frac{1}{2}(e_2+e_3)$
e_5	$\frac{1}{2}(e_1+e_4)$	$\frac{1}{2}(e_2+e_3)$	$\frac{1}{2}(e_2+e_3)$	$\frac{1}{2}(e_1+e_4)$

Рис.5 Таблиця множення неканонічної ГЧС 5-ї розмірності

Факторизуемо гіперкомплексну систему $\Gamma = N \cup \{0\}$ по підгрупі $A_6 = \{a_k : a_k = 6k, k \in \Gamma\}$ аналогічно попереднім підгрупам та отримаємо ГЧС $G_6 = \Gamma / A_6 = \{e_1, e_2, e_3, e_4, e_5, e_6\}$ шостої розмірності. Згортка ГЧС, що отримано, з врахуванням (7) буде мати вигляд (рис.6)

e_1	e_2	e_3	e_4	e_5	e_6
e_2	$\frac{1}{2}(e_1+e_3)$	$\frac{1}{2}(e_2+e_4)$	$\frac{1}{2}(e_3+e_5)$	$\frac{1}{2}(e_4+e_6)$	$\frac{1}{2}(e_1+e_5)$
e_3	$\frac{1}{2}(e_2+e_4)$	$\frac{1}{2}(e_1+e_5)$	$\frac{1}{2}(e_2+e_6)$	$\frac{1}{2}(e_1+e_3)$	$\frac{1}{2}(e_2+e_4)$
e_4	$\frac{1}{2}(e_3+e_5)$	$\frac{1}{2}(e_2+e_6)$	e_1	e_2	e_3
e_5	$\frac{1}{2}(e_4+e_6)$	$\frac{1}{2}(e_1+e_3)$	e_2	$\frac{1}{2}(e_1+e_3)$	$\frac{1}{2}(e_2+e_4)$
e_6	$\frac{1}{2}(e_1+e_5)$	$\frac{1}{2}(e_2+e_4)$	e_3	$\frac{1}{2}(e_2+e_4)$	$\frac{1}{2}(e_1+e_5)$

Рис.6. Таблиця множення ГЧС 6-ї розмірності

Так як в цій ГЧС, що отримано, є закономірність, яка полягає в наступному $e_1 \cdot e_1 = e_4 \cdot e_4 = e_1, e_1 \cdot e_2 = e_4 \cdot e_5 = e_2$, $e_1 \cdot e_3 = e_4 \cdot e_6 = e_3$, то можна здійснити повторну факторизацію по підмножині $\{e_1, e_4\}$. В результаті отримаємо ще одну ГЧС третьої розмірності зі згорткою (рис.7).

e_1	e_2	e_3
e_2	$\frac{1}{2}(e_1+e_3)$	$\frac{1}{2}(e_1+e_2)$
e_3	$\frac{1}{2}(e_1+e_2)$	$\frac{1}{2}(e_1+e_3)$

Рис.7. Таблиця множення ГЧС 3-ї розмірності

Аналогічно запропонованим методом можна отримати ГЧС більшої розмірності. Як видно з наведених вище прикладів, отримання ГЧС по підгрупах вигляду

$A_6 = \{a_k : a_k = 6k, k \in Q\}$,

$A_8 = \{a_k : a_k = 8k, k \in Q\}$ и т.д., тобто по підгрупам, елементи яких є парними, можна повторно факторизувати та отримувати ГЧС розмірності в 2 рази менше.

Висновки

Отже, у статті розглянуто метод переходу від нескінченновимірної гіперкомплексної системи до скінченновимірної неканонічної ГЧС методами факторизації.

Показано факторизацію нескінченновимірної гіперкомплексної системи по нескінченновимірним підгрупам, використовуючи згортку вигляду $\sigma_n \cdot \sigma_m = \frac{1}{2}(\sigma_{n+m} + \sigma_{|n-m|})$, з метою отримання скінченномірних гіперкомплексних числових систем, які, починаючи з третьої розмірності, є неканонічними.

Отримані системи парної розмірності (2, 4, 6, 8 ...), можна повторно факторизуватиь і отримати гіперкомплексну числову систему розмірності в два рази менше.

Список літератури

1. Синьков М.В. Гіперкомплексні числові системи: основи теорії, практичні використання, бібліографія / М.В. Синьков, Ю.Є. Боярінова, Я.О. Каліновський, Синькова Т.В., Федоренко О.В. – К. ІПРІ, 2009. – 44 с. – (Препр. /НАН України, Інт пробл. реєстрації інформац, 2009).
2. Кантор И. Л. Гиперкомплексные числа/ Кантор И. Л., Солодовников А.С. – М.: Наука, 1973. – 144 с.
3. Синьков М.В. Развитие задачи разделения секрета / Синьков М.В., Бояринова Ю.Е., Калиновский Я.А., Трубников П.В. // Реєстрація, зберігання і обробка даних. – 2003. – Т. 5 – № 4. – С. 90–96.
4. Одарич Я.В. Вычисления в неканонических гиперкомплексных числовых системах / Одарич Я.В., Наливайчук Е.Ю., Наливайчук Н.В. // Радіоелектронні і комп'ютерні системи. –2010. –№5. – С. 75-78.
5. Калиновский Я.В. Высокоразмерные изоморфные гиперкомплексные числовые системы и их использование для повышения эффективности вычислений / Калиновский Я.В., Бояринова Ю.Е – Киев: Инфодрук, 2012. – 82 с.
6. Одарич Я.В. Процедура перечисления гиперкомплексных числовых систем методом линейных преобразований./ Одарич Я.В. // Реєстрація, зберігання і обробка даних. – 2008. – Т. 6 – № 2. – С. 107–112.
7. Березанский Ю. М. Гармонический анализ в гиперкомплексных системах / Березанский Ю. М. , Калюжный А. А. – К.: Наукова думка, 1992. –352 с.