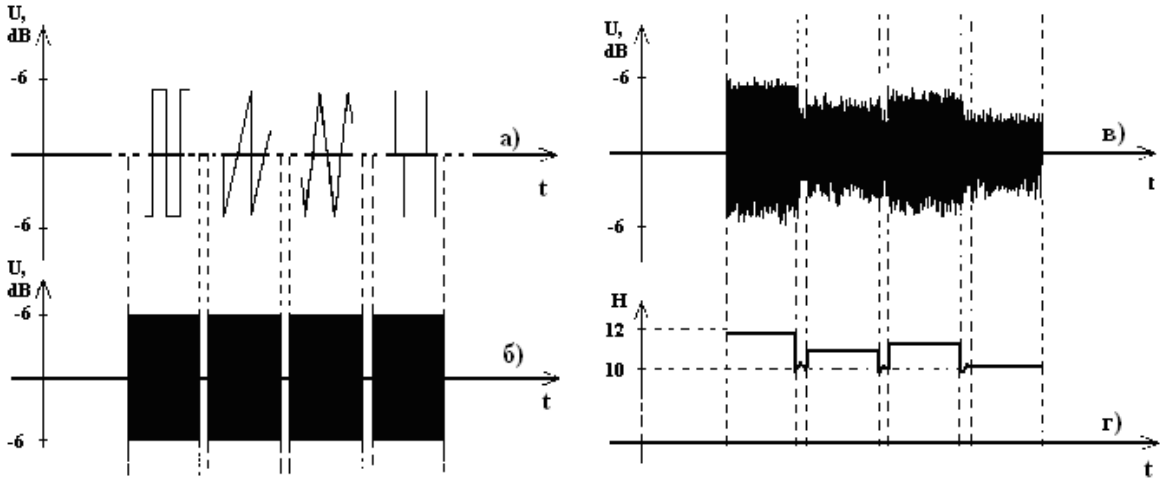

Рисунок 1 - Моделювання періодичних сигналів при дослідженні взаємних залежностей ентропії, потужності та розмаху сигналів

На рисунку 1 показано тільки декілька форм сигналів. Таким чином, встановлено, що оптимальним сигналом для застосування у способі обміну даними з використанням сигналів зі змінною ентропією є випадковий сигнал з характеристиками, близькими до «білого» шуму, тобто, з розподілом ймовірностей станів близьким до нормального та рівномірною спектральною щільністю потужності, також можливим є використання й інших сигналів, які суттєво впливають на ентропію сигналів у каналі, зокрема, періодичні негармонійні коливання прямокутної, трикутної, пилоподібної форми тощо.

Висновок

Проведено дослідження ефективності застосування різних форм сигналів для покращення показників ефективності при застосування різних імовірнісних характеристик, на основі якого встановлено, що максимальна ефективність спостерігається при використанні випадкових сигналів з нормальним розподілом ймовірностей станів та рівномірною спектральною щільністю.

Список використаних джерел

1. Козленко М. І. Дослідження ефективності застосування різних типів сигналів в інформаційних каналах систем керування та контролю // Методи та прилади контролю якості. – 2006. - № 16. - Івано-франківськ: ІФНТУНГ, 2006. – С. 91 - 93.
2. Козленко М. І., Мельничук С. І. Оцінка ефективності застосування різних сигналів при реалізації обміну даними на основі способу зміни ентропії сигналів інформаційного каналу в низових мережах // Вестник Херсонского национального технического университета. – 2006. - № 2(25). – Херсон: ХНТУ, 2006. - С. 231 - 234.
3. Козленко М. І., Мельничук С. І. Дослідження впливу форми періодичних сигналів на ентропію розподілу ймовірностей станів у провідникових каналах обміну даними // XIII Міжнародна конференція з автоматичного управління (Автоматика-2006). Тези доповідей тринадцятої міжнародної науково-технічної конференції. м. Вінниця, 25-28 вересня 2006 року. – Вінниця: видавництво ВНТУ “УНІВЕРСУМ- Вінниця”, 2006.– С. 338.

УДК 681.325

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ТЕОРЕТИКО-ЧИСЛОВОГО БАЗИСУ ГАЛУА

Николайчук Я.М.[1)], Степанюк Н.П.[2)], Дутчак М.В.[3)], Шкодін О.В. [4)]

Тернопільський національний економічний університет

[1)] д.т.н., професор; [2-4)] магістранти

І. Постановка проблеми

Проблема технології формування, перетворення, опрацювання та передавання інформаційних потоків на основі кодів поля Галуа потребує досконалого дослідження основ теорії чисел у різних теоретико-числових базисах, які широко застосовуються для формування, передавання цифрового опрацювання та зберігання даних. Застосування різних ТЧБ створює перспективи вдосконалення організації баз даних, підвищення надійності систем захисту даних, удосконалення методів побудови кодових шкал та дисків та інше.

II. Мета роботи

Метою дослідження є вивчення властивостей ТЧБ Галуа та розробка методів їх застосування при організації баз даних, побудові кодових шкал та дисків та проектуванні систем захисту даних в спеціалізованих комп'ютерних системах.

III. Характеристика теоретико-числових базисів

Вибір базисної функції виконується в залежності від системних характеристик різних каналів зв'язку та умов експлуатації комп'ютерних та телекомунікаційних систем. В сучасних комп'ютерних та телекомунікаційних системах широко використовуються ТЧБ на основі кусково–постійних дискретних функцій, які забезпечують значно простішу реалізацію цифрових генераторів, а також спрощують алгоритми цифрового опрацювання сигналів.

Підвищити ефективність кодування даних шляхом зменшення розрядності дозволяє використання менш надлишкових двійкових та кодів Грея. Двійкові коди Радемахера використовуються, як основні в комп'ютерних системах. Коди Грея застосовуються, як основа кодових шкал та в перетворювачах форми інформації завдяки унікальній властивості зміни лише одного розряду при переході між позиціями, яка дозволяє однозначно ідентифікувати кодові комбінації.

Здійснити перехід від паралельного подання коду повідомлення до вертикальної інформаційної технології та покращити показники систем дозволяють кодові системи Ґалуа. Кодові системи Ґалуа, як і двійкові коди, використовують при реалізації процедур цифрової обробки інформації. Отже, теоретичною основою кодів поля Галуа є теорія чисел, теорія структур, груп та полів Галуа [1-2].

IV. Система функцій Ґалуа та кодові системи Ґалуа

Перехід до різних упорядкувань функцій у системі Ґалуа здійснюється з базису Уолша з упорядкуванням функцій за рекурсивним законом. За *n*-розрядними фрагментами рекурсивної послідовності, яка утворюється відповідно до породжуючого вектора поля Ґалуа $GF(2^n)$, згідно відображення через систему функцій Радемахера формуються номери функцій Уолша та Ґалуа в системі.

Із рекурсивно впорядкованої системи Уолша відповідно впорядковані перші *n* функцій Ґалуа формуються згідно співвідношення

$$Gal(n,\theta,i) = Wal(Ent(2^n\theta), \frac{2^{i+1}-1}{2^n}),$$

де $i = 0,1,\ldots,2^n - 1$, *Ent*– функція виділення цілої частини.

Проведені дослідження встановили можливість формування функцій Ґалуа із систем Радемахера та Грея. Перші *n* функцій Ґалуа в системі подаються у вигляді добутку функцій Радемахера та Грея

$$Gal(n,\theta,i) = \prod_{k=0}^{n-1}(Rad(k+1, \frac{2^{i+1}-1}{2^n}))^{h_k} = \prod_{k=0}^{n-1}(Gry(k+1, \frac{2^{i+1}-1}{2^n}))^{r_k},$$

де $h_{n-1}h_{n-2}\ldots h_0$ – запис у коді Грея числа *q*, двійковий код якого є *n*-розрядним фрагментом $v_i v_{i+1} v_{i+2}\ldots v_{i+n-1}$ рекурсивної послідовності $v_0, v_1, v_2, \ldots$; $r_{n-1}r_{n-2}\ldots r_0$ – двійковий код, який є *n*-розрядним фрагментом $v_i v_{i+1} v_{i+2}\ldots v_{i+n-1}$ рекурсивної послідовності $v_0, v_1, v_2, \ldots$.

Повний набір 2^n функцій рекурсивної системи Ґалуа $Gal(n,\theta,i)$ отримують із перших *n* функцій системи процедурою рекурсивного зсуву на $\Delta\theta = \frac{1}{2^n}$ згідно другої діагоналі кожної наступної функції відносно попередньої

$$Gal(n,\theta,i+1) = Gal(n,\theta+\Delta\theta,i).$$

Впорядкування функцій Ґалуа в наборі відповідає синтезованому за породжуючим вектором упорядкуванню функцій Уолша.

Процедура переходу від дискретних значень функцій Уолша до дискретних значень функцій Ґалуа подається матричною операцією

$$\|Gal\| = \|W\| \cdot \|R\|,$$

де $\|Gal\|$ – матриця розміру $N\times n$ системи Ґалуа; $\|W\|$ – матриця розміру $N\times N$ рекурсивно впорядкованих функцій Уолша; $\|R\|$ – матриця розміру $N\times n$ відображеної вагової мережі Радемахера.

Для прикладу, матрична операція переходу від функцій Уолша до функцій Ґалуа та матриця розміру 8×8 дискретних значень функцій Ґалуа в полі $GF(2^3)$ з породжуючим вектором 1101 згідно процедури рекурсивного розширення подаються відповідно

$$\begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{Vmatrix} = \begin{Vmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & -1 \\ -1 & -1 & 1 \\ -1 & 1 & 1 \end{Vmatrix} \longrightarrow \begin{Vmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 \end{Vmatrix}.$$

При дискретизації за параметром часу перших n функцій Ґалуа та здійсненні бінарної заміни значень функцій 1 на 0, –1 на 1, згідно виразу

$$g_k(\theta_s)=(1-Gal(n-k-1,\theta_s))/2,$$

одержують матрицю кодових елементів Ґалуа розміру $n\times N$, $k=0,1,\ldots,n-1$.

При дискретизації системи N функцій Ґалуа $\{Gal(n,\theta,i)\}$, $i=0,1,\ldots.2^n-1$ та перетворенні значень функцій отримують повну матрицю кодових елементів Ґалуа розміру $N\times N$, впорядкованих із поелементним рекурсивним зсувом згідно другої діагоналі матриці Ґалуа. Номер s повідомлення однозначно визначається n-координатним вектором $n=log_2 N$.

Висновок

Використання властивості рекурентності базису Галуа в наш час склало фундаментальну основу розробки теорії та принципово нових технічних рішень багатьох складних задач і практичних застосувань у галузі цифрового формування, передавання і опрацювання інформаційних потоків, в тому числі при побудові кодових систем Галуа, кодових шкал Галуа, розробці баз даних та нових методів передавання інформації в умовах інтенсивних завад.

Список використаних джерел

1. Николайчук Я.М. Коди поля Галуа : теорія і застосування – Тернопіль: ТзОВ "Терно–граф", 2012. – 576 с.
2. Николайчук Я.М. Теорія джерел інформації - Тернопіль: ТзОВ «Терно-граф», 2010.- 536с.

УДК 681.3

СИСТЕМА ЗАХИСТУ МАНІПУЛЬОВАНИХ ДАНИХ В БАЗИСІ ГАЛУА

Николайчук Я.М.[1)], Шкодін О.В.[2)]
Тернопільський національний економічний університет
[1)] д.т.н., професор; [2)] магістрант

І. Постановка задачі

Сучасні тенденції розвитку пакетної передачі даних в мережі, потребують передавання інформації з максимальною швидкістю на максимальну відстань, із виправленням помилок і із захистом від несанкціонованого доступу. У зв’язку з цим актуальним є питання ефективного маніпулювання сигналів в базисі Галуа.