computing@tanet.edu.te.ua
www.computingonline.net

ISSN 1727-6209
International Journal
of Computing

АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОНАННЯ ТЕОРЕТИКО-ЧИСЛОВОГО ПЕРЕТВОРЕННЯ УОЛША НАД ПОЛЯМИ ГАЛУА

Наталія Превисокова

Кафедра інформатики, Прикарпатський національний університет імені Василя Стефаника,
м.Івано-Франківськ, вул. Шевченка, 57, natvolo@rambler.ru

Резюме: *Встановлено можливість реалізації перетворення Уолша над полями Галуа із поданням інформації та виконанням арифметичних операцій в кодах систем Галуа. Проаналізовано швидкодію пристроїв виконання арифметичних операцій перетворення Уолша-Галуа та складність їх апаратурної реалізації в двійковій системі числення та при Галуа-кодуванні.*

Ключові слова: *Перетворення Уолша, двійкове числення, кодування Галуа, час виконання арифметичних операцій, апаратурна складність.*

При реалізації системних функцій інфотехнологій застосовуються методи перетворення форми та цифрової обробки інформації з використанням дискретних перетворень. Необхідність обробки та передачі інформації в реальному часі зумовлює актуальність розроблення та створення ефективних систем обробки та передачі повідомлень. Апаратом реалізації процедур цифрової обробки інформації є перетворення, а саме, перетворення Фур'є, Уолша, Хаара, теоретико-числові та ін. Дискретні ортогональні перетворення використовуються для кодування, обробки, зменшення надлишковості інформації, зокрема, при обробці зображень, системах зв'язку, спектроскопії, радіолокації.

Дискретні перетворення визначені та реалізуються над полями комплексних чисел [1 - 6] та над скінченними полями [1, 2]. На сьогоднішній день серед теоретико-числових перетворень над скінченними полями Галуа використовуються перетворення Фур'є-Галуа. У випадку реалізації перетворень в базисі функцій Уолша знижуються вимоги щодо порядку поля Галуа та простіше здійснюється перетворення значень спектральних коефіцієнтів із поля Галуа в поле комплексних чисел [1], проте не було розроблено методи виконання теоретико-числового перетворення Уолша над полем Галуа та встановлено ефективності їх застосування, що зумовило актуальність досліджень у вказаному напрямку.

Дискретне перетворення Уолша виконується над скінченною послідовністю відліків інфопотоку і є методом обчислення спектральних коефіцієнтів, що визначають такі характеристики послідовності, як енергетичний та фазовий спектри.

Згідно класифікації Фур'є-подібних перетворень [2] над полем комплексних чисел визначене дискретне перетворення Уолша, а над полем Галуа $GF(p^m)$ − дискретне перетворення Уолша-Галуа.

Швидкодія засобів цифрової обробки інформації залежить від методу обробки, формування, перетворення, схемотехнічної реалізації та форми подання інформації. Для подання чисел в цифрових системах найчастіше використовується двійкова система числення [3, 4, 5, 6], зокрема, при реалізації відомих методів перетворення Уолша над полями Галуа [1, 2]. Проте, час виконання арифметичних операцій в двійковій системі залежить від розрядності внаслідок формування та поширення міжрозрядних переносів.

Аналіз результатів розробки сучасних методів ефективних обчислень вказав на можливість існування альтернативних методів кодування. В роботі [7] розроблено метод виконання арифметичних операцій додавання, віднімання та перемноження в полях Галуа, що ґрунтується на паралельній обробці операндів, поданих в кодах систем Галуа, та встановлено, що реалізація арифметичних операцій над кодами в полі Галуа позбавлена недоліків двійкової арифметики.

Результати проведених досліджень вказали на можливість використання даного методу при реалізації теоретико-числових перетворень. Основним завданням дослідження є встановлення можливості та обґрунтування ефективності застосування кодування Галуа для подання інформації при реалізації теоретико-числового перетворення Уолша над полями Галуа. Результатом застосування перетворення є збільшення швидкості цифрової обробки повідомлень.

Перетворення Уолша-Галуа послідовності $\{x(i)\}=\{x(0),x(1),...,x(N-1)\}$ подається у матричному записі згідно співвідношення [1]:

$$S(n)=W(n)x(n), \qquad (1)$$

де $i=0,1,\ldots,N-1$, $S(n)=[S(0),S(1),...$ $...,S(N-1)]$ – вектор спектральних коефіцієнтів перетворення Уолша-Галуа розмірністю $N=2^n$, $n=1,2,\ldots$, $W(n)$ – матриця $N\times N$ дискретних значень функцій Уолша над полем Галуа, $x(n)$ – транспонований вектор $[x(0),x(1),...,x(N-1)]^T$.

Матриця $W(n)$ ортогональна і симетрична, тому обернене перетворення Уолша записується у наступному вигляді:

$$x(n)=\frac{1}{N}W(n)S(n). \qquad (2)$$

Для того, щоб існувала однозначна відповідність між значеннями спектру в полі комплексних чисел і в полі Галуа необхідно, щоб порядок $q=p^m$ поля Галуа $GF(q)$, де p - просте, m – додатне ціле, над яким визначено перетворення Уолша-Галуа і спектр $S(n)$, одержаний в результаті цього перетворення, був не менший потужності $P(S(i))$, множини значень коефіцієнтів Уолша $S(i)$, визначеної над полем комплексних чисел при такому значенні i, для якого $P(S(i))$ максимальна [1], тобто

$$q \geq P(S(i)).$$

Якщо $N=p^r$, де p – просте число, то $P(S(i))=[(k-1)p^{r-1}]^p-[(k-1)p^{r-1}-1]^p$, де k – число рівнів квантування $x(i)$ [1].

Перетворення Уолша над полями Галуа як і над полем комплексних чисел обчислюється за швидкими алгоритмами перетворення, які вимагають виконання меншої кількості арифметичних операцій, а саме $N\log_2 N$ додавань та $\frac{N}{2}\log_2 N$ перемножень на відміну від $N(N-1)$ додавань та $\frac{N}{2}(N-1)$ перемножень при безпосередньому обчисленні згідно виразу (1) [1, 4].

Швидкий алгоритм перетворення Уолша-Галуа (ШПУГ) над розширеним полем Галуа $GF(2^m)$ складається із $n=\log_2 N$ етапів. Допоміжні значення $x_k(i)$ на кожному проміжному етапі визначаються співвідношенням

$$x_k(i)=ax_{k-1}(i)+x_{k-1}(i+bl), \qquad (2)$$

де $k=1,2,...,\log_2 N$ – номер етапу алгоритму перетворення; $N=2^n$ – кількість спектральних коефіцієнтів; $a=(-1)^{[i/l]} mod(2^m-1)$, $b=(-1)^{[i/l]}$; де $[i/l]$ – позначення цілої частини числа i/l, $l=2^{k-1}$.

Граф алгоритму швидкого перетворення Уолша-Галуа для випадку $N=8$ наведено на рис.1, де $\{x(i)\}=\{x(0),x(1),...,x(7)\}$ – значення вхідної послідовності, $S(n)$ – вектор коефіцієнтів перетворення Уолша-Галуа розмірністю $N=2^3$.

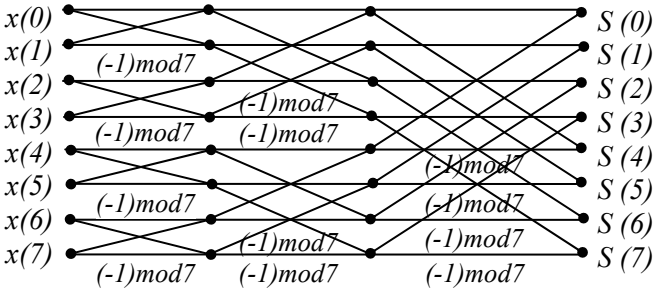

Рис. 1 – Граф алгоритму швидкого перетворення Уолша для *N=8*.

Арифметичні дії, які складають базову операцію, на кожному етапі перетворення можна подати як

$$x_k(i)=x_{k-1}(i)+x_{k-1}(j); \qquad (3)$$

$$x_k(j)=x_{k-1}(i)+[(-1)\,mod(2^m-1)]x_{k-1}(j). \qquad (4)$$

Граф алгоритму виконання однієї базової операції подано на рис.2.

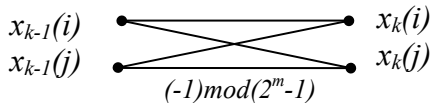

Рис. 2 – Граф алгоритму базової операції.

Загальна кількість базових операцій, необхідна для реалізації алгоритму, становить

$$\frac{N}{2} log_2 N .$$

Для оцінки величини зменшення часу обчислень проаналізуємо особливості виконання арифметичних модульних операцій у двійковій системі.

Основним методом реалізації модульних операцій є введення додаткових переносів між розрядами суматора з метою досягнення заданої величини модуля М, відмінної від величини модуля суматора без додаткових переносів, яка становить 2^m, де m – число розрядів суматора [1]. При виборі в якості модуля значень $2^m - 1$ необхідний лише один перенос зі старшого значущого розряду в молодший, оскільки перенос означає одержання числа 2^m, що дорівнює $1 mod(2^m - 1)$. При реалізації операції додавання за модулем $2^m - 1$ перенос зі старшого значущого розряду додається до молодшого. Таким чином, час додавання в суматорі за модулем $2^m - 1$ визначається із [1]

$$T_{д.с.mod} = 2T_{д.с.} + T_n , \qquad (5)$$

де $T_{д.с.}$ – час додавання у двійковому суматорі, T_n – затримка схеми генерації переносу зі старшого значущого розряду в молодший.

Паралельний суматор з паралельними переносами складається із двох частин: схеми додавання та схеми формування прискорених переносів [8, 9]. Схема додавання містить m спрощених однорозрядних суматорів на три входи та один вихід суми. Час додавання в двійковому суматорі з паралельними переносами обчислюється за формулою [8, 9]

$$T_{д.с.} = t_г + t_П + t_s = 5t_p , \qquad (6)$$

де враховані затримки при виробленні сигналів генерації $t_г = t_p$, переносу $t_П = 2t_p$ та сумування в найстаршому розряді $t_s = 2t_p$, де t_p – середня затримка поширення сигналу типовим логічним елементом. При $m > 8$ використовуються суматори групової структури з послідовними або паралельними переносами між групами [9]. В суматорах групової структури схема з розрядністю m поділяється на k груп по l розрядів, переноси між групами формуються за допомогою схем прискореного переносу. Час додавання в суматорі з паралельними переносами в групах та між групами визначається затримками формування сигналів генерації в групах $t_G = 3t_p$, затримкою в схемах прискореного переносу між групами t_c та часом сумування в останньому розряді старшої групи t_s [8]:

$$T_{д.с.} = t_G + t_c + t_s . \qquad (7)$$

В залежності від розрядності m суматора групової структури затримка в схемах прискореного переносу між групами становить $t_c = 2t_p$ для $m = 32$ або $t_c = 4t_p$ для $m = 64$, $T_n = 2t_p$. Із врахуванням співвідношень (5) та (6), час виконання операції додавання за модулем $2^m - 1$ становить

$$T_{д.с.mod} = 2T_{д.с.} + T_n = 12t_p .$$

Згідно співвідношень (5) та (7) $T_{д.с.mod} = 16t_p$ для $m = 32$, $T_{д.с.mod} = 20t_p$ для $m = 64$.

Порівняно із звичайним перемножувачем двійкових чисел, модульний перемножувач містить додатковий суматор для реалізації циклічного переносу і зведення добутку за модулем $2^m - 1$. Час виконання перемноження в такому перемножувачі визначається величиною

$$T_{д.м.mod} = T_{д.м.} + T_{д.с.} + T_n ,$$

де $T_{д.м.}$ – час виконання операції перемноження двох чисел без приведення результату за модулем, що визначається сумою затримок сигналів в кон'юнкторах t_p та затримки в найдовшому ланцюжку матриці m^2 однорозрядних суматорів [9]:

$$T_{д.м.} = t_p + (2m - 1)t_s = t_p + (2m - 1) \cdot 2t_p .$$

Алгоритм швидкого перетворення Уолша-Галуа полягає у послідовному виконанні $\frac{N}{2} log_2 N$ базових операцій (3) та (4).

При паралельному виконанні додавання та перемноження згідно виразів (3) та (4) відповідно тривалість базової операції в двійковій системі становить

$$T_{д.б.} = T_{д.с.mod} + T_{д.м.mod}.$$

Базова операція (3), (4) реалізується комплексним арифметичним пристроєм, у якому здійснюється перемноження на коефіцієнт $[(-1) mod(2^m - 1)]$ згідно виразу (4) та додавання пар чисел у співвідношеннях (3) та (4).

Критерієм апаратурної складності A пристрою є ціна за Квайном – сумарне число входів всіх логічних елементів схеми. Апаратурна складність арифметичних пристроїв [1, 8, 9] реалізації швидкого перетворення Уолша-Галуа при використанні двійкової системи визначається складністю модульного суматора $A_{д.с.mod}$, модульного перемножувача $A_{д.м.mod}$ та логічної схеми генерації переносу із старшого значущого розряду в молодший A_n:

$$A_{д.ШПУГ} = A_{д.с.mod} + A_n + A_{д.м.mod}.$$

Специфіка рекурсивного упорядкування методу кодування Галуа передбачає реалізацію арифметичних операцій (3), (4) перетворення на основі матриці програмованих логічних елементів (ПЛМ). Замість m-розрядного двійкового суматора використовується суматор на основі ПЛМ розмірністю $(2^m - 1) \times m^2$, m^2 двовходових логічних елементів "І" та m - входових суматорів за модулем два.

Час виконання операції додавання складається із часу доступу до елементів ПЛМ $t_{дост.}$, часу затримки поширення сигналу одним логічним елементом "І"– t_p та часу додавання в суматорах за модулем два t_p:

$$T_{G.c.} = t_{дост.} + t_p + t_c = 4t_p.$$

де t_p – усереднене значення затримки поширення сигналу одним типовим логічним елементом.

Згідно виразу (4) для виконання базової операції швидкого перетворення Уолша-Галуа необхідно здійснити одну операцію перемноження на константу. Реалізація даної операції потребує використання матриці програмованих логічних елементів розмірністю $(2^m - 1) \times m$.

Час виконання перемноження при реалізації швидкого перетворення Уолша-Галуа визначається часом доступу до елементів ПЛМ

$$T_{G.м.} = t_{дост.} = 2t_p.$$

Часом $T_{G.м.}$ при реалізації алгоритму перетворення можна знехтувати, оскільки операція перемноження у базовій операції (3), (4) виконується одночасно із додаванням згідно виразу (3). Таким чином, час виконання базової операції (3), (4) в кодових системах Галуа становить

$$T_{G.б.} = T_{G.c.} + T_{G.c.} = 2T_{G.c.}$$

Апаратурна складність арифметичних пристроїв реалізації [10] швидкого перетворення Уолша-Галуа при використанні Галуа-кодування визначається як сумарна складність суматора та перемножувача згідно виразу:

$$A_{G.} = A_{G.c.} + A_{G.м.},$$

де $A_{G.c.}$ та $A_{G.м.}$- апаратурна складність суматора та перемножувача в кодових системах Галуа відповідно.

Повний час, який витрачається на виконання арифметичних операцій при реалізації ШПУГ послідовностей довжини $N = 2^n$ у двійковому численні та у кодових системах Галуа визначається часом виконання $\frac{N}{2} log_2 N$ базових операцій:

$$T_{д.с.} = T_{д.б.} \frac{N}{2} log_2 N =$$

$$= (T_{д.с.mod} + T_{д.м.mod}) \frac{N}{2} log_2 N;$$

$$T_G = T_{G.б.} \frac{N}{2} log_2 N = 2T_{G.c.} \frac{N}{2} log_2 N =$$

$$= T_{G.c.} N log_2 N.$$

Для оцінки можливого скорочення часу виконання обчислень для виконання швидкого перетворення Уолша-Галуа при застосуванні запропонованого методу кодування Галуа проведено розрахунки часу виконання арифметичних операцій [8, 9, 11]. Оскільки для розрядностей $m = 3...8$ перевагу за швидкодією мають двійкові паралельні суматори з паралельними переносами [8, 9], то аналіз

проведено за умови використання двійкових паралельних суматорів з паралельними переносами для розрядностей $m = 4$ і $m = 8$, суматорів групової структури з паралельними переносами між групами для розрядностей $m \geq 16$ та матричних перемножувачів із середньою затримкою поширення сигналу одним типовим логічним елементом t_p, нс.

У таблиці 1 наведено значення, а на рис. 3 – залежності часу виконання арифметичних операції від розрядності ШПУГ в кодових системах Галуа T_G та в двійковій системі $T_{д.с.}$ для різних значень довжини послідовності $N = 2^n$:

Таблиця 1. Час виконання арифметичних операцій в кодових системах Галуа та в двійковій системі, нс

n	$T_{д.с.}$	T_G
4	$1088\,t_p$	$256\,t_p$
8	$51200\,t_p$	$8192\,t_p$
16	$46137344\,t_p$	$4194304\,t_p$
32	$1{,}08577E{+}13\,t_p$	$5{,}49756E{+}11\,t_p$
64	$1{,}68825E{+}23\,t_p$	$4{,}72237E{+}21\,t_p$

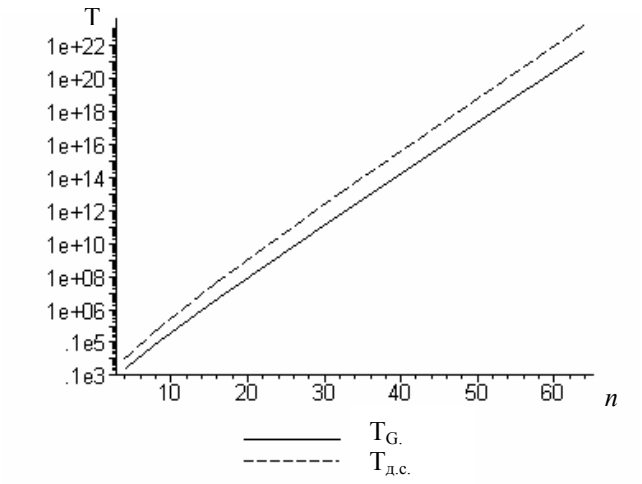

Рис. 3 – Залежності часу виконання арифметичних операцій від розрядності в кодових системах Галуа та в двійковій системі.

Із таблиці 1 можна підсумувати, що для довжин послідовностей від $N = 4$ до $N = 2^{64}$ виконання арифметичних операцій додавання та перемноження при реалізації перетворення Уолша із застосуванням методу кодування Галуа потребує у $k_T = \dfrac{T_{д.с.}}{T_G}$ разів менше часу, ніж у двійковому численні. В таблиці 2 наведено значення коефіцієнта прискорення k_T для значень розрядності n:

Таблиця 2. Коефіцієнт прискорення виконання арифметичних операцій в кодових системах Галуа та в двійковій системі

n	4	8	16	32	64
k_T	4,3	6,3	11,0	19,8	35,8

Здійснено оцінки ефективності апаратурної реалізації арифметичних пристроїв за критерієм $A \cdot T$ [9] при використані двійкового числення $A_{д.с.}T_{д.с.}$ та кодування Галуа $A_G T_G$. Результати порівняння таких пристроїв за даним критерієм і залежності від їх розрядності наведено в таблиці 3 та на рис. 4 відповідно.

Таблиця 3. Значення оцінок ефективності апаратурної реалізації арифметичних пристроїв за критерієм AT

n	$A_{д.с.}T_{д.с.}$	$A_G T_G$
4	624 512	52 736
8	107 008 000	39 305 216
16	3,41416E+11	9,34906E+12
32	3,05665E+17	1,55838E+23
64	1,84876E+28	1,13246E+43

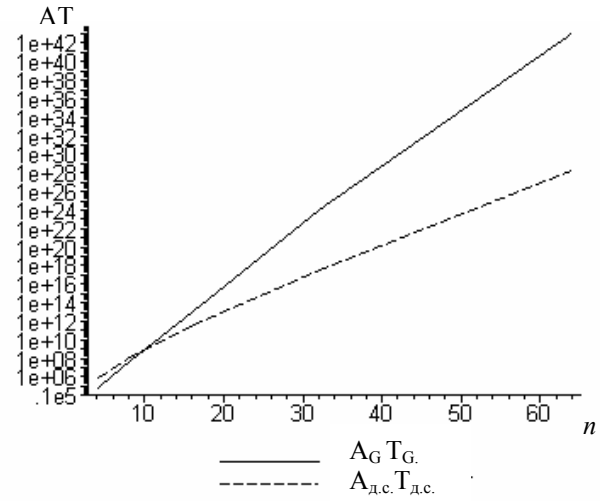

Рис.4 – Залежності оцінок ефективності апаратурної реалізації арифметичних пристроїв за критерієм AT від розрядності.

Здійснено порівняння обчислювальних пристроїв за методами виконання перетворення Уолша-Галуа із поданням інформації у двійковій

системі та із використанням Галуа-кодування за наступними основними показниками: часом виконання арифметичних операцій (кількість арифметичних операцій для обох схем однакова) та за критерієм АТ, де А – апаратурна складність пристрою, Т – час розв'язання задачі.

Аналіз одержаних результатів за критерієм АТ дозволив визначити для значень розрядностей $m < 16$ перевагу використання кодування Галуа, а для розрядностей $m \geq 16$ перевагу двійкового числення.

Для прискорення виконання ШПУГ методами паралельної обробки використовуються структури, що містять декілька паралельно діючих арифметичних пристроїв [3, 10]. Зокрема, час виконання ШПУГ у системі, що містить $N/2$ паралельно працюючих арифметичних пристроїв

$$T_{д.с.} = T_{д.б.} \log_2 N;$$
$$T_G = T_{G.б.} \log_2 N.$$

Отже, застосування кодів Галуа в таких системах призводить до зменшення часу виконання перетворення на величину

$$\Delta T = T_{д.с.} - T_G = (T_{д.б.} - T_{G.б.}) \log_2 N.$$

Таким чином, встановлено можливість реалізації ШПУГ із поданням інформації та виконанням арифметичних операцій в кодових системах Галуа. Проаналізовано швидкодію пристроїв виконання арифметичних операцій перетворення Уолша-Галуа та складність їх апаратурної реалізації в двійковій системі числення та при Галуа-кодуванні.

Встановлено, що при реалізації перетворення Уолша-Галуа в кодових системах Галуа, апаратурна складність арифметичних пристроїв схеми виконання перетворення для окремих значень розрядностей є більшою, водночас, час виконання арифметичних операцій для всіх розрядностей і, відповідно, час виконання перетворення менший, ніж при використанні двійкової системи числення.

Проведені дослідження доводять ефективність за показником часу застосування Галуа-кодування для виконання теоретико-числового перетворення Уолша над полями Галуа.

ЛІТЕРАТУРА

[1] Вариченко Л.В., Лабунец В.Г., Раков М.А. *Абстрактные алгебраические системы и цифровая обработка сигналов*. – Киев: Наук. Думка, 1986. – 248 с.

[2] Муттер В.М. *Основы помехоустойчивой телепередачи информации*. – М.: Энергоатомиздат, 1990. – 288 с.

[3] Рабинер Л. Р., Гоулд Б. Г. *Теория и применение цифровой обработки сигналов*. – М.: Мир, 1978. – 848 с.

[4] Залманзон Л. А. *Преобразования Фурье, Уолша, Хаара и их применение в управлении связи и других областях*. – М.: Наука. гл. ред. физ.-мат. лит., 1989. – 496 с.

[5] Бондарев В. Н., Трестер Г., Чернега В.С. *Цифровая обрабока сигналов: методы и средства*: Учебн. Пос.– Изд. 2-е. –Х.:Конус, 2001.–398 с.

[6] S. Kuo. *Real-time digital signal processing: implementations, applications and experiments with the TMS320C55X*. John Wiley&Sons LTD, West Sussex PO19 8SQ, England, 2006.

[7] Петришин Л. Б. *Теоретичні основи перетворення форми та цифрової обробки інформації в базисі Галуа*: Навчальний посібник. – К.: ІзіМН МОУ, 1997. – 237 с.

[8] Бабич Н.П., Жуков И.А. *Компьютерная схемотехника. Методы построения и проектирования*: Учебное пособие. – К.: МК-Пресс, 2004.– 576 с.

[9] Угрюмов Е.П. *Цифровая схемотехника*: Учеб. пособие для вузов. – СПб.: БХВ-Петербург, 2004. – 800 с.

[10] [10] Ракошиц В.С., Козлов А.В., Можаев И.А., Беляев А.А. Специализированные микропроцессоры, реализующие быстрые преобразования // *Цифровая обработка сигналов и ее применения*. – М., Наука, 1981. – 221 с.

[11] R.Tocci, N.Widmer. *Digital Systems.Principles and Applications.* Prentice Hall, New Jersey Columbus, 2001.

***Превисокова Наталія Володимирівна**, 1978 року народження. Закінчила Прикарпатський університет імені Василя Стефаника у 2000 році за спеціальністю "Математика". З 2005 року працює на посаді асистента, кафедри інформатики Прикарпатського національного університету ім. В.Стефаника.*

ANALYSIS OF EFFICIENCY THE NUMBER-THEORETIC WALSH TRANSFORM REALIZATION ABOVE THE GALOIS FIELD

Natalia Prevysokova

Prevysokova Natalija, Precarpathian National University,
Shevchenka st. 57, Ivano-Frankivsk, Ukraine, 76025, e-mail: natvolo@rambler.ru

Resume: *It is set possibility machine realization the Walsh transform above the Galois fields with presentation of information and implementation arithmetic operations in the Galois code systems. The speed of devices of implementation of arithmetic operations for the Walsh - Galois transformation is analysed. It is set and analyzed complication of it's apparatus realization in the binary system and in the Galois -code.*

The methods of transformation of form and digital processing of information with the use of discrete transforms are used in realization of system functions of information technologies. The necessity of processing and information transmission in the real time predetermines actuality of development and creation of the effective systems of processing and message transmission. Transforms are the vehicle of realization of procedures of information digital processing, namely, the Fourier, Walsh, Haar transform, number-theoretic and other discrete orthogonal transforms are used for the coding, processing, reduce amounts of information, in particular, at the image processing, communication networks, spectroscopy, radio-location.

The known results of researches the discrete Fourier and Walsh transforms are analyzed in the field of complex numbers [1-6] and in the finite field [1, 2]. The discrete Walsh transform is performed with the finite sequence of selected performance information flows and it is the method of calculation of spectral coefficients which determine such descriptions of sequence, as power and phase spectrums.

In order to classification of Fourier-similar transforms [2] the discrete Walsh transform is defined above the field of complex numbers and the discrete Walsh-Galouis transform is defined above the Galois field $GF(p^m)$.

For representation of information in case of realization Walsh-Galois transform it is suggested to use the code systems Galois's [7], what allows to avoid the defects of dynamics of implementation of arithmetic operations in the binary system.

The main task of research is establishment of possibility and ground efficiency of application of Galois coding for presentation of information during realization of the number-theoretic Walsh transform above the Galois fields. The increase of speed of digital information processing is the result of application of transform.

The Walsh-Galois transform is a sequence of finite length N. It obtained from a sequence of input data and it is given in a matrix form by equation (1). The terms of choice of order q of the Galois field $GF(q)$ are resulted for existence of synonymous accordance between the values of spectrum in the field of complex numbers and in the Galois field [1].

The Walsh-Galois transform above the Galois fields as well as above the field of complex numbers is calculated with application fast algorithms Walsh-Galois transform (FWGT), which require implementation of less of arithmetic operations. The flow graphs of algorithm of fast Walsh transform computation for length of the input sequence N=8 is plotted on Figure 1. The flow graph of base operation of an algorithm is shown in Figure 2. The common amount of base operations, necessary for realization of algorithm, makes $\frac{N}{2} log_2 N$.

For estimation of time shortening of calculations it is analysed the features of implementation of arithmetic module operations in the binary system. The basic method of realization of module operations is put into the units additional transfers between the bits of adder with the purpose of achievement of the set size of the module of M, different from the size of the module of adder without the additional transfers, which makes 2^m, where m is a number of bits of adder [1]. Time of addition in adder by the module $2^m - 1$ [1] is determined from expression (5) as a two time of addition in binary system and a time delay in scheme of carry unit.

Time of implementation of operation of addition is analyzed in a binary adder with the parallel transfers, which depending on a scheme is calculated by formulas (6), (7) [8, 9]. Time of implementation

of operation of addition on the module $2^m - 1$ is determined taking into account equations (5), (6), (7).

It is comparative with ordinary multiplier binary numbers, module multiplier contains one more adder for realization of cyclic carry and report of result by the module $2^m - 1$. Time of implementation of multiplying in such unit is determined by times of binary multiplication, binary addition and a time delay in scheme of carry unit.

There is a total number of inputs of all logical gates in scheme by the criterion of apparatus complication A to the device. Apparatus complication of arithmetic units [1, 8, 9] of realization of the fast Walsh-Galois transform at the use of the binary system $A_{д.ШПУГ}$ is determined by complication of module adder $A_{д.с.mod}$, module multiplier $A_{д.м.mod}$ and logical scheme of generation of carry from a meaningful significant bits most in junior one A_n.

Specific of recursion organization of method of Galois code foresees realization of arithmetic operations (3), (4) transformation on the basis of matrix of programmable logical gates. Time of implementation of operations of addition, multiplication by the constant and base operation of the fast Walsh-Galois transform is analyzed in the Galois's codes systems.

Apparatus complication of arithmetic units of realization [10] of the `fast Walsh-Galois transform` in the Galois codes use $A_{G.}$ is determined as total complication of adder and `multiplier`.

Timing realization of arithmetic operations [8, 9, 11] are executed for estimation reduction of time of performance of calculations fast Walsh-Galois transform and application of the offered method Galois coding. The analysis is carried out subject to the condition the use of parallel adders. Time of implementation arithmetic operations in the code systems Galois's T_G and in the binary system $T_{д.с.}$ is given in Table 1. Corresponding functional dependences of length of input sequence $N = 2^n$ are represented on a Figure 3.

It is possible to do a conclusion from the Table 1, that for lengths of sequences from $N = 4$ to $N = 2^{64}$ implementation of arithmetic operations of addition and multiplying at realization of the Walsh-Galois transform with application of Galois coding method requires in k_T one times less time, than with the binary system. The values of coefficient of acceleration of implementation arithmetic operations and the values of bit n are given in the Table 2.

Estimations of efficiency of apparatus realization of arithmetic units are done by a criterion $A \cdot T$ [9] at used binary system $A_{д.с.}T_{д.с.}$ and Galois code $A_G T_G$. Value of estimations of efficiency of apparatus realization of arithmetic units by the criterion AT are given in a Table 3. Dependences of estimations of efficiency of apparatus realization of arithmetic units by the criterion AT of a bit are plotted on a Figure4.

Comparison of computing devices is done by the methods of implementation of the Walsh-Galois transform with representation of information in the binary system and in the Galois code use by the following basic criterions: time of arithmetic operations implementation and by the criterion of AT, where A is apparatus complication of devices, T is time of decision of task. The analysis of the got results by AT criterion allowed to define for the values of adder bits $m < 16$ advantage of the use of Galois code and for adder bits $m \geq 16$ advantage of binary system.

Thus, possibility of computation fast Walsh-Galois transform is set with presentation of information and implementation of arithmetic operations in the Galois's code systems. The rapid-acting of devices of implementation of arithmetic operations of Walsh-Galois transform and complication of their apparatus realization in the binary scale of notation and in Galois code are analysed.

It is set that apparatus complication of arithmetic units of scheme of transformation for the some values of adder bits the realization of Walsh-Galois transform in the Galois's code systems is anymore, but the time of implementation of arithmetic operations for all adder bits and time of implementation of transformation is less, than at the use of binary system.

These researches prove to efficiency of the Galois coding application for implementation of the number-theoretic Walsh transform above the Galois fields by time criterion.