4. Усі вихідні дуги δ_r, що виходять із j-тої вершини, замінюємо дугами γ_r вигляду $\gamma_r = \{x_r, y_r, q_r, s_r\}$, де $q_r = \dfrac{p_r}{1-p}$, тут $p = p_{rr}$, $s_r = t_r + \dfrac{tp_r}{1-p}$, тут $t = t_{rr}$, для всіх $r = 1, 2, \ldots, m$.

Тепер можна записати загальний алгоритм скорочення ймовірнісних графів.

1. Побудувати зважений орієнтований граф $G(X, \Gamma)$ із часово-ймовірнісними характеристиками.
2. Якщо існують паралельні дуги, то скоротити цей фрагмент графа за відповідним алгоритмом 2.
3. Якщо існує хоча б одна проміжна вершина в графі, то зафіксувати її, інакше перейти до пункту 8.
4. Якщо проміжна вершина має дугу-петлю, то перейти до пункту 5, інакше – перейти до пункту 6.
5. Видалити дугу-петлю за допомогою алгоритму 3.
6. Видалити проміжну вершину за алгоритмом 1.
7. Перейти до пункту 2.
8. Записати результат у вигляді стрічкової матриці, яка відповідатиме скороченому графу.

Отже, у результаті проведеної верифікації правильності виконання алгоритмічного процесу кремнієвої компіляції за часово-ймовірнісним критерієм із використанням стрічкових матриць та переходом до скорочених графів виявилося, що верифікація процесу проектування топології інтегральних схем збігається на алгоритмічному рівні з мінімізацією цього процесу за часово-ймовірнісним критерієм.

1. Atamanyuk R. Improvement of method of the silicic compiling through discrete optimization of topology and structurally-technological limitations of the integrated circuit // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії: Матеріали Міжнародної науково-технічної конференції TCSET'2006 (Львів – Славське, 28 лютого – 4 березня 2006 р.). – Львів, 2006. – С.436–437.
2. Атаманюк Р. Оптимізація процесу кремнієвої компіляції за часово-ймовірнісним критерієм // Міжнародна конференція студентів і молодих науковців з теоретичної та експериментальної фізики ЕВРИКА-2006 (Львів, 15–17 травня 2006 р.). – Львів, 2006. – С.85.
3. Эйрис Р. Проектирование СБИС. Метод кремниевой компиляции. – М.: Наука, 1988. – 456 с.
4. Проектирование СБИС / М. Ватанабэ, К. Асада, К. Кани, Т. Оцуки: Пер. с япон. – М.: Мир, 1988. – 304 с.

The verification of silicic compiling process which is modeled by the probability graphs is reduced to the shorting its graph and so to foundation all graphs which satisfy to the time-probability criterion. In this sense the band matrixes and the deleting vertexes method are used.

Key words: *silicic compiling, band matrixes, vertexes method.*

УДК 004.415.3+519.711
ББК 22.181

Н.В. Превисокова, Л.Б. Петришин

ТЕОРЕТИКО-ЧИСЛОВІ ОСНОВИ ДИСКРЕТНОГО ГАРМОНІЧНОГО АНАЛІЗУ В СИСТЕМІ РАДЕМАХЕРА

З єдиних позицій теоретико-числових перетворень здійснено аналіз та встановлено ряд проміжних систем функцій, що утворюють відповідні коди чи кодові системи. Визначено черговість і процедури їх творення та взаємоперетворень, що дозволило класифікувати та в майбутньому оцінити ефективність дискретного гармонічного аналізу в поданих системах функцій.

Ключові слова: *унітарні функції, функції Радемахера, дискретний гармонічний аналіз, кодові системи, аналітичні взаємозалежності системи функцій.*

Вступ. Останнім часом широкого розповсюдження набувають складні територіально розподілені інформаційні системи, які містять у собі засоби формування, перетворення, передавання та оброблення інформації [1, 2]. Більшість обчислювальних систем функціонує з використанням традиційних кодів і при переході до інших, спеціалізовано орієнтованих методів кодування виникає потреба кодового та алгоритмічного адаптування. Це зумовило необхідність установлення аналітичних взаємозалежностей між базисами та системними функціями та визначення їхньої первинності та функціоналів взаємоперетворення.

Досвід наукової роботи й наукові результати [3–4] підтверджують можливість ефективної технічної, алгоритмічної, програмної реалізації та покриття більшості системних функцій із забезпеченням хороших динамічних параметрів при переході до інших методів кодування.

Проблема аналізу ефективності взаємозв'язку різних дискретних базисів і систем функцій неодноразово вирішувалась ученими в галузі цифрового оброблення та перетворення сигналів [3, 5, 6], проте не охоплювалась з єдиних теоретичних позицій усієї повноти взаємодії зв'язків різних базисів та систем функцій, взаємозалежності між базисами, системами функцій та відповідними їм кодами та кодовими системами, що не дало можливості повністю здійснити ефективні міжбазисні та міжсистемні функціональні перетворення.

У пропонованих матеріалах статті здійснено аналіз дискретних теоретико-числових базисів і систем та подано результати дослідження математичних основ, аналітичних взаємозалежностей і визначення основних властивостей, на підставі яких здійснено класифікацію базисів та систем функцій, а також створених за їх допомогою кодових систем і базисних матриць теоретико-числових трансформацій [4].

Для визначення теоретико-числових основ кодів та кодових систем здійснимо дослідження основних упорядкувань базисних функцій та систем функцій, установимо функціональні взаємозалежності базисних перетворень та кодових систем, що ними творяться.

Дискретні лінійно-збіжні теоретико-числові базиси та системи функцій підрозділяються на дискретно-гармонічні та дискретно-нерегулярні. Аналіз теоретико-числових базисів та систем функцій розпочнемо з першої групи, оскільки склад її функцій є одним з основних.

Дискретно-гармонічні теоретико-числові базиси та системи функцій. Як вихідні в засобах перетворення форми інформації широкого застосування набули унітарні коди [2, 4, 6], котрі характеризуються значною розрядною надлишковістю інформаційних слів, яка зумовлена тим, що кількість розрядів бінарного подання слова відповідає повній шкалі квантування діапазону перетворення N. Оскільки унітарні коди не є ефективними при прийманні-передаванні та цифровому обробленні, бо потребують відповідної N-розрядної шини даних, виникає необхідність підвищення ефективності кодування шляхом зменшення кількості розрядів. Щоб здійснити перехід до більш ефективних кодів, виникає необхідність аналітичного подання унітарних кодів та встановлення функціональних залежностей з іншими кодами чи системами кодування.

Для математичного подання унітарних кодів використовуються унітарні функції, які аналітично подаються таким виразом:

$$Uni(m,\theta,i) = sign(\sin(2^m \pi(\theta + i \cdot 2^{1-n}))),$$

де $n = \log_2 N$ – найвищий порядок набору системи функцій;

N – модуль цілочислових дискретних значень системи;

$\theta = t/T$; $(0 \le \theta < 1)$ – нормований параметр часу на одиничному інтервалі визначення;

$\mathrm{T} = 2\pi$; $0 \le t < 2\pi$; t – потокове значення часу;

$i = 0,1,\dots,2^{n-m} - 1$ – порядковий номер функції в наборі з номером m;

$m = 0,1,\dots,n$ – номер набору функцій у системі n-го порядку.

Система унітарних функцій є лінійно залежною, оскільки частина функцій системи є лінійною комбінацією інших функцій системи, і не утворює базису.

Однією із характеристичних властивостей систем кодування є ортогональність їх системних функцій за часом чи за частотою.

Унітарні функції не є ортогональними в частотній ділянці, оскільки:

$$\int_0^1 Uni(m,\theta,i)Uni(k,\theta,i)d\theta \ne 0$$

для визначених k, m, i, j, де $k \ne m$, $i \ne j$, і не ортогональні у фазовій ділянці, тому що

$$\int_0^1 Uni(m,\theta,i)Uni(m,\theta,j)d\theta \neq 0,$$

а функція $Uni(m,\theta,j)$ є результатом фазового зсуву функції $Uni(m,\theta,i)$.

Неортогональність системи унітарних функцій є її властивістю, яка зумовлює некомпактне пакування кодових елементів системи, що спричиняє до значної надлишковості інформаційних потоків.

Функції $Uni(m+1,\theta,i)$ старших порядків $m+1$ у повному наборі є результатом попарного добутку вибіркових функцій $Uni(m,\theta,i)$ нижчих порядків m (крім $Uni(0,\theta,0)$) згідно з наступними залежностями:

$$Uni(m,\theta,i)\cdot Uni(m,\theta,i+2^{n-m-2}) = Uni(m+1,\theta,i), \tag{1}$$

$$Uni(m,\theta,i+2^{n-m-1})\cdot Uni(m,\theta,i+2^{n-m-1}+2^{n-m-2}) = Uni(m+1,\theta,i), \tag{2}$$

для яких $i = 0,1,\ldots,2^{n-m-1}-1$, а також згідно з

$$Uni(m,\theta,i)\cdot Uni(m,\theta,i+3\cdot 2^{n-m-2}) = Uni(m+1,\theta,i+2^{n-m-2}), \tag{3}$$

для цього виразу $i = 0,1,\ldots,2^{n-m-2}-1$.

Доведення співвідношень (1) – (2) проведемо за індукцією.

Згідно з означенням унітарних функцій виконується співвідношення:

$$Uni(m,\theta,i+1) = sign(\sin(2^m\pi(\theta+(i+1)\cdot 2^{1-n}))) =$$

$$= sign(\sin(2^m\pi(\theta+i\cdot 2^{1-n}+2^{1-n}))) = Uni(m,\theta+2^{1-n},i). \tag{4}$$

Твердження (1) – (2) виконуються для $i = 0$.

Припустимо, що для будь-якого $k = i$, $k = 0,1,\ldots,2^{n-m-1}-2$ твердження справедливі, тобто:

$$Uni(m,\theta,k)\cdot Uni(m,\theta,k+2^{n-m-2}) = Uni(m+1,\theta,k) \tag{5}$$

$$Uni(m,\theta,k+2^{n-m-1})\cdot Uni(m,\theta,k+2^{n-m-1}+2^{n-m-2}) = Uni(m+1,\theta,k). \tag{6}$$

Згідно зі співвідношеннями (4)–(5) для $i = k+1$

$$Uni(m,\theta,k+1)\cdot Uni(m,\theta,k+1+2^{n-m-2}) =$$

$$= Uni(m,\theta+2^{1-n},k)\cdot Uni(m,\theta+2^{1-n},k+2^{n-m-2}) = Uni(m+1,\theta+2^{1-n},k) = Uni(m+1,\theta,k+1).$$

Згідно зі співвідношеннями (4), (6) також виконується:

$$Uni(m,\theta,k+1+2^{n-m-1})\cdot Uni(m,\theta,k+1+2^{n-m-1}+2^{n-m-2}) =$$

$$= Uni(m,\theta+2^{1-n},k+2^{n-m-1})\cdot Uni(m,\theta+2^{1-n},k+2^{n-m-1}+2^{n-m-2}) =$$

$$= Uni(m+1,\theta+2^{1-n},k) = Uni(m+1,\theta,k+1),$$

тобто твердження (1) – (2) виконуються для всіх $i = 0,1,\ldots,2^{n-m-1}-2$, що й необхідно довести.

Доведення співвідношення (3) проводиться за індукцією.

Справджується також взаємозалежність:

$$Uni(m,\theta,i)\cdot Uni(m,\theta,i+2^{n-m-1}) = Uni(0,\theta,2^{n-1}),$$

для якої $i = 0,1,\ldots,2^{n-m-1}-1$.

Доведення залежності проводиться за індукцією.

З наведених викладок можна підсумувати, що унітарні функції $Uni(m+1,\theta,i)$ вищих порядків $m+1$ у певному наборі порядку $m+1$ є добутками вибіркових функцій $Uni(m,\theta,i)$ нижчих порядків m.

Система унітарних функцій та творені за її допомогою унітарні коди є первинними в послідовності перетворень форми цифрової інформації [4].

Аналіз літературних джерел підтверджує факт відсутності інформації про перехідні базиси чи системи функцій від системи унітарних функцій до інших, а також про функціонали їх перетворень. Також не відомо аналітики здійснення перетворення унітарних кодів в інші коди. Але з теорії кодування відомо, що першим кроком до зменшення розрядності даних у два рази є перехід до кодів Лібова – Крейга [6]. З метою вирішення задачі встановлення залежності системи унітарного кодування з іншими і, зокрема, з кодуванням Лібова – Крейга як перехідного вперше введено систему дискретно-фазових функцій, що визначається як основа вказаного кодування Лібова – Крейга.

Формально система унітарних функцій порядку $m-1$ визначає свій період 2π на половині періоду π системи дискретно-фазових функцій порядку m із формальним поданням

$$Dyf(0,\theta,0)=Uni(0,\theta,0),$$
$$Dyf(m,\theta,i)=Uni(m-1,2\theta,i).$$

Дискретно-фазові функції в наборах m до порядку n подаються згідно з таким узагальненим аналітичним виразом:

$$Dyf(m,\theta,i)=sign(\sin(2^m\pi(\theta+i\cdot 2^{-n}))),$$

де $i=0,1,\ldots,2^{n-m+1}-1$ – порядковий номер функції в наборі з номером m.

Система дискретно-фазових функцій на періоді $T=2\pi$ відображає фазовий зсув $\Delta\varphi$ *sign*-процедури над функцією $\sin(2\pi)$, де $\Delta\varphi=T/N=2\pi/2^n=\pi/2^{n-1}$.

Система дискретно-фазових функцій є лінійно залежною, оскільки частина функцій системи є лінійною комбінацією інших функцій системи. Унаслідок цього така система не утворює базису. Також система дискретно-фазових функцій є неортогональною, тому що:

$$\int_0^1 Dyf(m,\theta,i)Dyf(m,\theta,j)d\theta\neq 0.$$

Одночасно дискретно-фазові функції є ортогональними в частотній ділянці, оскільки для $m\neq k$

$$\int_0^1 Dyf(m,\theta,i)Dyf(k,\theta,j)d\theta=0.$$

Дискретно-фазові функції не є ортогональними у фазовій ділянці, тому що довільна функція $Dyf(m,\theta,j)$ є результатом фазового зсуву функції $Dyf(m,\theta,i)$, де $i\neq j$, а

$$\int_0^1 Dyf(m,\theta,i)Dyf(m,\theta,j)d\theta\neq 0.$$

Функції в наборах порядків $m+1$ є результатом попарного добутку вибіркових функцій наборів порядків m згідно з такими залежностями:

$$Dyf(m,\theta,i)\cdot Dyf(m,\theta,i+2^{n-m-1})=Dyf(m+1,\theta,i), \tag{7}$$

$$Dyf(m,\theta,i+2^{n-m})\cdot Dyf(m,\theta,i+2^{n-m}+2^{n-m-1})=Dyf(m+1,\theta,i), \tag{8}$$

де $i=0,1,\ldots,2^{n-m}-1$, а також згідно із залежністю:

$$Dyf(m,\theta,i)\cdot Dyf(m,\theta,i+3\cdot 2^{n-m-1})=Dyf(m+1,\theta,i+2^{n-m-1}), \tag{9}$$

для якої $i=0,1,\ldots,2^{n-m-1}-1$.

Доведення співвідношень (7) – (9) проводиться за індукцією.

З вищенаведеного за аналогією з унітарними функціями випливає те, що множина функцій $Dyf(m+1,\theta,i)$ наборів порядку $m+1$ є визначеною процедурою добутку вибіркових функцій $Dyf(m,\theta,i)$ наборів порядку m.

Дискретно-фазові функції розглядаються як перехідні та як основа творення базисів чи систем функцій Радемахера, Ґрея, Уолша, кодування цифрових даних в яких здійснюється з меншою розрядністю порівняно з N для унітарного кодування за допомогою n-розрядних слів (де $n=\log_2 N$) [4, 6].

Для встановлення вказаних функціональних залежностей здійснимо деякі перетворення. Оскільки повна дискретно-фазова система вміщує всі складові фазового зсуву функції виду $sign(\sin(2^n\pi\theta+\Delta\varphi))$, то при $\Delta\varphi=\pi/2$ вказані функції трансформуються у функції виду $sign(\cos(2^n\pi\theta))$ [4].

Набір sin- та cos-складових системи дискретно-фазових функцій можна подати у вигляді:

$$Dyf(n,\theta,i)=\begin{cases} sign\sin(2^n\pi(\theta+\Delta\varphi)) \\ sign\cos(2^n\pi(\theta+\Delta\varphi)).\end{cases}$$

Екстракція $\sin$-складових за кожним із порядків n набору функцій утворює систему функцій Радемахера $Rad(n,\theta)$, за допомогою якої твориться звичайний двійковий код, а екстракція $\cos$-складових – відповідно систему функцій Ґрея $Gry(n,\theta)$, що є основою коду Ґрея [4, 6]:

$$Rad(n,\theta)=Dyf(n,\theta,0)=sign(\sin(2^n\pi\theta));$$

$$Gry(n,\theta)=sign(\cos(2^n\pi\theta)).$$

Взаємодоповнення двох наведених систем полягає в тому, що система функцій Радемахера вміщує набір непарних функцій $f(t)=-f(-t)$, а система функцій Ґрея вміщує парні функції $f(t)=f(-t)$. Це накладає відомі обмеження при дискретному гармонічному аналізі процесів, у спектри яких включені парні та непарні складові функції [3, 4, 5].

2. Функції Радемахера. Екстракція *sin*-складових за кожним із порядків n набору дискретно-фазових функцій утворює систему функцій Радемахера:

$$Rad(n,\theta)=Dyf(n,\theta,0)=sign(\sin(2^n\pi\theta)).$$

З означення можна твердити, що функції Радемахера є періодичними з періодом $1/2^{n-1}$ на інтервалі визначення $\theta\in[0,1)$.

Функції Радемахера приймають постійні значення на інтервалах $[i/2^n;(i+1)/2^n]$, де $i=0,1,...,2^n-1$, а в точках розриву $i/2^n$ вони неперервні справа.

Функції Радемахера ортонормовані на відрізку $[0;1)$ [7], оскільки

$$\int_0^1 Rad(n,\theta)Rad(k,\theta)d\theta=0$$

та

$$\int_0^1 Rad(n,\theta)Rad(n,\theta)d\theta=1.$$

Система функцій Радемахера утворює в просторі інтегрованих із квадратом функцій $L_2[0,1)$ неповну систему ортонормованих функцій [8], оскільки для довільного n:

$$\int_0^1 Rad(n,\theta)Rad(1,\theta)Rad(2,\theta)d\theta=0.$$

Тобто існує функція $Rad(1,\theta)Rad(2,\theta)$, тотожно не рівна нулю на $[0,1)$ та ортогональна до всіх функцій системи.

Указані функції є ортогональними в частотній ділянці, оскільки:

$$\int_0^1 Rad(n,\theta)Rad(k,\theta)d\theta=0.$$

Система функцій Радемахера ортогональна у фазовій ділянці, оскільки:

$$\int_0^1 Rad(n,\theta+\Delta\varphi)Rad(k,\theta)d\theta=0$$

та

$$\int_0^1 Rad(n,\theta+\Delta\varphi)Rad(k,\theta+\Delta\xi)d\theta=0,$$

де $\Delta\varphi\neq\Delta\xi$.

Система Радемахера хоча і є ортонормованою, та не утворює базису, тобто повної системи. Однак ця система функцій важлива тим, що за її допомогою формується система функцій Уолша.

У матеріалах статті подано основні властивості систем функцій унітарних, дискретно-фазових, Радемахера, які мають прикладне застосування при реалізації системних складових інфотехнології. Установлені аналітичні залежності між системами функцій дозволили аналітично описати та реалізувати відповідні процедури перетворення форми інформації.

1. Палагин А.В., Николайчук Я.Н. Опыт разработки микропроцессорных распределенных систем реального времени. – К.: Знание, 1988. – 19 с.
2. Романов В.А., Клочан П.С. Преобразователи формы информации для персональных ЭВМ. – К.: Знание, 1988. – 16 с.
3. Вариченко Л.В., Лабунец В.Г., Раков М.А. Абстрактные алгебраические системы и цифровая обработка сигналов. – К.: Наукова думка, 1986. – 248 с.
4. Петришин Л.Б. Теоретико-числові основи кодових систем Галуа / Івано-Франк. держ. техн. ун-т нафти і газу. – Івано-Франківськ, 1995. – 101 с. Моногр. деп. в ДНТБ України 20.12.95 №57 - Ук 96.
5. Залманзон Л.А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. – М.: Наука, 1989. – 496 с.
6. Орнатский П.П. Теоретические основы информационно-измерительной техники. – К.: Вища школа, 1983. – 455 с.
7. Ефимов А.В. Математический анализ (специальные разделы). – М.: Высшая школа, 1980. – 279 с.
8. Алексич Г. Проблемы сходимости ортогональных рядов. – М.: Инлитиздат, 1963. – 359 с.

From sole the positions of number-theoretic transformations the analysis is carried out and a set of intermediate systems of functions, that form the corresponding codes or code systems, is set. It is built the order and procedures of their creation and mutual transformations, that permitted to classify and in following to estimate efficiency of discrete harmonic analysis in the considered systems of functions.

Key words: *unitary functions, Rademacher functions, discrete harmonic analysis, code systems, analytical relations of system of functions.*

УДК 004.421.5

ББК 32.811.4

М.В. Лаврів, Л.Б. Петришин

ГЕНЕРАТОРИ РІВНОМІРНО РОЗПОДІЛЕНИХ ПСЕВДОВИПАДКОВИХ ВЕЛИЧИН

Запропоновано два нові методи генерування псевдовипадкових чисел; описано процеси генерування випадкових чисел згідно із запропонованими методами; подано порівняльну характеристику ступеня рівномірності даних методів генерування згідно із статистичними методами визначення типу розподілів – χ^2 та Колмогорова – Смірнова.

Ключові слова: *генератори випадкових чисел, метод χ^2, метод Колмогорова – Смірнова.*

Методи та засоби генерування випадкових чисел застосовують при вирішенні прикладних задачах інформатики, зокрема при статистичних дослідженнях Монте-Карло, імовірнісному моделюванні, кодуванні, перетворенні форми та цифровій обробці інформації, тестуванні, чисельному аналізі, системах прийняття рішень, комп'ютерному програмуванні, у криптографії та системах захисту. Як на недоліки методів генерування випадкових чисел слід указати на складність їх технічної реалізації, обмеження швидкодії формування відліків, неможливість відтворення отриманих характеристик розподілів, передбачення генерованих послідовностей через їх випадковий характер, що стали причиною використання на практиці математичних методів синтезу псевдовипадкових послідовностей, які реалізуються здебільшого алгоритмічно за допомогою рекурентних залежностей. При цьому кожне наступне число утворюється з визначеної кількості попередніх шляхом обчислення за деякою заданою функцією. Серед методів генерування псевдовипадкових розподілів широке застосування отримали методи з рівномірним розподілом, для яких кожен із відліків характеризується однаковою ймовірністю появи в процесі генерування.

Лінійний конгруентний метод характеризується простотою алгоритму генерування та задовільними ймовірнісними характеристиками розподілу, що зумовило його широке практичне застосування [1, 2]. Такий метод визначається вихідними параметрами: m – модуль ($m > 0$), a – множник ($0 \le a < m$), b – приріст ($0 \le b < m$), x_0 – початкове значення ($0 \le x_0 < m$). Процедура генерування здійснюється згідно із залежністю $x_{n+1} \equiv (ax_n + b) \bmod m$. Період