5. *Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В.* Математические и компьютерные основы криптологии. Учебное пособие. – М.: Новое издание, 2003. – 272 с.

6. *Земор Ж.* Курс криптографии. – Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2006. – 256 с.

7. *Рябко Б.Я., Фионов А.Н.* Криптографические методы защиты информации: Учебное пособие. – 2005.

8. *Фомичев В.М.* Дискретная математика и криптология. Курс лекций / Под общ. ред. д-ра физ.-мат. н. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.

9. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

10. *Кац М.* Статистическая независимость в теории вероятностей, анализе и теории чисел. – М.: Издательство иностранной литературы, 1963. – 156 с.

В статті розглядається частотне тестування криптографічних генераторів псевдовипадкових послідовностей.
Ключові слова: псевдовипадкові числа, генератор, алгоритм.

В статье рассматривается частотное тестирование криптографических генераторов псевдослучайных последовательностей.
Ключевые слова: псевдослучайные числа, генератор, алгоритм.

The article is devoted to the frequency of testing cryptographic pseudorandom sequence generators.
Key words: Pseudorandom number, generator, algorithm.

Поступила 16.06.2010

УДК 681.3.06

д.т.н., проф. Дудикевич В.Б. (НУ «Львівська політехніка»),
д.т.н., проф. Кузнєцов О.О. (СНС Харківського УПС),
Томашевський Б.П. (НЦ СВ академії СВ)

МЕТОД НЕДВІЙКОВОГО РІВНОВАГОВОГО КОДУВАННЯ

Постановка проблеми в загальному вигляді і аналіз літератури

Обчислювальна ефективність виконання арифметичних операцій безпосередньо залежить від способу представлення чисел, над якими виконуються операції, тобто від застосованої системи відліку [1-4]. Найбільш поширеною є позиційна система числення, в якій один і той же числовий знак (цифра) в запису числа має різні значення, в залежності від розряду, де він розташований [1, 2]. До числа таких систем належить сучасна десяткова система числення, виникнення якої пов'язано з рахунком на пальцях, двійкова система числення, що використовується в сучасних обчислювальних машинах та ін.

Змішана система числення є узагальненням позиційної системи; її основою є зростаюча послідовність чисел і кожне представлене число виражається через лінійну комбінацію елементів основи [1, 2]. До змішаних відносять систему числення Фібоначчі, факторіальну, біноміальну та ін. системи [1 - 4].

Слід зазначити, що на системі біноміального числення засновано безліч прикладних програм, в тому числі т.зв. біноміальні коди, які належать до класу нелінійних двійкових надлишкових кодів, що використовуються для підвищення завадостійкості двійкових асиметричних каналів передачі даних [3, 4]. Головна властивість біноміальних кодів, що складається в рівній вазі Хеммінга (числі ненульових елементів) всіх кодових слів, використовується для ефективного виявлення асиметричних похибок передаваних послідовностей. У цьому випадку зміна ваги Хеммінга послідовності є адекватним критерієм виявлення помилки в двійкових асиметричних каналах передачі даних.

Інше, не менш важливе, вживання рівноважних кодів полягає в побудові доказово стійких шифросистем, безпека яких обґрунтовується зведенням завдання обчислення секретного ключа до рішення теоретико-складної задачі синдромного декодування [5-8]. Так, наприклад, у роботах [7, 8] розглядаються шифросистеми доказової стійкості, в яких сеавсовими ключами виступають рівновагові кодові послідовності. У роботі [8] показано, що найбільшу ефективність дає використання довгих недвійкових кодів, що передбачає формування недвійкових рівновагових послідовностей. У той же час, проведений аналіз [1-4] показав, що розроблена на сьогоднішній день теорія і вживані методи біноміального рахунку дозволяють реалізувати рівновагове кодування лише двійковими послідовностями і не передбачають формування недвійкових рівновагових кодів. Це обумовлює актуальність даної статті, метою якої є розробка методу недвійкового рівновагового кодування на основі узагальненого біноміально-позіційного представлення. Запропонований метод дозволяє узагальнити відомий підхід до недвійкового випадку і практично реалізувати обчислювальні алгоритми формування недвійкових послідовностей фіксованої ваги.

Позиційні і змішані системи числення. Метод і алгоритм двійкового рівновагового кодування

Позиційна система числення базується на позиційній нумерації, тобто, на місцевому значенні цифр і визначається деяким числом $b > 1$ (основа системи числення) таким, що b одиниці в кожному розряді об'єднуються в одну одиницю наступного за старшинством розрядом. Система числення з основою b також називається b - їчною позиційною системою[1,2].

Число x в b - їчній позиційній системі числення подається у вигляді лінійної комбінації ступенів числа b:

$$x = \sum_{i=0}^{n-1} a_i b^i$$

де a_i – це цілі числа, які називаються цифрами, що задовольняють нерівність

$$0 \le a_i < b,$$

i - порядковий номер розряду, починаючи з нульового, n - число розрядів (довжина) позиційного коду.

Кожний ступінь b^i в такому записі називається розрядом, старшинство розрядів і відповідних їм цифр визначається значенням показника i. Зазвичай для ненульового числа x потрібно, щоб старша цифра a_{n-1} в b -їчному визначенні x була також ненульовою.

Якщо не виникає суперечностей (наприклад, коли всі цифри визначаються у вигляді унікальних письмових знаків), число записують у вигляді послідовності його b – їчних цифр, вирахуваних за зростанням старшинства розрядів зліва направо:

$$x=(a_0\ a_1\ \ldots\ a_{n-1})$$

Змішана система числення є узагальненням b - їчної системи і також, як правило, належить до позиційних систем числення. Основою змішаної системи є зростаюча послідовність чисел

$$b_0, b_1, b_2, \ldots$$

і кожне число визначається як лінійна комбінація:

$$x = \sum_{i=0}^{n-1} a_i b_i ,$$

де на коефіцієнти a_i накладаються деякі кодові обмеження.

Записом числа x в змішаній системі числення називається перерахунок його цифр в порядку зменшення індексу i починаючи з першого ненульового. Якщо b_i - b^l для деякого b^l, то змішана система числення співпадає з b - їчною позиційною системою числення.

Біноміальна система числення заснована на визначенні чисел через зростаючу послідовність біноміальних коефіцієнтів

$$b_0 = \binom{u_1}{1}, b_1 = \binom{u_2}{2}, \ldots, b_{n-1} = \binom{u_n}{n},$$

$$b_i = \binom{u_{i+1}}{i+1} = \frac{u_{i+1}!}{(i+1)!\cdot(u_{i+1}-i-1)!}, \; 0 \le u_1 < u_2 < \ldots < u_n = \frac{n!}{w!\cdot(n-w)!},$$

де w - число ненульових елементів біноміального коду.

Число x в біноміальній системі визначається як лінійна комбінація:

$$x = \sum_{i=0}^{n-1} a_i b_i = \sum_{i=0}^{n-1} a_i \binom{u_{i+1}}{i+1},$$

де коефіцієнти $a_i \in \{0,1\}$

У випадку, коли не виникає розбіжностей у розрахунку біноміальних коефіцієнтів

$$b_i = \binom{u_{i+1}}{i+1}$$

тобто, коли задане правило формування набору чисел $0 \le u_1 < u_2 < \ldots < u_n$,

число x записують за зростанням старшинства розрядів a_i зліва направо:

$x = (a_0 \quad a_1 \quad \ldots \quad a_{n-1})$.

Розглянута біноміальна система числення використовується для побудови *двійкових рівноваговш кодів,* вона складається з множини двійкових послідовностей з фіксованим числом ненульових елементів в кожній послідовності (фіксованою вагою Хеммінга).

Введемо таке позначення: n - довжина рівновагового коду, тобто число елементів (розрядів) кодових послідовностей (кодових слів); $C = \{C_0, C_1, \ldots, C_{M-1}\}$

- множина кодових слів рівно вагового коду, де

$$C_j = (C_{j_0} \quad C_{j_1} \quad \ldots \quad C_{j_{n-1}}) \in C, \; C_{j_i} \in \{0,1\}, \; j = 0,1,\ldots,M-1, \; i = 0,1,\ldots,n-1,$$

при чому для всіх векторів $C_j, j = 0,1,\ldots,M-1$ маємо рівність ваги Хеммінга:

$$\forall j: w(C_j) = const = w$$

де

$$w(C_{j_0} \quad C_{j_1} \quad \ldots \quad C_{j_{n-1}}) = \#(C_{j_0} \quad C_{j_1} \quad \ldots \quad C_{j_{n-1}})_{(C_{j_i} \neq 0)},$$

$\#(C_{j_0} \quad C_{j_1} \quad \ldots \quad C_{j_{n-1}})_{(C_{j_i} \neq 0)}$ - число таких C_{j_i}, $i = 0,1,\ldots,n-1$, що $C_{j_i} \neq 0$.

Потужність рівноважного коду (число елементів множини С) визначається числом двійкових векторів довжини n і ваги w:

$$|C| = M = \frac{n!}{w!(n-w)!}.$$

Відомий метод біноміального (двійкового рівновагового) кодування [3,4] оснований на представленні інформаційних даних у вигляді числового еквівалента (позначимо його символом (числом) *A)* з подальшим розгортанням у лінійну комбінацію біноміальних коефіцієнтів так, щоб виконувалась система кодових обмежень за довжиною рівновагових послідовностей *n*, ваги кодових слів *w* і потужності коду *M :*

$$\begin{cases} \forall j : w(C_j) = const = w; \\ 0 \le A < M; \\ 0 \le w \le n. \end{cases}$$

Число *A* подається у вигляді рівновагової двійкової послідовності $C_A = (C_{A0}\ C_{A1}, \ldots, C_{A_{n-1}})$

$$A = \sum_{i=0}^{5} C_{A_{n-i-1}} b_i ,$$

де

$$b_i = \binom{n-i-1}{w-l},$$

l – номер ненульогово елемента $C_{A_{n-m-1}}$, для якого

$$b_l \le \sum_{m=0}^{i-1} C_{A_{n-m-1}} b_m .$$

Очевидно, що сума в правій частині виразу дорівнює сумі тільки тих b_m, для яких відповідні елементи вектора C_A не дорівнюють нулю $(C_{A_{n-m-1}} \neq 0)$. Використовуючи

введений вище номер *l* ненульового елементу в C_A, процес формування двійкової рівновагової кодової послідовності схематично подамо в такому вигляді (мал. 1).

Рис. 1. Схема формування кодових слів двійкового рівновагового коду

Відомий алгоритм двійкового рівновагового кодування, заснований на розглянутому вищеметоді, перетворить число *A* на рівновагову двійкову послідовність $C_A = (C_{A_0}\ C_{A_1}\ \ldots\ C_{A_{n-1}}$

і складається з таких кроків:

1. Ввести параметри n, w і число $A < M$, яке належить двійковому рівноваговому кодуванню.
2. Прийняти $x=A$, $i=0$, $l=0$.
3. Вирахувати число: $b_i = \binom{n-i-1}{w-l}$
4. Якщо $b_i > x$:
- $C_{A_{n-i-1}} = 1$
- $i = i + 1$ і перейти до кроку 3.
5. Якщо $b_i \le x$:
- $C_{A_{n-i-1}} = 1$
- $x = x - b_i$
- $i = i + 1$
- $l = l + 1$ і перейти до кроку 3.
6. Вивести вектор $C_A = (C_{A_0} C_{A_1} \ldots . C_{A_{n-1}})$

Приклад. Нехай $n=6$, $w=4$. Результат роботи розглянутого вище алгоритму в отриманій відповідності всіх чисел A, їх двійкових представлень $I_A = (I_{A_0} I_{A_1} \ldots . I_{A_{k-1}})$ в позиційному двійковому коді довжини

$$k = \lceil \log_2 M \rceil = \lceil \log_2 15 \rceil = 4$$

і знайдених двійкових рівноважових векторів C_A наведено в таблиці 1.

Таблиця 1

A	I_A	C_A	A	I_A	C_A
0	(0 0 0 0)	(1 1 1 1 0 0)	8	(0 0 0 1)	(0 1 1 1 0 1)
1	(1 0 0 0)	(1 1 1 0 1 0)	9	(1 0 0 1)	(1 1 0 0 1 1)
2	(0 1 0 0)	(1 1 0 1 1 0)	10	(0 1 0 1)	(1 0 1 0 1 1)
3	(1 1 0 0)	(1 0 1 1 1 0)	11	(1 1 0 1)	(0 1 1 0 1 1)
4	(0 0 1 0)	(0 1 1 1 1 0)	12	(0 0 1 1)	(1 0 0 1 1 1)
5	(1 0 1 0)	(1 1 1 0 0 1)	13	(1 0 1 1)	(0 1 0 1 1 1)
6	(0 1 1 0)	(1 1 0 1 0 1)	14	(0 1 1 1)	(0 0 1 1 1 1)
7	(1 1 1 0)	(1 0 1 1 0 1)			

Слід зазначити, що отримане подання чисел задовольняє аналітичним співвідношенням:

$$A = \sum_{i=0}^{3} I_{A_i} 2^i$$

і $A = \sum_{i=0}^{5} C_{A_{n-i-1}} b_i$, $b_i = \binom{5-i}{4-l}$ у введених вище позначеннях. Сформована множина з 15 двійкових рівноважових векторів C_A утворює рівноваговий біноміальний $C = \{C_0, C_1, \ldots, C_{14}\}$, який не може використовуватися як для контролю помилок в асиметричних каналах передачі даних, так і в кодових шифросистемах як сеансові ключі.

Слід зазначити, що розглянутий метод не передбачає формування недвійкових рівновагових послідовностей (векторів C_A с $C_{j_i} \in \{0,1,\ldots,q-1\}, q > 2$) і не дозволяє, таким чином, реалізувати недвійкове рівновагове кодування.

У статті пропонується новий метод недвійкового рівновагового кодування на основі узагальненого біноміально-позиційного подання, який дозволяє узагальнити розглянутий вище підхід для недвійкового випадку і практично реалізувати обчислювальні алгоритми формування недвійкових послідовностей фіксованої ваги.

3. Пропонований метод недвійкового рівновагового кодування

Для поширення розглянутого підходу формування рівновагових послідовностей на недвійковий випадок пропонується нова форма *узагальненого біноміально-позиційного подання чисел.* Пропонована система числення належить до класу змішаних систем і базується на поданні чисел через зростаючу послідовність біноміальних коефіцієнтів, кожен з яких кодується позиційною нумерацією, тобто подання розрядів при біноміальних коефіцієнтах засноване на місцевому значенні цифр.

Розглянемо число x у пропонованій узагальненій біноміально-позиційній системі числення:

$$x = \sum_{i=0}^{n-1} a_i b_i$$

Пропонуємо:

$$a_i \in \{0,1,\ldots,q-1\}, b_i = \binom{u_{i+1}}{i+1} = \frac{u_{i+1}!}{(i+1)! \times (u_{i+1}-i-1)!}$$

$$0 \le u_1 < u_2 < \cdots < u_n = \frac{n!}{w! \times (n-w)!}$$

де w - число ненульових елементів узагальненого біноміально-позиційного коду.

Тоді число x подається через зростаючу послідовність біноміальних коефіцієнтів $b_0, b_1, \ldots, b_{n-1}$ і відповідну послідовність $a_0, a_1, \ldots, a_{n-1}$.

Розглянемо ненульові елементи $a_i \neq 1, i = 0,1,\ldots,n-1$ послідовність $a_0, a_1, \ldots, a_{n-1}$ і перенумеруємо їх, тобто, позначимо їх як елементи послідовності $a_0, a_1, \ldots, a_{w-1}$, $l = 0,1,\ldots,w-1$, причому $\forall l; a_l \in \{1,\ldots,q-1\}$.

Послідовність $a_0, a_1, \ldots, a_{w-1}$ і всі її елементи a_l (ненульові елементи послідовності $a_0, a_1, \ldots, a_{n-1}$ пронумеровані в порядку зростання старшинства розрядів) утворюються з використанням позиційної системи відліку з основи, $q-1$, тобто, $q-1$ одиниць у кожному розряді об'єднуються в одну одиницю наступного за старшинством розряду. Набір ненульових елементів a_l, $l = 0,1,\ldots,w-1$ задає число x_i, яке подається у позиційній системі в такий спосіб:

$$x_i = \sum_{l=0}^{w-1} (a_l - 1)h^l,$$

де $h=q-1$- основа використаної позиційної системи, $1 \le a_l < q$

Зростаюча послідовність біноміальних коефіцієнтів $b_0, b_1, \ldots, b_{n-1}$ задає число x_A, яке подається у біноміальній системі числення у вигляді:

$$x_A = \sum_{i=0}^{n-1} a_{A_i} b_i,$$

де $a_{A_i} \in \{0,1\}$.

Число x у пропонованій узагальненій біноміально-позиційній системі числення задовольняє рівнянню

$$x = a_{A_i} \cdot (q-1)^w + x_i,$$

що задає основне кодове обмеження на елементи узагальненого біноміально-позиційного коду.

Таким чином, число x у пропонованій системі узагальненого біноміально-позиційного рахунку подається як лінійна комбінація:

$$x = \sum_{i=0}^{n-1} a_i\, b_i = x_A \cdot (q-1)^w + x_i = (q-1)^w \sum_{i=0}^{n-1} a_{A_i} b_i + \sum_{l-0}^{w-1} (a_l - 1)(q-1)^l$$

Запропоноване узагальнення біноміально-позиційного способу подання чисел полягає в комплексному використанні позиційної системи відліку та системи біноміального рахунку: перший додаток у правій частині рівняння через зростаючу послідовність біноміальних коефіцієнтів задає розміщення ненульових елементів узагальненого біноміально-позиційного коду, другий додаток задає власні значення ненульових елементів послідовності в позиційному коді.

Запропонований спосіб подання чисел покладемо в основу методу недвійкового рівновагового кодування. Для абстрактного визначення недвійкового рівновагового коду введемо такі формальні позначення: n – довжина коду; $C = \{C_0, C_1, \ldots, C_{m-1}\}$ - множина кодових слів, $C_j = (C_{j0}, C_{j1}, \ldots, C_{j_{n-1}}) \in C$, $C_{j_i} \in \{0,1, \ldots, q-1\}$, $j = 0,1, \ldots, M-1, i = 0,1, \ldots, n-1$, причому $\forall j: w(C_j) = const = w$.

Потужність поданого недвійкового рівновагового коду визначається числом векторів довжини n і ваги w з елементами множини $\{0,1, \ldots, q-1\}$:

$$|C| = M = (q-1)^w \frac{n!}{w!\,(n-w)!}$$

Пропонований метод заснований на поданні інформаційних даних у вигляді числового еквіваленту A з подальшим розгортанням у лінійну комбінацію біноміальних коефіцієнтів, кожен з яких кодується позиційною нумерацією так, щоб виконувалася система кодових обмежень за довжиною рівновагових послідовностей n, ваги кодових слів w та потужності коду M:

$$\begin{cases} \forall j: w(C_j) = const = w; \\ 0 \le A < M; \\ 0 \le w \le n; \\ 0 \le C_{j_i} \le q; \end{cases}$$

Число A подається у вигляді рівновагової недвійкової послідовності $C_A = (C_{A0}\, C_{A1}, \ldots, C_{A_{n-1}})$, причому

$$A = A_A \cdot (q-1)^w + A_I$$

де

$$A_A = \sum_{i=0}^{n-1} a_{A_i} b_i,\ b_i = \binom{n-i-1}{w-l},$$

$$A_I = \sum_{l=0}^{w-1} (a_l - 1) h^l,\ h = q-1.$$

Процес формування рівновагової недвійкової послідовності подамо в чотири етапи.

1. Подання числа A в вигляді чисел $A_Б$ і $A_П$:

$$A_A = \left\lfloor \frac{A}{(q-1)^w} \right\rfloor,$$
$$A_I = (A) \bmod \left((q-1)^w\right),$$

де $\lfloor y \rfloor$ - ціла частина числа y.

Однозначності подання числа A у вигляді чисел $A_Б$ і $A_П$ обґрунтовуються на китайській теоремі про залишки [4].

Число $A_Б$ лежить в проміжку $0 \le A_Б < \frac{M}{(q-1)^w}$ і може, таким чином бути подане у біноміальній системі числення з кодовими обмеженнями:

$$\begin{cases} \forall j: w(c_j) = const = w; \\ 0 \le A_Б < \frac{n!}{w!(n-w)!}; \\ 0 \le w \le n. \end{cases}$$

Число $A_П$ лежить в проміжку $0 \le A_П < (q-1)^w$ і, відповідно, може бути подане в позиційній системі числення з основою $h = q - 1$.

2. Подання числа $A_Б$ у біноміальній системі числення:

$$A_A = \sum_{i=0}^{n-1} a_{A_i} b_i,\ b_i = \binom{n-i-1}{w-l}.$$

3. Подання числа $A_П$ у позиційній системі числення:

$$A_I = \sum_{l=0}^{w-1} (a_l - 1) h^l,\ h = q - 1.$$

4. Формування послідовності $C_A = (C_{A0}\ C_{A1}, \ldots, C_{A_{n-1}}) \in C$:

$C_{A_i} = a_i a_{A_i}, i = 0,1, \ldots, n-1, l = 0,1, \ldots, w-1$

Тобто, якщо для деякого $i = 0,1,\ldots,n-1$ у вигляді $A_Б$ маємо $a_{A_i} = 0$, тоді отримаємо, $C_{A_i} = 0$; якщо $a_{A_i} = 1$, тоді отримаємо $C_{A_i} = a_l$,тобто потрібний елемент дорівнює відповідному ненульовому елементу в представленні $A_П$.

Перераховані етапи реалізуються сукупністю прийомів і операцій арифметичного кодування і подання чисел у системі залишкових класів (етап 1), біноміального двійкового кодування (етап 2), позиційного кодування (етап 3) і комбінаторики (етап 4).

Процес формування недвійкової рівновагової кодової послідовності схематично подамо в такому вигляді (мал. 2). Слід зазначити, що розглянута вище схема двійкового рівновагового кодування використовується тут як складовий елемент, при виконанні операцій кодування числа $A_Б$ у біноміальній системі числення.

Пропонований алгоритм недвійкового рівновагового кодування, заснований на запропонованому методі, перетворює число A на рівновагову недвійкову послідовність $C_A = (C_{A0}\ C_{A1}, \ldots, C_{A_{n-1}})$ і складається з таких кроків.

1. Ввести параметри n, w, q і число $A < M$, що підлягає недвійковому рівно ваговому кодуванню.
2. Подати число A в вигляді $A = A_A \cdot (q-1)^w + A_I$, тобто, обчислити:

2.1. $A_{A^{\cdot}} = \left\lfloor \frac{A}{(q-1)^w} \right\rfloor$;

2.2. $\mathrm{A}_{\dot{\mathrm{i}}} = (\mathrm{A}) mod((q-1)^w)$.

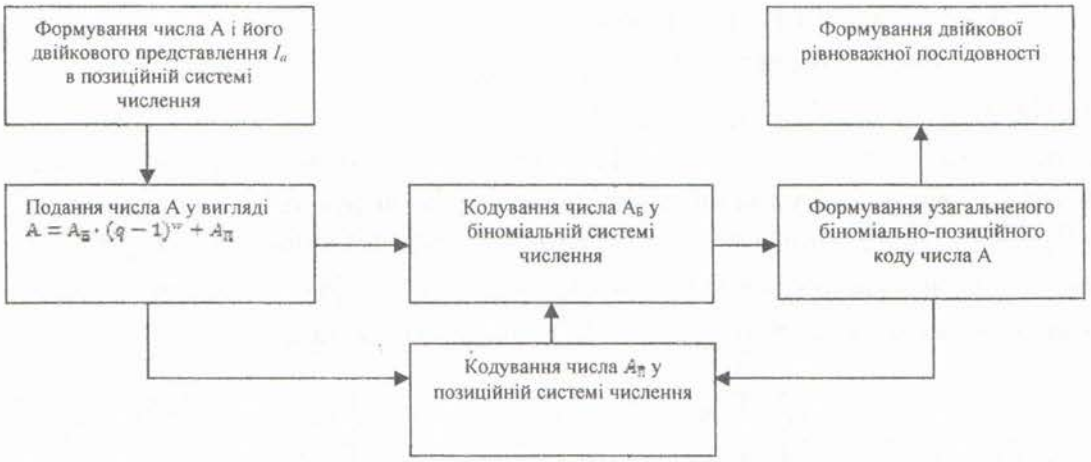

Рис.2. Схема формування кодових слів недвійкового рівно вагового коду

3. Закодувати число $A_{A^{\cdot}}$ двійковим біноміальним кодом:
   3.1. Прийняти $x=A_{A^{\cdot}}$, $i=0$, $l=0$.
   3.2. Обрахувати число $b_i = \binom{n-i-1}{w-l}$.
   3.3. Якщо $b_i > x$:
      3.3.1. $a_{A^{\cdot}_{n-i-1}} = 0$;
      3.3.2. $i = i+1$ і перейти до кроку 3.2.
   3.4. Якщо $b_i \le x$:
      3.4.1. $a_{A^{\cdot}_{n-i-1}} = 1$;
      3.4.2. $x = x - b_i$
      3.4.3. $i = i+1$
      3.4.4. $l = l+1$ і перейти до кроку 3.2.
   3.5. Сформувати вектор $(a_{A^{\cdot}_0} \quad a_{A^{\cdot}_1} \quad a_{A^{\cdot}_{n-1}})$.
4. Закодувати число $\mathrm{A}_{\dot{\mathrm{i}}}$ позиційним кодом довжини w за основою q-1:
   4.1. Взяти $x = A_{\dot{\mathrm{i}}}, l = 0$.
   4.2. Обчислити $a_l = (x) mod(q-1) + 1$;
   4.3. Обчислити $x = \left\lfloor \frac{x}{q-1} \right\rfloor$;
   4.4. $l = l+1$;
   4.5. Якщо $l < w$, перейти до кроку 4.2;
   4.6. Сформувати вектор $(a_0 \quad a_1 \quad a_{w-1})$.
5. Сформувати недвійкову рівновагову послідовність:
   5.1. Прийняти $i = 0, l = 0$.
   5.2. Якщо $a_{A^{\cdot}_i} \neq 0$:
      5.2.1. $\mathrm{C}_{Ai} = a_l$;

5.2.2. $l = l + 1$

5.2.3. $i = i + 1$ і перейти до кроку 5.2.

5.3. Якщо $a_{A_i} = 0$:

5.3.1. $C_{A_i} = 0$;

5.3.2. $i = i + 1$ і перейти до кроку 5.2.

5.4. Сформувати вектор $(C_{A0}\ C_{A1}, \ldots, C_{A_{n-1}})$.

6. Вивести вектор $(C_{A0}\ C_{A1}, \ldots, C_{A_{n-1}})$.

Приклад. Нехай $n = 3, w = 1, q = 4$. Тоді $0 \le A < 9$. Результат роботи n запропонованого алгоритму у вигляді отриманої відповідності всіх чисел A, їх двійкових представлень $I_A = (I_{A0}\ I_{A1}\ I_{A_{k-1}})$ в позиційному двійковому коді довжини $k = \lceil \log_2 M \rceil = \lceil \log_2 9 \rceil = 4$, чисел A_A і A_i, відповідних їм векторів $(a_{A_0}\ a_{A_1}\ a_{A_2})$ і $(a_0\ )$ і сформованих недвійкових рівновагових векторів $C_A = (C_{A0}\ C_{A1}, \ldots, C_2)$ наведено в таблиці 2.

Таблиця 2

A	I_A	A_A	$(a_{A_0}\ a_{A_1}\ a_{A_2})$	A_i	$(a_0\ )$	$C_A = (C_{A0}\ C_{A1}, \ldots, C_2)$
0	(0 0 0 0)	0	(1 0 0)	0	(1)	(1 0 0)
1	(1 0 0 0)	0	(1 0 0)	1	(2)	(2 0 0)
2	(0 1 0 0)	0	(1 0 0)	2	(3)	(3 0 0)
3	(1 1 0 0)	1	(0 1 0)	0	(1)	(0 1 0)
4	(0 0 1 0)	1	(0 1 0)	1	(2)	(0 2 0)
5	(1 0 1 0)	1	(0 1 0)	2	(3)	(0 3 0)
6	(0 1 1 0)	2	(0 0 1)	0	(1)	(0 0 1)
7	(1 1 1 0)	2	(0 0 1)	1	(2)	(0 0 2)
8	(0 0 0 1)	2	(0 0 1)	2	(3)	(0 0 3)

Сформована множина із 9 недвійкових рівновагових векторів $C_A = (C_{A0}\ C_{A1}, \ldots, C_{A2})$ утворює недвійковий рівноваговий код $\widetilde{N} = \{\widetilde{N_0}, C_1, \ldots, C_8\}$.

Наведемо ще один, більш складний приклад.

Приклад. Нехай $n = 3, w = 2, q = 4$. Тоді $0 \le A < 27$. Результат роботи запропонованого алгоритму наведено в таблиці 3.

Сформована множина із 27 недвійкових рівновагових векторів $C_A = (C_{A0}\ C_{A1}, \ldots, C_{A2})$ утворює недвійковий рівноваговий код $\widetilde{N} = \{\widetilde{N_0}, C_1, \ldots, C_{26}\}$, який може використовуватися як для контролю помилок в недвійкових асиметричних каналах передачі даних, так і в шифросистемах на недвійкових кодах як сеансових ключах [8,9].

Таким чином, запропонована система числення на основі узагальненого біноміально-позиційного подання чисел дозволяє комплексно використовувати як місцеве значення цифр кодової послідовності значення біноміальних коефіцієнтів. Застосування розробленої системи відліку дозволяє створювати ефективні методи та алгоритми недвійкового рівновагового кодування для їх використання в різних практичних додатках.

Висновки

За результатами проведених досліджень запропонована нова система числення на основі узагальненого біноміально-позиційного подання чисел. Вона полягає в комплексному використанні системи біноміального обрахунку (через зростаючу послідовність біноміальних коефіцієнтів задається розміщення ненульових елементів) і позиційної системи числення (значення ненульових елементів задаються через місцеве значення чисел).

Таблиця 3

A	I_A	A_{A^-}	$(a_{A_0}\ a_{A_1}\ a_{A_2})$	$A_{\bar{i}}$	$(a_0\ a_1)$	$(C_{A0}\ C_{A1}, \ldots, C_2)$
0	(0 0 0 0 0)	0	(1 1 0)	0	(1 1)	(1 0 0)
1	(1 0 0 0 0)	0	(1 1 0)	1	(2 1)	(2 0 0)
2	(0 1 0 0 0)	0	(1 1 0)	2	(3 1)	(3 0 0)
3	(1 1 0 0 0)	0	(1 1 0)	0	(1 2)	(0 1 0)
4	(0 0 1 0 0)	0	(1 1 0)	1	(2 2)	(0 2 0)
5	(1 0 1 0 0)	0	(1 1 0)	2	(3 2)	(0 3 0)
6	(0 1 1 0 0)	0	(1 1 0)	0	(1)	(0 0 1)
7	(1 1 1 0 0)	0	(1 1 0)	1	(2)	(0 0 2)
8	(0 0 0 1 0)	0	(1 1 0)	2	(3)	(0 0 3)
9	(1 0 0 1 0)	1	(1 0 1)	0	(1 1)	(1 0 1)
10	(0 1 0 1 0)	1	(1 0 0)	0	(1)	(1 0 0)
11	(1 1 0 1 0)	1	(1 0 0)	1	(2)	(2 0 0)
12	(0 0 1 1 0)	1	(1 0 0)	2	(3)	(3 0 0)
13	(1 0 1 1 0)	1	(1 1 0)	0	(1)	(0 1 0)
14	(0 1 1 1 0)	1	(1 1 0)	1	(2)	(0 2 0)
15	(1 1 1 1 0)	1	(1 1 0)	2	(3)	(0 3 0)
16	(0 0 0 0 1)	1	(1 0 1)	0	(1)	(0 0 1)
17	(1 0 0 0 1)	1	(1 0 1)	8	(3 3)	(3 0 3)
18	(0 1 0 0 1)	2	(0 1 1)	0	(1 1)	(0 1 1)
19	(1 1 0 0 1)	2	(0 1 1)	1	(2 1)	(0 2 1)
20	(0 0 1 0 1)	2	(0 1 1)	2	(3 1)	(0 3 1)
21	(1 0 1 0 1)	2	(0 1 1)	3	(1 2)	(0 1 2)
22	(0 1 1 0 1)	2	(0 1 1)	4	(2 2)	(0 2 2)
23	(1 1 1 0 1)	2	(0 1 1)	5	(3 2)	(0 3 2)
24	(0 0 0 1 1)	2	(0 1 1)	6	(1 3)	(0 1 3)
25	(1 0 0 1 1)	2	(0 1 1)	7	(2 3)	(0 2 3)
26	(0 1 0 1 1)	2	(0 1 1)	8	(3 3)	(0 3 3)

Вперше запропонований метод недвійкового рівновагового кодування на основі узагальненого біноміально-позиційного подання чисел, який дозволяє поширити відомий підхід на недвійковий випадок і практично реалізувати обчислювальні алгоритми формування недвійкових послідовностей фіксованої ваги.

Список літератури

1. *Гашков С.Б.* Системы счисления и их применение. М.: МЦНМО, 2004. — 52 с.

2. *Борисенко А.А.* Биномиальный счет. Теория и практика: Монография. — Сумы: ИТД «Университетская книга», 2004. — 170 с.

3. *Бережна О.В.* Методи і алгоритми адаптивного рівноважного кодування для інформаційних систем.

Автореф. дис… канд. техн. наук: 05.13.06 / Харк. нац. ун-т радіоелектрон. — Х., 2002. — 19 с. — укр.

4. *Мак-Вильямс Ф.Дж., Слоэн Н. Дж.А.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.

5. *McEliece. R.J.* A Public-Key Criptosystems and Algebraic Coding Theory // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January — February, 1978. — P. 114-116.

6. *Niederreiter. H.* Knapsack-Type Criptosystems and Algebraic Coding Theory // Probl. Control and Inform. Theory. — 1986. — V.15. — P. 19-34.

7. *Сидельников В.М.* Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. — 2002. — 22 с.

8. *Стасев Ю.В., Кузнецов А.А.* Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов. // Кибернетика и системный анализ: Международный научно-теоретический журнал. — Киев: НАНУ. — 2005. — №3. — С. 47-57.

Розглядаються змішані системи числення, що використовують біноміальне представлення чисел, досліджуються методи нелінійного кодування рівно ваговими кодами, в основі яких лежить біноміальний розрахунок. Пропонується метод недвійкового рівно вагового кодування на основі узагальненого біноміально-позиційного представлення, який дозволяє узагальнити відомий підхід на недвійковий випадок і практично реалізувати обчислювальні алгоритми формування недвійкових послідовностей фіксованої ваги.
Ключові слова: рівновагове кодування, система числення, біноміальний код, недвійкове кодування.

Рассматриваются смешанные системы счисления, использующих биномиальное представление чисел, исследуются методы нелинейного кодирования ровновесовыми кодами, в основе которых лежит биномиальный расчет. Предлагается метод недвоичного ровновесового кодирования на основе обобщенного биномиальной-позиционного представления, позволяющий обобщить известный подход на недвоичный случай и практически реализовать вычислительные алгоритмы формирования недвийкових последовательностей фиксированной веса.
Ключевые слова: равновесное кодирование, система счисления, биномиальный код, недвоичное кодирования

The mixed notation, using the binomial representation of numbers, methods of nonlinear coding, which are based on the binomial calculation, are investigated. A method for nonbinary coding based on generalized binomial-positional representation, which allows to generalize well-known approach to the nonbinary case and practically implement the computational algorithms for formation of non-binary sequences of fixed weight.
Keywords: equilibrium coding, notation, binomial code, nonbinary coding.

Надійшла 16.05.2010

УДК [004.415.24:519.237.8]:004.056.8

д.т.н., проф. Шумейко А.А.
(Институт предпринимательства «Стратегия»),
ТищенкоТ.Н., Пасько А.И.
(Днепродзержинский государственный технический университет),

ИСПОЛЬЗОВАНИЕ ПОЛИНОМИАЛЬНОГО ПРОГНОЗА ДЛЯ ВНЕДРЕНИЯ В ИЗОБРАЖЕНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Старейший из водяных знаков был употреблен в 1282 г. в Болонье [1], что было связано с бурным развитием в Европе бумажной промышленности. Фабрики для идентификации и защиты своей продукции от подделок начали применять водяные знаки. Позже водяные знаки стали на защиту почтовых марок, денег и различных ценных бумаг. С развитием компьютерной техники и информационных технологий появились различные способы представления информации в цифровом виде, что повлекло за собой массовое использование цифровых фотографий, фильмов, музыки и их чрезвычайно быстрое распространение в глобальной сети интернет. На современном этапе история повторяется,