УДК 004.94; 515.173; 681.3

М. В. Синьков, Ю. Є. Боярінова, Я. О. Каліновський,
Т. Г. Постнікова, Т. В. Синькова, О. В. Федоренко
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Розвиток теорії гіперкомплексного представлення інформації та її застосування

Представлено найбільш значимі етапи розвитку представлення інформації гіперкомплексними числами та показано внесок учених ІПРІ НАН України, який відображає значимі результати, отримані в цьому напрямку. Наведено приклади рішення деяких практичних задач із використанням гіперкомплексних чисел.

Ключові слова: *гіперкомплексна числова система, кватерніни, ізоморфізм, нелінійні функції, схема розподілення секрету, цифровий фільтр.*

Дослідження в галузі гіперкомплексних числових систем виконувалися протягом 20-ти років у відділі спеціалізованих засобів моделювання Інституту проблем реєстрації інформації Національної академії наук України.

Автори вважають своїм обов’язком подякувати колишнім співробітникам Інституту та відділу, які внесли свій значний внесок у розвиток цього нового наукового напрямку: д.т.н. Н.М. Губарені, к.т.н. І.Л. Бородкіній, к.т.н. Л.Б. Удовікіній, к.т.н. А.Ф. Яніку, А.А. Чапор.

Питання ефективного представлення інформації були й залишаються [1–5] важливими для моделювання та вирішення задач у різних галузях науки та техніки. Досвід показує, що форма представлення інформації обумовлює можливі характеристики по продуктивності обробки даних, а також можливості по створенню ефективної процедури моделювання, знаходження помилок та їхнє виправлення тощо. Прикладами таких форм представлення інформації можуть бути непозиційні системи числення, фібоначчиєві числові системи, системи з від’ємною основою.

Особливе місце серед нетрадиційних форм представлення інформації займають гіперкомплексні числові системи (ГЧС) [6]. Ця форма представлення інформації у своєму розвитку глибоко пов’язана із фундаментальними основами математики. Так, після появи комплексних чисел на розвиток гіперкомплексних числових систем виявила вплив теорія функцій комплексного змінного, загальна алгебра та деякі розділи математичного аналізу. Таким чином, наука про гіперкомплексні числові системи мала свій особливий шлях розвитку, який супроводжувався вищевказаними розділами математики.

Треба підкреслити, що «доля» гіперкомплексних числових систем дуже нерівномірна. Між відкриттям комплексних чисел і кватерніонів лежить інтервал часу в три сторіччя. Розвиток подій після формування системи кватерніонів характеризується бурхливим ростом. Особливо треба наголосити, що останні півтора-два десятиріччя дають велику кількість робіт і прикладів як теоретичного, так і прикладного напрямків. Усе це вказує на необхідність приділити увагу питанням і проблемам гіперкомплексних числових систем.

Етапи розвитку теорії гіперкомплексних числових систем

Початок розвитку теорії гіперкомплексних числових систем пов’язують із відкриттям у 1843 р. Р. Гамільтоном системи кватерніонів. Ним же був запропонований цілий ряд застосувань кватерніонів у геометрії, астрономії та фізиці. У тому ж році Д. Гревс відкрив октоніони як результат подвоєння кватерніонів комплексними числами, а А. Кейлі дослідив їхні властивості. Зокрема, він установив, що ця 8-вимірна числова система неасоціативна. Г. Грассман у 1844 р. створив теорію n-вимірних просторів, яка також стала фундаментом теорії гіперкомплексних числових систем. У 1847 р. Е. Куммер узагальнив фундаментальну теорему арифметики на комплексні числа, а Д. Гревс дослідив алгебру форм $a+be+ce^2$, де $e^3=-1$, та довів, що ця алгебра є прямою сумою систем дійсних і комплексних чисел $R \oplus C$.

У 1851 р. Б. Риман запропонував відображення комплексної площини на сферу («сфера Римана»), чим створив основи теорії комплексного та гіперкомплексного змінного. А. Кейлі в 1858 р. розробив матричне представлення кватерніонів. Це дозволило використовувати розвинуті до того часу методи матричного аналізу до теорії гіперкомплексного змінного.

Вагомий внесок у розвиток теорії гіперкомплексних числових систем зробив К. Вейерштрасс, довівши те, що комплексні числа зберігають усі властивості дійсних чисел. Він також установив, що кожна комутативна гіперкомплексна числова система без нільпотентних елементів являє собою пряму суму деякої кількості систем дійсних і комплексних чисел.

Перші систематичні дослідження в галузі перечислення гіперкомплексних числових систем здійснив у 1870 р. Б. Пірс. Він створив таблиці 162-х гіперкомплексних числових систем, а його син Ч. Пірс довів, що з усіх гіперкомплексних числових систем вимірності до 7 включно, тільки системи дійсних, комплексних чисел і кватерніони мають операцію ділення.

В. Кліффорд розробив геометрію руху з використанням бікватеріонів і на основі алгебри Грассмана створив алгебру, що одержала назву «алгебра Грассмана», яка має дуже важливе значення для багатьох галузей науки та техніки. Зокрема, Р. Ліпшиць у 1886 р. у роботі «Untersuchungen über die Summen von Quad-raten» Грассмана застосував її до моделювання поворотів у евклідових просторах.

Поняття ізоморфних гіперкомплексних числових систем на основі невиродженого лінійного перетворення базису систем сформулював Е. Штуді [7] у 1889 р. Він же систематизував класи ізоморфізмів таких систем вимірності від другої до четвертої, в яких n-а степінь кожного гіперкомплексного числа з цієї системи є лінійною комбінацією всіх попередніх степенів того ж числа:

$$a^n = \sum_{k=0}^{n-1} \alpha_k a^k \ , \ a \in \Gamma \ .$$

Крім того, Е. Штуді почав користуватися поняттям «канонічна гіперкомплексна числова система», як такої системи, у якій добуток двох базисних елементів дорівнює якомусь базисному елементу з коефіцієнтом ± 1 або 0:

$$e_i \cdot e_j = \rho e_k \, , \quad i, j, k \in \{1,2,...,n\} \ , \quad \rho = \pm 1,0 \, .$$

Важливим етапом розвитку теорії гіперкомплексних числових систем було встановлення в 1893 р. Ф. Моліном ізоморфізму комплексних простих алгебр і матричних алгебр. Пізніше цей факт був підтверджений Г. Фробеніусом. Ним же в 1878 р. була доведена теорема, згідно з якою кожна асоціативна гіперкомплексна числова система з діленням ізоморфна одній із трьох систем: системі дійсних чисел R, комплексних чисел C або кватерніонів H. Дещо пізніше ця теорема була узагальнена: «кожна альтернативна гіперкомплексна числова система з діленням ізоморфна одній із чотирьох систем: системі дійсних чисел R, комплексних чисел C, системі кватерніонів H або системі октав Q». А. Гурвиць довів цю теорему для будь-яких нормованих гіперкомплексних числових систем, тобто таких систем, у яких норма добутку двох чисел дорівнює добуткові норм цих же чисел, а В. Мілнор показав, що вимогам комутативності та асоціативності множення задовольняють тільки системи R, C, H та Q.

Якщо до кінця XIX-го ст. гіперкомплексні числові системи знаходили застосування лише в наукових дослідженнях, то із цього часу починають з'являтися роботи, які дозволяють використовувати гіперкомплексні числа й для вирішення інженерних задач.

В. Кліффорд, Г. Кокс (H. Cox) та А. Бухгейм дослідили властивості трьох типів бікватерніонів — подвоєння систем кватерніонів за допомогою комплексних, подвійних і дуальних чисел, а Е. Штуді в 1891 р. у роботі «Von Bewegungen und Umlegungen» установив зв'язок між дуальними бікватерніонами та групою рухів евклідового простору. На цій основі Р. Болл створив теорію гвинтів [8], яка знайшла важливі застосування в механіці твердого тіла. А.П. Котельников значно розвинув цю теорію [9], а Ф.М. Діментберг застосував теорію гвинтів для аналізу та синтезу плоских і просторових механізмів з багатьма ступенями волі [10].

Е. Нетер у роботі [11], яка вийшла в 1929 р., дослідила зв'язки між гіперкомплексними числовими системами та теорією представлень. В.В. Люш у роботах [12, 13], будує гіперкомплексні числа, виходячи з вирішення задачі про представлення числами векторів у просторі трьох і більше вимірів, а також розповсюджує на ці числа багато методів диференціального та інтегрального числення.

У 1973 р. вийшла книга І.Л. Кантора та О.С. Солодовникова «Гіперкомплексні числа» [14], у якій систематизовано багато даних про теорію та застосування гіперкомплексних чисел та їхні зв’язки із загальною алгеброю.

М.В. Синьков та Н.М. Губарені в роботі [6] дослідили методи побудови систем залишкових класів у багатьох гіперкомплексних числових системах: подвійних, дуальних, триплексних, квадриплексних числах, кватерніонах, бікватерніонах, октавах, алгебрах Грассмана, Кліффорда та ін. Це відкрило шлях до використання цих методів у вирішенні практичних задач, де потрібні скінченні поля. Це насамперед різні задачі криптографії.

Сучасний стан розвитку теорії гіперкомплексних числових систем характеризується дослідженнями за багатьма напрямками. Найбільш важливими з них є такі:

1) розвиток загальної теорії гіперкомплексних числових систем і дослідження їхніх структурних властивостей [14, 15];

2) дослідження класів ізоморфізмів гіперкомплексних числових систем і методів їхнього перечислення [16, 17];

3) дослідження аналітичних функцій від гіперкомплексного змінного в різних системах і побудова їхніх уявлень у вигляді гіперкомплексних функцій [1, 18, 19,];

4) дослідження методів розв’язування та властивостей розв’язків різних типів диференціальних рівнянь від гіперкомплексного змінного та з гіперкомплексними коефіцієнтами [2, 3, 20–22];

5) розробка алгоритмічного та програмного забезпечення, призначеного для проведення арифметичних, алгебраїчних й аналітичних обчислень у різних гіперкомплексних числових системах. Програмне забезпечення розроблюється як у мовах програмування низького рівня (C^{++}, Fortran, VisualBasik), так і за допомогою систем символьних обчислень типу MathCAD, Maple, Mathematica та ін. [23–25].

Методи гіперкомплексних числових систем знайшли дуже важливі застосування в теоретичній фізиці. Чисельні посилання можна одержати з роботи О.Л. Смоліна [26] та на сайті www.att.net/~t.ell//QuatRef.htm(2006).

Найбільшу кількість застосувань у технічних науках знайшли кватерніони. Це обумовлено тим, що за їхньою допомогою дуже зручно та ефективно моделювати обертання твердого тіла, у тому числі й навколо декількох осей.

Із численних застосувань кватерніонів відзначимо тільки деякі, найбільш важливі:

1) у задачах навігації, орієнтації та управління рухом твердого тіла в тривимірному просторі [27, 28], у тому числі й під водою [29];

2) комп’ютерна графіка, де необхідно розрахувати як буде виглядати на екрані тіло, що обертається, у багатьох проміжних положеннях для створення ефектів анімації [30];

3) дослідження деформації пружних та еластичних конструкцій;

4) фільтрація зображення на базі кватерніонного перетворення Фур’є [31];

5) обробка кольорового зображення; S.J. Sangwine у [32] запропонував використати для представлення будь-якого кольору трьома основними кольорами (че-

рвоний–зелений–синій) векторну частину кватерніона. При цьому значно спрощуються алгоритми фільтрації кольорового зображення;

6) у криптографії кватерніонне представлення інформації використовується для підвищення стійкості шифрів [5].

Якщо за допомогою кватерніонів можна моделювати тільки обертання твердого тіла, то для моделювання обертання та переміщення використовуються дуальні числа — бікватерніони — подвоєння кватерніонів за допомогою дуальних чисел, а також подвійні кватерніони — подвоєння кватерніонів за допомогою системи подвійних чисел. У роботі [33] на основі дуальних чисел виведено рівняння динаміки твердого тіла: вирази для дуальних моментів, кількості руху, кінетичної енергії, рівнянь Ньютона та Лагранжа. Дуальні числа, дуальні та подвійні кватерніони знайшли широке застосування в задачах моделювання та управління плоскими механізмами, роботами та маніпуляторами з багатьма степенями свободи й навіть моделювання скелета людини [34, 35].

Алгоритми моделювання переміщення твердого тіла в тривимірному просторі загального вигляду на основі подвійних кватерніонів мають більшу точність порівняно з алгоритмами, які використовують ортогональні матриці або одиничні кватерніони. Великий ефект дає застосування гіперкомплексних числових систем при побудові алгоритмів обробки багатовимірних сигналів [36]. При цьому останнім часом використовуються як некомутативні системи, так і комутативні. Особливо вони ефективні в алгоритмах перетворення Фур'є. При цьому, квадриплексна числова система, як підкреслюють автори [37] «гарантує синтез алгоритмів двовимірних перетворень із складністю, меншою, ніж у відповідних комплексних або кватерніонних прототипів».

Необхідність розробки методів фільтрації комплексних і гіперкомплексних сигналів привела в останнє десятиріччя до створення структур цифрових реверсивних фільтрів із гіперкомплексними коефіцієнтами [38]. При створенні таких структур використовується те, що передавальна функція у вигляді дрібно-раціонального виразу може бути перетворена в гіперкомплексну функцію із дрібно-раціональними компонентами більш високих степенів із дійсними коефіцієнтами. При цьому кожний компонент у принципі можна розглядати як передавальну функцію по відповідному каналу структури.

Методи гіперкомплексних числових систем успішно використовуються й у дослідженні стійкості режимів електроенергетичних систем [39], коли в розв'язках систем рівнянь, які моделюють електроенергетичну систему, існують комплексні розв'язки, а електричні величини — також комплексні величини. Але їхні уявності мають іншу природу порівняно з уявностями розв'язків системи рівнянь. Використання в даному випадку кватерніонів і квадриплексних чисел дозволило створити ефективні алгоритми пошуку усталених режимів електроенергетичних систем.

Гіперкомплексні числові системи успішно використовуються й у процесах обробки модульованого сигналу [40], де застосовується бікомплексна гіперкомплексна числова система.

Вихідні визначення

ГЧС n-го порядку вважається завданою над полем $\boldsymbol{R}$, якщо визначені базис системи $i_1, i_2, ..., i_n$ (переважно $i_1 = 1$) і таблиця множення (закон композиції) базисних елементів:

$$i_m i_k = \sum_{s=1}^{n} \gamma_{mk}^{s} i_s \,, \tag{1}$$

де $\gamma_{mk}^{s} \in \boldsymbol{R}$ — структурні константи $(m, k = 1, ..., n)$.

Усього структурних констант — n^3. Тоді гіперкомплексне число має вигляд:

$$A = \sum_{s=1}^{n} a_s i_s \,.$$

Усі ГЧС можна класифікувати за двома ознаками.

1. Комутативність:

— для комутативних ГЧС: $\gamma_{mk}^{s} = \gamma_{km}^{s}$;

— для некомутативних: $\gamma_{mk}^{s} \neq \gamma_{km}^{s}$.

2. Асоціативність:

— для асоціативних ГЧС:

$$\gamma_{km}^{u} \gamma_{ut}^{s} = \gamma_{mt}^{u} \gamma_{ku}^{s} \,;$$

— для неасоціативних ГЧС ця рівність не виконується.

Як приклад, розглянемо найбільш розповсюджену ГЧС — систему комплексних чисел. Це комутативна система другого порядку з базисом i_1, i_2 і законом композиції:

$$i_1 i_2 = i_2 i_1 = i_2 \,;\; i_1 i_1 = i_1 \,;\; i_2 i_2 = -i_1 \,.$$

Її вісім структурних констант мають вигляд:

$$г_{11}^{1} = 1 \,;\; \gamma_{11}^{2} = 0 \,;\; \gamma_{21}^{1} = \gamma_{12}^{1} = 0 \,;\; \gamma_{21}^{2} = \gamma_{12}^{2} = 1 \,;\; \gamma_{22}^{1} = -1 \,;\; \gamma_{22}^{2} = 0 \,.$$

У кожній ГЧС визначені такі основні операції.

1. Додавання — виконується покомпонентно:

$$A + B = \sum_{s=1}^{n} (a_s + b_s) i_s \,.$$

2. Множення. Воно визначається за допомогою закону композиції (1):

$$A \cdot B = \sum_{s=1}^{n} a_s i_s \cdot \sum_{s=1}^{n} b_s i_s = \sum_{s=1}^{n} \sum_{t=1}^{n} \sum_{m=1}^{n} a_s b_t \gamma_{st}^{m} i_m \,.$$

Неважко довести, що для комутативних систем:

$$A \cdot B = B \cdot A;$$

для некомутативних:

$$A \cdot B \neq B \cdot A;$$

для асоціативних систем:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)\,.$$

Ділення гіперкомплексних чисел вводиться на основі визначення множення. Часткою від ділення числа A на число B є таке число X, що:

$$A = B \cdot X\,,$$

або

$$\sum_{m=1}^{n} a_m i_m = \sum_{s=1}^{n} \sum_{t=1}^{n} \sum_{m=1}^{n} b_s x_t \gamma_{st}^{m} i_m \,.$$

Порівнюючи коефіцієнти при однакових i_m, одержимо лінійну систему:

$$\sum_{s=1}^{n} \sum_{t=1}^{n} b_s \gamma_{st}^{m} x_t = a_m\,, \quad m = 1,...,n\,,$$

визначник якої для деяких B, що не обов'язково дорівнює нулю, може перетворюватися на нуль. Це означає, що в таких ГЧС ділення неможливе не тільки на нуль, але й на деяку множину чисел, які звуться дільниками нуля.

У відповідності з теоремою Фробеніуса дільників нуля немає тільки в системах дійсних і комплексних чисел, у некомутативній системі квартерніонів і неасоціативній системі октав — системі 8-го порядку. Усі інші системи мають дільники нуля, вигляд яких у різних системах різний. Наприклад, у системі подвійних чисел с базисом i_1, i_2 та законом композиції

	i_1	i_2
i_1	i_1	0
i_2	0	i_2

дільники нуля мають вигляд:

$$a_1 i_1 \neq 0\,;\ a_2 i_2 \neq 0\,.$$

Дійсно

$$a_1 i_1 \cdot a_2 i_2 = a_1 a_2 \cdot i_1 i_2 = a_1 a_2 \cdot 0 = 0\,.$$

Методи класифікації гіперкомплексних числових систем

Як відмічалося вище, ГЧС визначається n^3 структурними константами. Тому множина ГЧС — нескінченна.

Деякі ГЧС можна одержати з інших за допомогою лінійного перетворення базису. Такі ГЧС є ізоморфними. Ізоморфізм розподіляє всю множину ГЧС на класи, кількість яких скінчена для ГЧС однієї розмірності. Визначення кількості класів ізоморфізму й хоча б одного представника кожного класу є однією з основних задач теоретичних основ гіперкомплексного представлення інформації. Зараз найбільш вивчені два методи класифікації класів ізоморфізмів:

1) комбінаційним переліком структурних констант;

2) за допомогою алгебри шляхів на графах.

Перший метод заснований на регулярному перегляді значень структурних констант. Якщо ГЧС ізоморфна якійсь із попередніх, то вона не включається до складу класів ізоморфізмів. Ця процедура дуже трудомістка й потребує великого обсягу обчислень. Тому цей метод придатний тільки для перечислення класів ізоморфізмів ГЧС невеликої розмірності.

Значно більші можливості має метод алгебри шляхів на графах, детальний розгляд якого представлено в роботах [41, 42]. Згідно цього методу схема ГЧС шляхом застосування певної неформальної процедури представляється квадратною матрицею — матрицею інцідентності. Тоді питання про ізоморфізм двох ГЧС зводиться до переводу матриць інцідентності одна в одну одночасними перестановками рядків і стовпців. Виходячи з того, що матриця інцідентності складається тільки з нулів та одиниць, то вирішення задачі про ізоморфізм двох ГЧС стає значно менш трудомісткою, ніж у першому методі. Недоліком цього методу є те, що деякі етапи побудови матриці інцідентності важко формалізувати, але розробки в цьому напрямку обіцяють принести важливі результати.

Роботи, проведені нами за допомогою цих методів для комутативних ГЧС, дали таку кількість класів ізоморфізмів: ГЧС 2-го порядку —3; 3-го порядку — 6; 4-го — 14.

Методи представлення нелінійних функцій від гіперкомплексного змінного

Нелінійні функції від гіперкомплексного змінного визначаються за аналогією з функціями комплексного змінного. Будемо вважати експонентою від гіперкомплексного змінного M суму ряду, аналогічного ряду для експоненти від комплексної змінної:

$$e^M = \sum_{s=0}^{\infty} \frac{M^s}{s!}\,.$$

Але обчислити суму такого ряду в загальному вигляді й особливо для ГЧС, які неможливо представити у вигляді прямої суми ГЧС нижчих порядків, дуже важко. Розглянемо гіперкомплексну функцію:

$$F(t) = e^{Mt+K} = \sum_{s=0}^{\infty} \frac{(Mt+K)^s}{s!},$$

де M та K — гіперкомплексні числа.

Виходячи з того, що

$$F(t) = \sum_{s=0}^{\infty} \frac{(Mt+K)^s}{s!} = \sum_{s=0}^{\infty} \sum_{r=0}^{\infty} \frac{P_r(m_1,...,m_n) i_s}{s!},$$

де $P_r(m_1,...,m_n)$ — поліном ступеня r, то цей ряд абсолютно збігається, і його можна почленно диференціювати:

$$\dot{F}(t) = M \sum_{s=0}^{\infty} \frac{(Mt+K)^s}{s!} = MF(t).$$

Тобто $F(t)$ — рішення диференціального рівняння:

$$\dot{X} = MX. \tag{2}$$

Це означає, що експоненту від гіперкомплексного змінного можна визначити і як рішення рівняння (2).

Але рівняння (2) зводиться до системи лінійних диференціальних рівнянь від дійсного змінного. Це можна зробити, якщо перемножити M та X згідно з таблицею множення та прирівняти вирази при однакових базисних одиницях у лівій та правій частинах. Одержимо систему:

$$\dot{Y} = M^* Y, \tag{3}$$

компоненти рішення якої й будуть компонентами експоненти від гіперкомплексної змінної.

Система (3) називається системою лінійних диференціальних рівнянь, асоційованою з даною ГЧС, тому що вигляд матриці M^* залежить від структурних констант даної ГЧС.

Рішення системи (3) має n довільних постійних. Їхні значення вибираються таким чином, щоб виконувалась основна властивість експоненти:

$$e^0 = E,$$

де E — одиничний елемент даної ГЧС.

Характеристичне рівняння системи (3)

$$M^* - \lambda E = 0$$

має n коренів, склад яких відображає структурні властивості даної ГЧС. Якщо характеристичне рівняння має m співпадаючих дійсних коренів або $\frac{m}{2}$ співпадаючих спряжених комплексних коренів, то дана ГЧС має в своєму складі радикали m-го порядку. За допомогою експоненціальної функції можна визначити логарифмічну функцію, як обернену експоненціальній. У роботах [41, 42] виведені представлення цих функцій для деяких класів ізоморфізмів комутативних систем 2–4 порядків. Деякі приклади представлені в цій статті.

Інші види нелінійностей можна одержати за допомогою диференціальних рівнянь другого порядку:

$$\ddot{X} = MX .$$

З ними асоціюється система з $2n$ лінійних диференціальних рівнянь першого порядку

$$\dot{Y} = M^* Y .$$

Рішення цієї системи має $2n$ довільних постійних, значення яких визначаються початковими умовами. Якщо ці значення визначаються рядом

$$\sum_{s=0}^{\infty} \frac{M^{2s+1}}{(2s+1)!},$$

то одержимо гіперболічний синус — ShM .

Ряд

$$\sum_{s=0}^{\infty} \frac{M^{2s}}{(2s)!}$$

визначає гіперболічний косинус ChM . Між експонентною та гіперболічними функціями існує залежність:

$$e^M = ShM + ChM .$$

Дослідження властивостей одержаних функцій показує, що вони багато в чому аналогічні властивостям функцій від комплексного змінного.

Представлення нелінійностей для деяких гіперкомплексних числових систем

1. Квазідуальна ГЧС.

Гіперкомплексне число має вигляд $M = m_1 + m_2 i$.

Закон композиції:

$$i^2 = p + qi\,;\; p + \frac{q^2}{4} > 0\,;\; k = \sqrt{p + \frac{q^2}{4}}\,.$$

Представлення нелінійних функцій:

— експонента $e^M = e^{(m_1 + \frac{q}{2} m_2)} (1 - \frac{q}{2} m_2 + m_2 i)$;

— логарифм $LnM = \ln \frac{2m_1 + qm_2}{2} - \frac{qm_2}{2 + qm_2} + \frac{2m_2}{2m_1 + qm_2} i$;

— гіперболічні функції:

$$ShM = sh(m_1 + \frac{q}{2} m_2) ch(km_2) - \frac{q}{2k} ch(m_1 + \frac{q}{2} m_2) sh(km_2) + ch(m_1 + \frac{q}{2} m_2) ch(km_2) \frac{i}{k},$$

$$ChM = ch(m_1 + \frac{q}{2} m_2) ch(km_2) - \frac{q}{2k} sh(m_1 + \frac{q}{2} m_2) sh(km_2) + sh(m_1 + \frac{q}{2} m_2) sh(km_2) \frac{i}{k}.$$

2. Гіперкомплексна система з таблицею множення:

	i_1	i_2	i_3	i_4
i_1	i_1	i_2	i_3	i_4
i_2	i_2	$-i_1$	i_4	$-i_3$
i_3	i_3	i_4	0	0
i_4	i_4	$-i_3$	0	0

$$M = m_1 i_1 + m_2 i_2 + m_3 i_3 + m_4 i_4\,,$$

$$e^M = e^{m_1} (\cos m_2 (i_1 + m_3 i_3 + m_4 i_4) + \sin m_2 (i_2 - m_4 i_3 + m_3 i_4))\,,$$

$$LnM = \ln m_1 i_1 + ((-1)^k \arcsin \frac{m_2}{m_1} + 2\pi k) i_2 +$$
$$+ \frac{1}{m_1^2} (m_3 \sqrt{m_1^2 - m_2^2} + m_2 m_4) i_3 + \frac{1}{m_1^2} (m_4 \sqrt{m_1^2 - m_2^2} + m_2 m_3) i_4,$$

$$SnM = sh(m_1) \cos(m_2) i_1 + ch(m_1) \sin(m_2) i_2 +$$
$$+ (m_3 ch(m_1) \cos(m_2) - m_4 sh(m_1) \sin(m_2)) i_3 + (m_3 ch(m_1) \sin(m_2) + m_4 ch(m_1) \cos(m_2)) i_4,$$

$$ChM = ch(m_1)\cos(m_2)i_1 + sh(m_1)\sin(m_2)i_2 +$$

$$+(m_3 sh(m_1)\cos(m_2) - m_4 ch(m_1)\sin(m_2))i_3 + (m_3 ch(m_1)\sin(m_2) + m_4 sh(m_1)\cos(m_2))i_4.$$

3. Квадріплексна ГЧС з таблицею множення:

	i_1	i_2	i_3	i_4
i_1	i_1	i_2	i_3	i_4
i_2	i_2	$-i_1$	i_4	$-i_3$
i_3	i_3	i_4	$-i_1$	$-i_2$
i_4	i_4	$-i_3$	$-i_2$	i_1

$$M = m_1 i_1 + m_2 i_2 + m_3 i_3 + m_4 i_4,$$

$$e^M = \frac{e^{m_1}}{2}[(e^{m_4}\cos(m_3 - m_2) + e^{-m_4}\cos(m_3 + m_2))i_1 +$$

$$+(-e^{m_4}\sin(m_3 - m_2) + e^{-m_4}\sin(m_3 + m_2))i_2 +$$

$$+(e^{m_4}\sin(m_3 - m_2) + e^{-m_4}\sin(m_3 + m_2))i_3 +$$

$$+(e^{m_4}\cos(m_3 - m_2) - e^{-m_4}\cos(m_3 + m_2))i_4],$$

$$LnM = \frac{1}{4}\ln N(m)i_1 + (\frac{1}{2}arctg\frac{2(m_1 m_2 + m_3 m_4)}{m_1^2 - m_2^2 + m_3^2 - m_4^2} + 2\pi k)i_2 +$$

$$+(\frac{1}{2}arctg\frac{2(m_1 m_2 + m_2 m_4)}{m_1^2 + m_2^2 - m_3^2 - m_4^2} + 2\pi k)i_3 + \frac{1}{4}\frac{(m_1 + m_4)^2 + (m_3^2 - m_2^2)}{(m_1 - m_4)^2 + (m_3 + m_2)^2}i_4,$$

$$ShM = \frac{1}{2}[(sh(m_1 - m_4)\cos(m_3 - m_2) + \cos(m_3 - m_2)sh(m_1 + m_4))i_1 +$$

$$+(ch(m_1 - m_4)\sin(m_2 + m_3) - ch(m_1 + m_4)\sin(m_3 - m_2))i_2 +$$

$$+((ch(m_1 - m_4)\sin(m_3 + m_2) + ch(m_1 + m_4)\sin(m_3 - m_2))i_3 +$$

$$+(-ch(m_1 - m_4)\cos(m_3 + m_2) + sh(m_1 + m_4)\cos(m_3 - m_2))i_4],$$

$$ChM = \frac{1}{2}[(ch(m_1 + m_4)\cos(m_3 - m_2) + \cos(m_3 + m_2)ch(m_1 \_ m_4))i_1 +$$

$$+(sh(m_1 - m_4)\sin(m_2 + m_3) - sh(m_1 + m_4)\sin(m_3 - m_2))i_2 +$$

$$+((sh(m_1 + m_4)\sin(m_3 - m_2) + sh(m_1 - m_4)\sin(m_3 + m_2))i_3 +$$

$$+(-ch(m_1 - m_4)\cos(m_3 + m_2) + sh(m_1 + m_4)\cos(m_3 - m_2))i_4].$$

Рішення задачі розподілення секрету з використанням гіперкомплексних числових систем

Схемою розподілення секрету (СРС) називається така схема, що дозволяє «розділити» секрет між декількома учасниками таким чином, щоб заздалегідь за-дана дозволена множина учасників могла однозначно відновити секрет, а недозволена — не одержати ніякої додаткової інформації про можливе значення секрету. Існує деяка схема розподілення, названа (k,t)-граничною схемою. У найпростішому варіанті цієї схеми будь-яке повідомлення розподіляється на t частин так, що за будь-яких k частин можна відновити повідомлення [43].

Схема на основі гіперкомплексних чисел. Модулярний підхід до формулювання й вирішення задач розподілення секрету вперше запропонували Ч. Асмус і Л. Блюм. Усі перетворення в цій задачі основані на використанні теорії чисел.

Розглянемо модулярну схему, де модулі вибираються як гіперкомплексні числа $m_1, m_2, ..., m_n$ із взаємно простими коефіцієнтами. Залишками є: $a_i = S \bmod m_i$, де $S = S_0 + iS_i$, S_0 — секретний ключ, S_i — вибирається випадково й рівно ймовірно дилером за визначеною умовою. $X_A = \{x_A + rm_A : r \in Z[i]\}$ — множина рішень системи порівнянь $x \equiv a_i (\operatorname{mod} m_i)$. Результатом є секрет $s_0 = \operatorname{Re}(x_A)$.

Для комплексних, подвійних і дуальних чисел також розроблено теорію порівнянь. Важливою умовою для обчислень є можливість представлення комплексних, подвійних і дуальних чисел у «діапазоні» множини відповідно комплексних, подвійних і дуальних чисел. Для подвійних і для дуальних чисел буде справедливе розширення фундаментальної теореми Гауса про ізоморфізм лишків подвійних і дуальних чисел стосовно дійсних, якщо дійсний модуль N дорівнює нормі відповідно подвійного чи дуального модуля і за умови взаємної простоти коефіцієнтів модулів. Усе це підтверджує можливість побудови задачі розподілення секрету й поліпшення її обчислювальної складності для алгебр подвійних і дуальних чисел.

Після задачі розподілення секрету необхідно відновити отриману інформацію. Алгоритм відновлення являє собою багатокрокову процедуру, в якій на кожному кроці перетворення здійснюється знаходження шуканої величини в розширюваному діапазоні. Цей алгоритм заснований на виконанні простих операцій. Найбільші труднощі тут можна зустріти при обчисленні оберненої величини. Важливу роль в алгоритмі грає функція Ейлера, що в аналітичному вигляді представлена тільки в полі дійсних чисел. При роботі з гіперкомплексними системами для обчислення оберненої величини використовуються штучні прийоми, один з яких базується на ізоморфному переході в область дійсних чисел із застосуванням фундаментальної теореми Гауса, а другий застосовує алгоритм Евкліда. Для гіперкомплексних чисел теж можна використовувати алгоритм Евкліда, але треба враховувати деякі додаткові умови: необхідно контролювати — чи є число дільником нуля, а також при діленні необхідно, щоб гіперкомплексне число було цілим.

Для вирішення задачі знаходження оберненої величини ефективним є й ізоморфний перехід від залишків гіперкомплексної системи до залишків дійсних чисел.

Для запропонованої схеми розподілення секрету для гіперкомплексних чисел розглянемо важливе питання стійкості схеми [5].

Оцінимо значення параметрів $\tau_A = |S_A|$, $I_A = -\log(|S_A| / |S_0|)$, перший з яких дорівнює числу випробувань, вироблених учасниками коаліції A для пошуку секретного ключа $s^{(0)}$ за наявними у них проекціями, а другий — «комбінаторній» кількості, що міститься в наборі проекцій $(c_i : i \in A)$ про ключ $s^{(0)}$.

Для відновлення секретного ключа $s^{(0)} \in S_0$ за набором проекцій $(c_i : i \in A)$ учасникам коаліції A буде потрібно виконати не менш

$$\tau_A = |S_A| \geq \frac{\pi M_2}{4(M_1 + 2\sqrt{M_2})} - 1 - \pi\sqrt[4]{M_2}$$

випробувань елементів множини S_0. При цьому кількість інформації щодо ключа $s^{(0)}$, який міститься в наборі $(c_i : i \in A)$, задовольняє нерівності

$$I_A \leq -\log\left(\frac{\pi\sqrt{M_2}}{4M_1}\left(\frac{1}{1+\frac{2\sqrt{M_2}}{M_1}}\right) - \frac{1}{\sqrt{M_2}} - \frac{\pi}{\sqrt[4]{M_2}}\right).$$

Розглянемо модулярну СРС $\Sigma^{(0)}(m'_1, m'_2, \ldots, m'_n)$ над кільцем Z, що відповідає послідовності натуральних чисел $m'_1, m'_2, \ldots, m'_n$, які задовольняють умові

$$M'_1 \overset{\text{def}}{=} \max_{\substack{A \subseteq P: \\ |A|=k-1}} m'_A < M'_2 \overset{\text{def}}{=} \min_{\substack{A \subseteq P: \\ |A|=k}} m'_A,$$

де $m'_A = \prod_{i \in A} m'_i$, $A \subseteq P$. Зазначена СРС є (k,n) граничною схемою розподілення секрету для множини секретних ключів $S'_0 = \{s'_0 \in Z : M'_1 < s'_0 < M'_2\}$. Справедлива рівність $|S'_0| = M'_2 - M'_1 - 1$.

Тоді для параметрів τ'_A і I'_A, що визначаються аналогічно введеним вище параметрам τ_A і I_A відповідно, справедливі наступні оцінки:

$$\frac{M'_2 - M'_1}{M'_1} - 1 \leq \frac{M'_2 - M'_1}{m'_A} - 1 \leq \tau'_A \leq \frac{M'_2 - M'_1}{m'_A} + 1,$$

$$\log m'_A + \log\left(\frac{M'_2 - M'_1 - 1}{M'_2}\right) \leq I'_A \leq \log M'_1 + \log\left(\frac{M'_2 - M'_1 - 1}{M'_2 - 2M'_1}\right).$$

Далі обмежимося розглядом коаліцій $A \subseteq P$, що задовольняють умові $m'_A = M'_1$. У цьому випадку при великих значеннях M'_1 і M'_2 справедливі наступні рівності:

$$\tau'_A = \frac{M'_2 - M'_1}{M'_1},$$

$$I'_A = \log M'_1 .$$

Припустимо, що СРС $\Sigma(m_1, m_2, \ldots, m_n)$ і $\Sigma^{(0)}(m'_1, m'_2, \ldots, m'_n)$ задовольняють наступній умові $m'_i = N(m_i)$, $i \in \overline{1,n}$. У цьому випадку $m'_A = N(m_A)$ для кожного $A \subseteq P$, зокрема, $M_1 = M'_1$, $M_2 = M'_2$. Помітимо, що при виконанні цієї умови множини ключів у розглянутих схемах розподілення секрету мають різні потужності $|S_0| = \sqrt{M_2}$, $|S'_0| = M_2 - M_1$. Тому коректне порівняння стійкості зазначених СРС припускає використання параметрів I_A, I'_A.

Нехай M_1, $M_2 \to \infty$ так, що $\frac{M_2^{3/4}}{M_1} \to \infty$, $M\ \frac{\sqrt{M_2}}{M_1} \to 0$. Тоді справедлива наступна нерівність: $I'_A - I_A \geq \log\left(\frac{\pi}{4}\sqrt{M_2}\right) + o(1)$, де $o(1) \to 0$ при M_1, $M_2 \to \infty$. Це означає, що кількість інформації про секретний ключ, що міститься в проекціях учасників забороненої коаліції A СРС $\Sigma(m_1, m_2, \ldots, m_n)$, приблизно на $\log\left(\frac{\pi}{4}\sqrt{M_2}\right)$ біт менше, ніж кількість інформації про ключ, що міститься в проекціях учасників такої ж коаліції СРС $\Sigma^{(0)}(m'_1, m'_2, \ldots, m'_n)$. Аналогічний результат, що свідчить про більш високу стійкість запропонованої СРС у порівнянні з модулярною схемою розподілення секрету в дійсних числах, виходить і в тому випадку, коли потужності множини ключів у обох СРС (практично) збігаються.

Отже, обчислювальна стійкість СРС, що відповідає системі гіперкомплексних цілих чисел, вище обчислювальної стійкості СРС, що відповідає системі цілих чисел, при (практично) однакових потужностях множини секретних ключів в обох схемах.

Синтез структур цифрових фільтрів із використанням гіперкомплексних числових систем

Роботи по використанню ГЧС для синтезу структур цифрових фільтрів проводяться протягом кількох останніх років. Вони засновані на тому, що при позбавленні «уявностей» у знаменнику передавальної функції з гіперкомплексними коефіцієнтами одержується гіперкомплексна передавальна функція, порядок якої дорівнює добуткові порядку вихідної передавальної функції на вимірність ГЧС. При цьому кожну компоненту цієї гіперкомплексної функції можна розглядати як деяку передавальну функцію дійсного фільтра. Структурні схеми фільтрів із дійсними та гіперкомплексними коефіцієнтами показано на рис. 1 і рис. 2 ($\dim \Gamma = 4$).

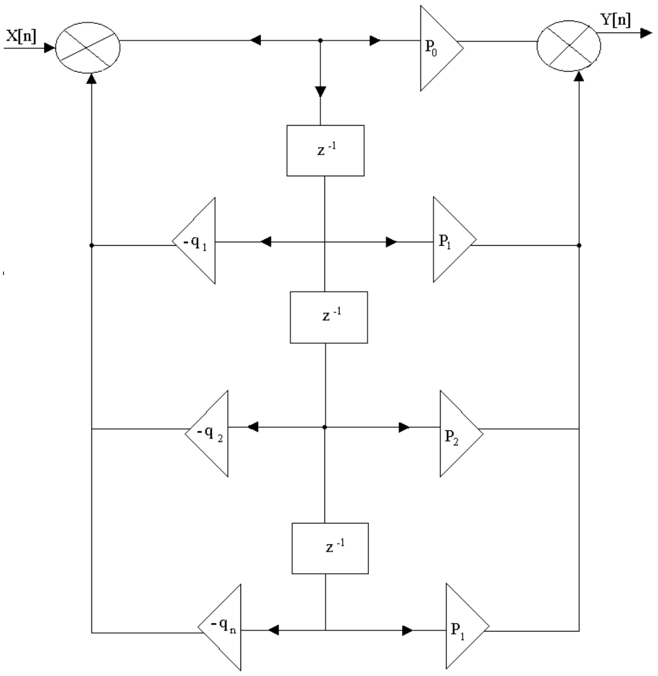

Рис. 1. Структурна схема дійсного фільтра

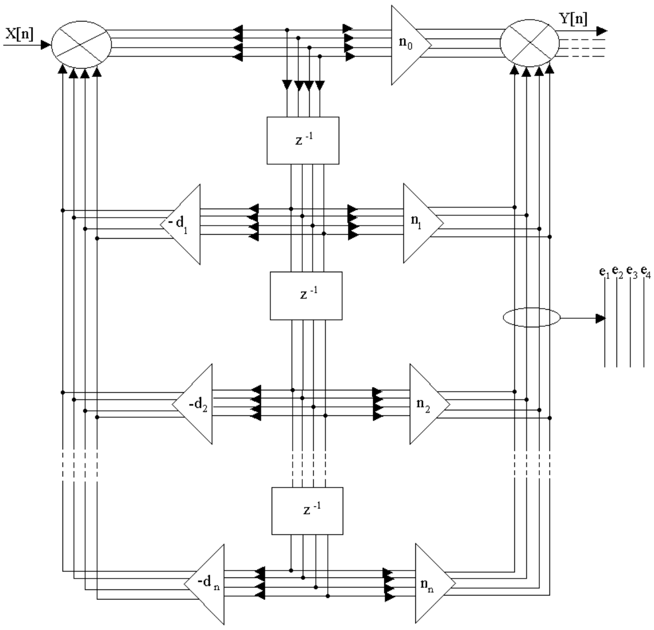

Рис. 2. Структурна схема гіперкомплексного фільтра

Робота фільтрів описується одним і тим же різницевим рекурентним рівнянням:

$$y[n] = \sum_{i=0}^{l} p_i x[n-i] - \sum_{i=1}^{l} q_i y[n-i],$$

але в другому випадку всі коефіцієнти гіперкомплексні. Сигнал на вході гіперкомплексного фільтра такої структури — дійсний, але після першого ж множення на один із коефіцієнтів фільтра він перетворюється в гіперкомплексний. Вихід — гіперкомплексний, але використовується тільки один із каналів, передавальна функція якого співпадає із заданою.

Наприклад, дійсний фільтр третього порядку з передавальною функцією

$$G_3(z)=\frac{0{,}287589\,z^3+0{,}6888683\,z^2+0{,}6888683\,z+0{,}287589}{z^3+0{,}418204\,z^2+0{,}473048\,z+0{,}061292}$$

може бути еквівалентований фільтром першого порядку $H_T=\dfrac{A+Bz^{-1}}{e_1+Cz^{-1}}$ з триплексними коефіцієнтами:

$$A=0{,}287589\,e_1+1{,}85903517\,e_2-7{,}226039798\,e_3\,;\;B=8{,}010652\,e_2;$$
$$C=0{,}13986328\,e_1+0{,}644012706\,e_2+0{,}0013858400\;53e_3.$$

Амплітудно-частотна характеристика першого компонента цієї передавальної функції повністю співпадає з амплітудно-частотною характеристикою фільтра з дійсними коефіцієнтами (рис. 3).

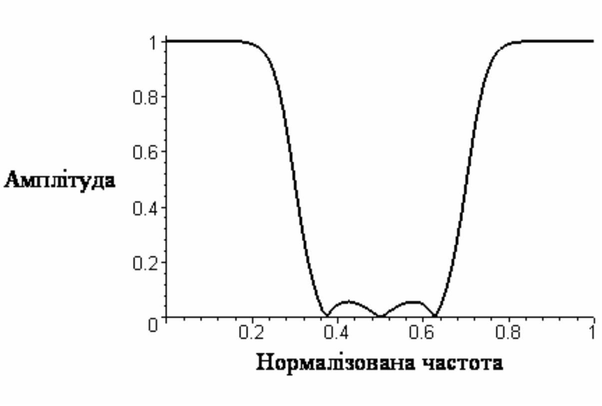

Рис. 3. Передавальна функція гіперкомплексного цифрового фільтра третього порядку

На рис. 4 показано вхідний сигнал, а на рис. 5 — вихідний сигнал фільтра з дійсними коефіцієнтами. На рис. 6–8 показано вихідні сигнали з гіперкомплексними коефіцієнтами.

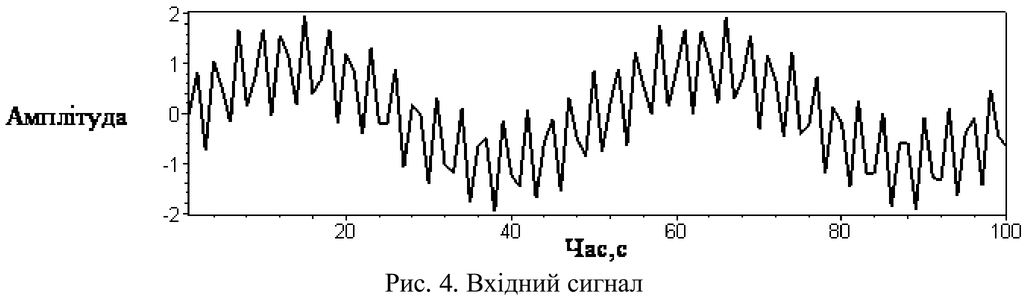

Рис. 4. Вхідний сигнал

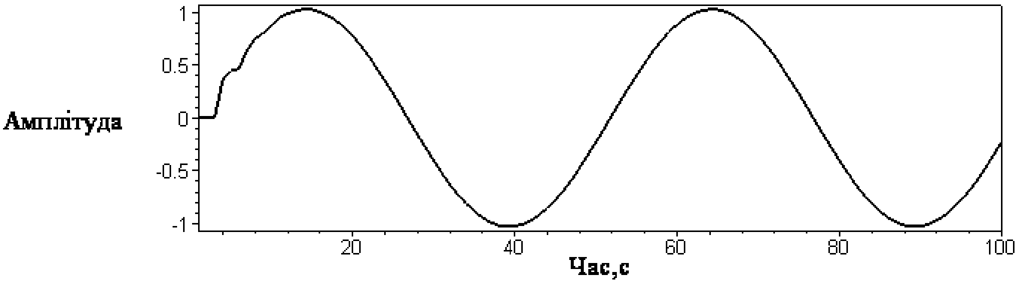

Рис. 5. Вихідний сигнал після фільтра 3-го порядку з дійсними коефіцієнтами

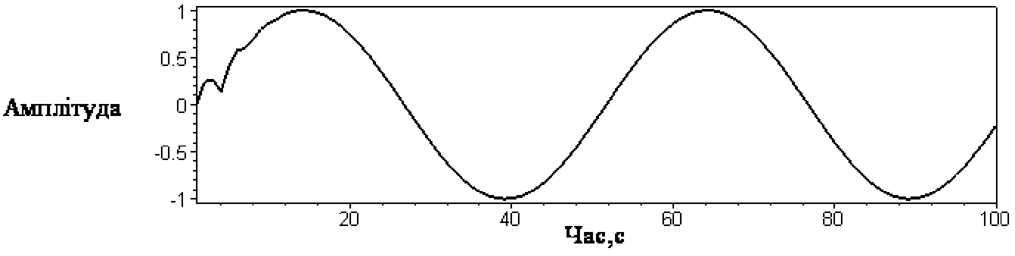

Рис. 6. Вихідний сигнал на першому виході триплексного фільтра.

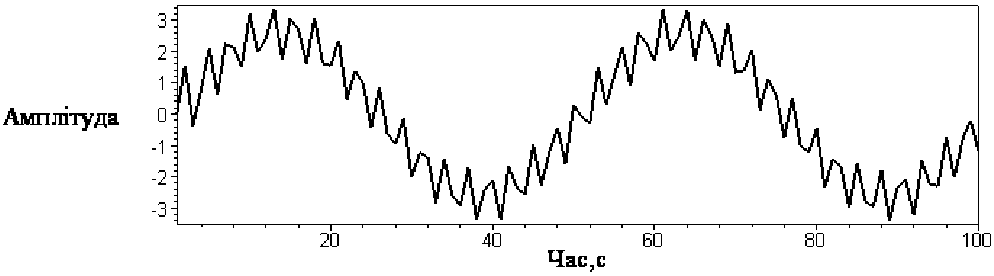

Рис. 7. Вихідний сигнал на другому виході триплексного фільтра

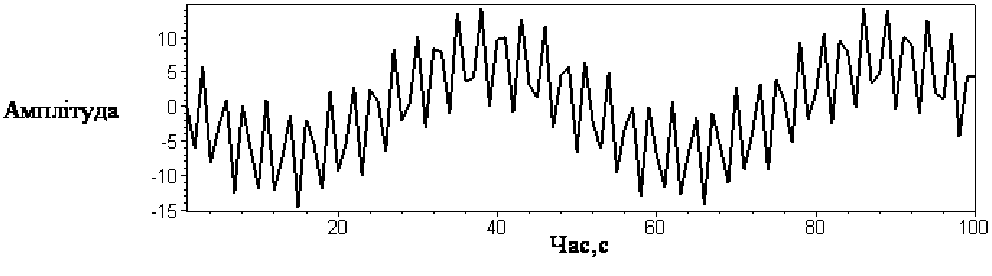

Рис. 8. Вихідний сигнал на третьому виході триплексного фільтра

З рис. 5 і 6 видно, що фільтр з гіперкомплексними коефіцієнтами обробляє сигнал ідентично до фільтра з дійсними коефіцієнтами.

Як показало комп’ютерне моделювання на функціональному рівні за допомогою середовища Quartus, яке було проведено у Відділі спеціалізованих систем моделювання Інституту проблем реєстрації інформації НАН України, гіперкомплексні цифрові фільтри дозволяють роботу на значно вищій тактовій частоті, ніж звичайні цифрові фільтри за інших рівних умов.

Висновки

1. Питання, пов'язані з перечисленням гіперкомплексних числових систем, є важливими, і їхнє вирішення може розкрити подальші перспективи у вивченні цих систем.

2. Важливими для подальшого розвитку теоретичних і практичних положень теорії моделювання будуть кроки по створенню основ математичного аналізу гіперкомплексного змінного. Значну увагу при цьому треба приділяти питанням розвитку теорії функцій гіперкомплексного змінного.

3. Указані вище теоретичні питання орієнтовані на створення ефективних умов і засобів вирішення практичних задач із різних галузей науки та техніки, серед яких керування та орієнтація рухомих об'єктів у просторі, керування роботами та механізмами з багатьма ступенями свободи, керування підводними об'єктами, анімація та обробка кольорового зображення, поліпшення параметрів радіоелектронних приладів, наприклад, цифрових фільтрів, кінематика та динаміка елементарних частинок та інші задачі теоретичної фізики, багаторівнева амплітудна модуляція сигналів, проектування електричних машин і багато інших прикладів.

1. *Синьков М.В., Калиновский Я.А., Бояринова Ю.Е., Федоренко А.В.* Построение некоторых функций в гиперкомплексной числовой системе 4-го порядка // Реєстрація, зберігання і оброб. даних. — 2006. — Т. 8, № 1. — С. 9–16.

2. *Синьков М. В., Калиновский Я.А., Бояринова Ю.Е., Федоренко А.В.* О дифференциальных уравнениях, определяющих функции гиперкомплексного переменного // Реєстрація, зберігання і обробка даних. — 2006. — Т. 8, № 3. — С. 20–24.

3. *Синьков М.В., Калиновский Я.А., Бояринова Ю.Е., Синькова Т.В., Федоренко А.В.* Разработка структур эффективных цифровых фильтров с помощью гиперкомплексного представления информации // Управління розвитком. — 2006. — № 6. — С. 83–84.

4. *Синьков М.В., Калиновский Я.А., Бояринова Ю.Е.* Построение алгоритмов решения нестационарных линейных дифференциальных уравнений в гиперкомплексных числовых системах // Реєстрація, зберігання і оброб. даних. — 2006. — Т. 8, № 4. — С. 38–44.

5. *Алексейчук А.Н., Бояринова Ю.Е.* Модулярная схема разделения секрета над кольцом целых гауссовых чисел // Реєстрація, зберігання і оброб. даних. — 2007. — Т. 9, № 1. — С. 87–99.

6. *Синьков М.В., Губарени Н.М.* Непозиционные представления в многомерных числовых системах. — К.: Наук. думка., 1979. — 136 с.

7. *Study E.* Űber Systeme von Complexen Zahlen // Nachrichten von der K.G.D.M. zu Gottingen. —1889. — N 9. — P. 237–268.

8. *Ball R.S.* The Theory of Screws. Cambridge University Press. — 1-st edition, 1900.

9. *Котельников А.П.* Винтовое счисление и некоторые его приложения к геометрии и механике. — Казань, 1895. — 214 с.

10. *Диментберг Ф.М.* Винтовое исчисление и его приложения в механике. — М.: Наука, 1965. — 200 с.

11. *Noether E.* Hypercomplex Grossen und Darstellungstheorie // Mathematische Zeitschrift. — 1929. — B. 30. — P. 641–692.

12. *Люш В.В.* Теория универсальных чисел и приложения ее к решению алгебраических уравнений // Труды Второго Всесоюзного математического съезда. — Л., 1936. — Т. 2. — С. 49–56.

13. *Люш В.В.* Теория функций триплексного переменного. — Л.: Изд-во ЛКИ, 1936. — 186 с.

14. *Кантор И.Л., Солодовников А.С.* Гиперкомплексные числа. — М.: Наука, 1973. — 144 с.

15. *Rochon D., Shapiro M.* On Algebraic Properties of Bicomplex and Hyperbolic Numbers // Anal. Univ. Oradea, fasc. Math. — 2004. — N 11. — P.71-110.

16. *Dieterich E.* Zur Klassifikation Vierdimensionaler Reeller Divisionsalgebren // Math. Nachr. — 1998. — N 194. — P. 13–22.

17. *Nobauer C.* The Number of Isomorphism Classes of d.g. Near-Rings on the Generalized Quaternion Groups // Proc. of the Conf. on Near-Rings and Near-Fields. — Stellenbosch (South Africa). — 2001. — P. 133–137.

18. *Scheicher K., Tichy R.F., Tomantschger K.W.* Elementary Inequalities in Hypercomplex Numbers Anzeiger. — 1997. — Abt. II. — N 134. — P. 3–10.

19. *Синьков М.В., Калиновский Я.А., Бояринова Ю.Е., Синькова Т.В.* Биплексные числовые системы и функции в них // Реєстрація, зберігання і обробка даних. — 2005. — Т. 7, № 4. — С. 21–29.

20. *Davenport C.M.* An Analytical Solution for the Boussinesq Equation // On line: home.usit.net/~cmdaven/boussnsq.htm (2003).

21. *Стельмашук Н.Т.* Об интегрировании обыкновенных дифференциальных уравнений с F-производными // Дифференциальные уравнения. — 1987. — № 2. — С. 357–358.

22. *Синьков М.В., Синькова Т.В., Калиновский Я.А., Бояринова Ю.Е.* Развитие исследований алгоритмов решения линейных дифференциальных уравнений от гиперкомплексного переменного порядка выше первого // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 6, № 2. — С. 19–27.

23. *Chaitin-Chatelin F., Meskauskas T., Zaoui A.* Computation with Hypercomplex Numbers // GERFACS Technical Report TR/PA/00/69 // On line: http://www.gerfacs.fr (2000).

24. *Синьков М.В., Боярінова Ю.Є., Каліновський Я.О., Постнікова Т.Г., Синькова Т.В.* Алгоритмічно-програмний інструментарій аналітичних обчислень над гіперкомплексними числами в системі комп'ютерної математики MAPLE // Реєстрація, зберігання і оброб. даних. — 2005. — Т. 7, № 2. — С. 18–24.

25. *Синьков М.В., Боярінова Ю.Є., Каліновський Я.О., Постнікова Т.Г., Синькова Т.В.* Модульні операції над гіперкомплексними числами в системі комп'ютерної математики MAPLE // Реєстрація, зберігання і оброб. даних. — 2005. — Т. 7, № 3. — С. 55–62.

26. *Смолин А.Л.* Гиперкомплексные преобразования Лоренца, эфир и остальная физика. — М.: Диалог-МГУ, 1999. — 105 с.

27.Бранец В.Н., Шмыглевский И.П. Применение кватернионов в задачах ориентации твердого тела. — М.: Наука, 1973. — 319 с.

28. *Будьонний М.Ф., Каліновський Я.О., Панов А.П., Петренко А.І., Постнікова Т.Г., Синьков М.В., Синькова Т.В.* Про автоматизоване проектування системи програмно-апаратних засобів на базі гіперкомплексних чисел для задач орієнтації твердого тіла. Частина 1 // Реєстрація, зберігання і обробка даних. — 2001. — Т. 3, № 4. — С. 73–83.

29. *Ignagni M.B.* Optimal Strapdown Attitude Integration Algorithms // AIAA J. of Guadance, Control and Dynamics. —1990. — Vol. 13, N 2. — P. 363–369.

30. *Mukundan R.* Quaternions: From Classical Mechanics to Computer Graphics, and Beyond // Proc. of the 7th Asian Technology Conf. in Mathematics. — 2002. — P. 97–106.

31. *Felsberg M., Bulow T., Sommer G.* Non-commutative Hypercomplex Fourier Transforms of multidimensional Signals // On line: //www.isy.liu.se/~mfe/ publications.html (2001).

32. *Sangwine S.J.* Colour in Image Processing // Electronics & Communication Engineering J. — 2000. — Vol. 12, N 5. — P. 211–219.

33. *Brodsky V., Shoham M.* Dual Numbers Representation of rigid body dynamics // J. of Mechanisms and Machine Theory. — 1999. — Vol. 34, N 5. — P. 693–718.

34. *Bayro-Corrochano E.* Motor Algebra Approach for Visually Guided Robotics // Pattern Recognition. — 2002. — Vol. 35. — P. 279–294.

35. *Ning Ying, Wangdo Kim*. Use of Dual Euler Angles to Describe General Spatial Movements of Human Joints // On line: asme.pinetec.com/bio2001/data/pdfs/a0014419.pdf.

36. *Синьков М.В., Калиновский Я.А., Бояринова Ю.Е., Синькова Т.В., Федоренко А.В.* Разработка структур эффективных цифровых фильтров с помощью гиперкомплексного представления информации // Управління розвитком. — 2006. — № 6. — С. 83–84.

37. *Chichyeva M.A., Chernov V.M.* «One-step» Short-Length DCT Algorithms with Data Representation in the Direct Sum of Associative Algebras // Proc. CAIP'97. — Springer, LNCS 1296. — 1997. — P. 590–596.

38. *Toyoshima H., Higuchi S.* Design of Hypercomplex All-Pass Filters to Realize Complex Transfer Functions // Proc. Second Int. Conf. Information, Communications and Signal Processing. — 1999, Dec. — **2B3.4**. — P. 1–5.

39. *Щербина Ю.В., Клипков С.И.* Использование квазикомплексных векторов для исследования существования установившихся режимов энергетических систем // Электронное моделирование. — 1987. — № 1. — С. 54–56.

40. *Луковников В.И.* Основы бикомплексного исчисления и его применение к расчету электромеханических систем с модуляцией // Электричество. — 1978. — № 2. — С. 26–31.

41. *Kalinowski J.A., Roenko N.V. Sinkov M.V.* Building Nonlinear Functions on Quaternion and Other Hypercomplex Number Systems for the Solution of Applied Mechanics Problems // Proc. of the First Conf. on Parallel Proc. and Appl. Math. — Poland, 1994. — P. 170–177.

42. *Калиновский Я.А., Роенко Н.В., Синьков М.В.* Методы построения нелинейностей в расширениях комплексных чисел // Кибернетика и системный анализ. — 1996. — № 4. — С. 178–181.

43. *Синьков М.В., Бояринова Ю.Е., Калиновский Я.А., Трубников П.В.* Развитие задачи разделения секрета // Реєстрація, зберігання і оброб. даних. — 2003. — Т. 5, № 4. — С. 90–96.

Надійшла до редакції 20.07.2007