

Згідно представленого алгоритму на рис.2: після пуску ЕОМ зчитується поточне значення температури T_1 , потім обчислюється поточна міцність Y (T_1), після чого задаються параметри сировинного режиму: $X_1= 6-8\%$; $X_2= 1-7 \text{ м}^2/\text{г}$; $X_3= 70-92\%$; $X_4= 0,4-1,2 \text{ м}^2/\text{г}$; $X_5= 6-8,5\%$; $X_7 = 1,4\text{год}$; $X_8 = 19^0\text{С}$; $X_9 = 5\text{год}$; $A_0 = 1,63$; $A_1 = 0,053$; $A_2 = 0,042$; $A_3 = 0,005$; $A_4 = 0,021$; $A_5 = 0,32$; $A_6 = -0,068$; $A_7 = 0,024$; $A_8 = -0,16$; $A_9 = -0,22$. За даними ЕОМ розраховує необхідну міцність Y . Якщо $Y(T_1) \geq Y$, то видається інформація про закінчення технологічного процесу на ЕОМ. В іншому випадку поточна температура порівнюється із заданою X_8 . Якщо поточне значення температури більше заданого, видається інформація на відкриття електромагнітного клапану впуску пари з перепускного трубопроводу і впуску гострої пари з паропроводу. Після цього ЕОМ повертається до читання коду температури. Якщо поточна температура менше або дорівнює заданій, видається повідомлення про відкриття засувки впуску пари в один із сусідніх автоклавів через паропровід перепускного пара і через паропровід гострої пари. ЕОМ повертається до читання коду температури. Цикл запарювання закінчується при досягненні заданої міцності виробів. Результати про закінчення тепловологої обробки виробів виводяться на екран.

Висновки: Використання запропонованого способу контролю тепловологої обробки силікатних виробів в автоклаві дозволяють при заданій міцності виробів і розрахованих оптимальних значеннях температури, швидкості її підйому, тривалості циклу при постійній температурі, змінювати подачу теплоносія в автоклав, що в подальшому призведе до економії часу тепловологої обробки та витрат енергоресурсів.

Список використаної літератури

1. Авторское свидетельство № 857073 СССР М.К.666.711(088.8).Способ автоклавной обработки силикатного кирпича. В.Н. Глухов, А.А.Чумаков, Н.Г.Ботов.- 1981- №31
2. Авторское свидетельство №490097 СССР М.К.621.646.223(088.8). Способ автоматического регулирования процесса тепловлажностной обработки в автоклаве. В.С. Зорохов, К.З. Исканиев, В.М. Шинкаренко, Н.С. Эльман - 1976 - №40
3. Мухина Т.Г.Производство силикатного кирпича -М: Стройиздат, 1982-225с
4. Буцуев С.Д., Михайлов В.С. Автоматика и автоматизация производственных процессов. Пособие для вузов.- М.:Высш.школа.1990 – 256 с.

АНАЛІЗ ПОСЛІДОВНОСТЕЙ НА ВИХОДІ ЗСУВНОГО РЕГІСТРУ З ЛІНІЙНИМ ЗВОРОТНИМ ЗВ'ЯЗКОМ

Шрамченко Б.Л.

Україна, м. Київ,

Київський національний університет технологій та дизайну

Показано, каким образом из существования эквивалентных регистра Фибоначчи и регистра Галуа следует, что максимальный период последовательности на выходе регистра Фибоначчи равен $2^r - 1$, где r – количество разрядов регистра. Установлено, что инверсный порядок отводов регистра Фибоначчи влечет инверсию последовательности на выходе.

Аналіз відповідності між двома конфігураціями регістру зсуву з лінійним зворотним зв'язком (РЗЛЗЗ)

Традиційним засобом, що використовується при побудові генераторів потокових ключів є РЗЛЗЗ [1]. У загальному випадку регістр з лінійним зворотним зв'язком можна представити як показано на рис. 1.

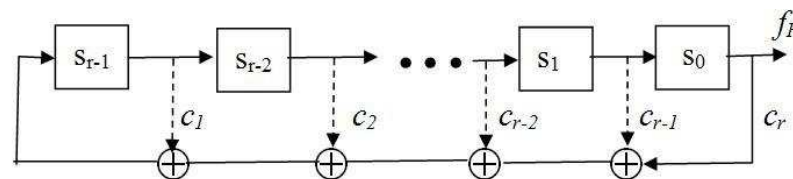


Рис. 1. РЗЛЗЗ (конфігурація Фібоначчі).

Мітка c_i вказує на те, чи існує зв'язок, біля якого вона розташована на схемі. Якщо $c_i = 1$, зв'язок існує, а якщо $c_i = 0$, - ні. В літературі [2] ця схема отримала назву «конфігурація Фібоначчі».

Існує інша схема РЗЛЗЗ, що дозволяє отримати на виході ту ж саму послідовність. Ця схема (рис. 2) називається «конфігурацією Галуа».

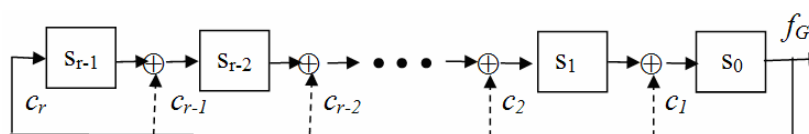


Рис. 2. РЗЛЗЗ (конфігурація Галуа).

У регістрі Галуа кожне значення на виході (у кожному такті) додається до значення у відповідних розрядах. Тому тільки останній, правий біт дорівнює значенню на виході регістру. Усі інші розряди містять деякі проміжні значення.

Схема на рис. 1 показує, що член послідовності на виході, починаючи з r -го, є сумою за модулем 2 тих попередніх, яким відповідають одиничні коефіцієнти c_i . Наприклад, у суму входить безпосередньо попередній член, якщо $c_1 = 1$. Якщо $c_2 = 1$, то у суму входить член послідовності, що передує поточному на дві позиції, і т.д. При цьому член, що передує на r позицій завжди є доданком, або $c_r \equiv 1$.

Якщо скористатися позначенням a_i^t для стану комірки s_i у такті t , то для конфігурації Фібоначчі можна записати

$$a_{r-1}^{t+1} = \sum_{i=1}^r a_{r-i}^t,$$

та

$$\forall i \mid 1 < i \leq r, a_{r-i}^{t+1} = a_{r-i+1}^t.$$

Тому кожний член послідовності на виході регістру можна представити у вигляді

$$a_0^t = a_1^{t-1} = a_2^{t-2} = \dots = a_{r-1}^{t-r+1} = c_i a_{r-i}^{t-r} \sum_{i=1}^r$$

Оскільки $a_i^{t-r} = a_0^{t-r+i}$,

$$a_0^t = \sum_{i=1}^r c_i a_0^{t-i}.$$

У конфігурації Галуа, що відповідає поданій конфігурації Фібоначчі, кожний член послідовності дорівнює сумі тих же попередніх. Однак формується кожний член не в одному такті, а - в r . При цьому кожний член послідовності на виході регістру додається до поточного стану тих комірок, що містять проміжний стан наступних елементів послідовності, і які відповідають одиничним коефіцієнтам c_i .

Для конфігурації Галуа мають місце наступні співвідношення.

$$\begin{aligned} a_{r-1}^{t-r+1} &= a_0^{t-r}, \\ a_{r-2}^{t-r+2} &= c_{r-1} a_0^{t-r+1} \oplus a_{r-1}^{t-r+1}, \\ a_{r-3}^{t-r+3} &= c_{r-2} a_0^{t-r+2} \oplus a_{r-2}^{t-r+2}, \\ &\dots \\ a_0^t &= c_1 a_0^{t-1} \oplus a_1^{t-1}. \end{aligned}$$

Виконавши послідовно підстановки для a_i^{t-i} , $i = 1, r-1$, отримуємо

$$a_0^t = \sum_{i=1}^r c_i a_0^{t-i},$$

де $c_r = 1$. Таким чином, побудована вказаним способом конфігурація Галуа дає на виході послідовність, що визначається тим же рекурентним співвідношенням, що і послідовність на виході поданої конфігурації Фібоначчі. Як бачимо, порядок, у якому застосовуються числа c_i у конфігурації Фібоначчі, протилежний тому, що у конфігурації Галуа.

Для того, щоб регістр Галуа видавав на виході ту ж саму послідовність, що і регістр Фібоначчі, крім відповідності між відводами, треба, щоб мала місце і відповідність між початковими станами регістрів. Визначимо початковий стан ($b_{r-1}, b_{r-2}, \dots, b_0$) регістру Галуа при поданому початковому стані ($a_{r-1}, a_{r-2}, \dots, a_0$) регістру Фібоначчі.

Очевидно, що $b_0 = a_0$, як перший член послідовності на виході, що збігається з початковим станом комірки s_0 в обох регістрах.

Далі, з рівняння $b_1 \oplus c_1 a_0 = a_1$ отримуємо

$$b_1 = c_1 a_0 \oplus a_1.$$

Використовуючи співвідношення

$$\begin{aligned} b_2 \oplus c_2 a_0 \oplus c_1 a_1 &= a_2, \text{ маємо} \\ b_2 &= c_2 a_0 \oplus c_1 a_1 \oplus a_2. \end{aligned}$$

Продовжуючи аналогічно, для будь-якого $i < r$ можемо записати

$$b_i = c_i a_0 \oplus c_{i-1} a_1 \oplus \dots \oplus c_1 a_{i-1} \oplus a_i.$$

Застосування поліномів для аналізу поведінки РЗЛЗЗ

Кожному стану регістру, незалежно від конфігурації, можна поставити у відповідність поліном

$$a_{r-1} x^0 \oplus a_{r-2} x^1 \oplus \dots \oplus a_0 x^{r-1}.$$

Коефіцієнти цього поліному належать полю $GF(2)$. Сума двох поліномів з коефіцієнтами ($a_{r-1}, a_{r-2}, \dots, a_0$) та ($b_{r-1}, b_{r-2}, \dots, b_0$), відповідно, визначається як поліном з коефіцієнтами ($(a_{r-1} \oplus b_{r-1}, a_{r-2} \oplus b_{r-2}, \dots, a_0 \oplus b_0)$). При множенні двох таких

поліномів коефіцієнт при кожному x^i ($i = 0, 2r-2$) добутку визначається як

$$a_{r-1} b_{r-i+1} \oplus a_{r-2} b_{r-i+2} \oplus \dots \oplus a_{r-i+1} b_{r-1}.$$

Поліном, який відповідає наступному стану регістру, утворюється множенням поліному, що відповідає поточному

стану, на x (так відображається зсув) та виконанням деякої додаткової операції. У конфігурації Галуа, ця додаткова операція полягає у тому, що коли у поточному стані $a_0 = 1$, до результату добутку додається поліном

$$x^r \oplus c_1 x^{r-1} \oplus c_2 x^{r-2} \oplus \dots \oplus c_{r-1} x \oplus 1.$$

А це означає, що множення поточного поліному на x здійснюється за модулем $c(x) = x^r \oplus c_1 x^{r-1} \oplus c_2 x^{r-2} \oplus \dots \oplus c_{r-1} x \oplus 1$, оскільки визначена вище операція додавання поліномів збігається з операцією віднімання. Таким чином множина станів регістру Галуа утворює кільце з визначеною раніше операцією додавання поліномів та множенням за модулем $c(x)$.

Розглянемо приклад двох регістрів (регістр Фібоначчі на рис. 3 та регістр Галуа на рис. 4, що породжують однакові послідовності). В обох регістрах $c_1 = c_3 = 1$, а $c_2 = 0$. Тому $c(x) = x^4 \oplus x^3 \oplus x \oplus 1$. Приклад роботи цих регістрів, які формують однакові послідовності на виході, представлений у табл. 1 для регістру Фібоначчі та у табл. 2 - для регістру Галуа.

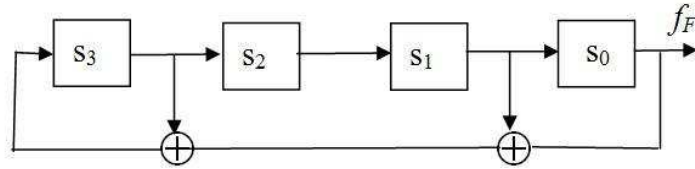


Рис. 3. Приклад чотирьохрозрядного регістру Фібоначчі.

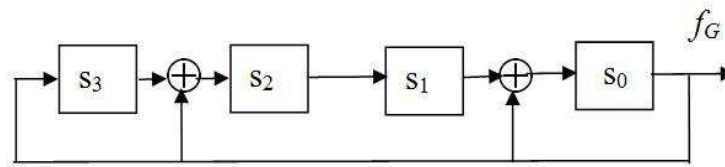


Рис. 4. Чотирьохрозрядний регістр Галуа, що відповідає регістру на рис. 3.

Таблиця 1

a_3	a_2	a_1	a_0	$a(x)$
1	0	0	1	$x^3 \oplus 1$
0	1	0	0	x
0	0	1	0	x^2
1	0	0	1	$x^3 \oplus 1$

Таблиця 2

b_3	b_2	b_1	b_0	$b(x)$
0	0	1	1	$x^3 \oplus x^2$
1	1	0	0	$x^4 \oplus x^3 \pmod{g(x)} = x \oplus 1$
0	1	1	0	$x^2 \oplus x$
0	0	1	1	$x^3 \oplus x^2$

У розглянутому прикладі $T = 3$.

У випадку, коли $c(x)$ – простий, для регістру Галуа поліноми $a(x)$ степеню не більше $r-1$ утворюють поле $GF(2^r)$ [3] з операцією додавання $a(x) + a^*(x) = a_{r-1} \oplus a_{r-1}^* \oplus (a_{r-2} \oplus a_{r-2}^*)x \oplus \dots \oplus (a_1 \oplus a_1^*)x^{r-2} \oplus (a_0 \oplus a_0^*)x^{r-1}$. При цьому у поліному степеню $k < r - 1$ усі коефіцієнти при степенях x більше k дорівнюють нулю. Операція множення виконується за модулем $c(x)$.

У цьому поліному x породжує деяку підгрупу $x, x^2, \dots, x^m \pmod{c(x)} = 1$. Це означає, що при будь-якому початковому стані регістру з відповідним поліномом $a(x)$ наступним станам відповідають поліноми $xa(x) \pmod{c(x)}, x^2a(x) \pmod{c(x)}, \dots, x^m a(x) \pmod{c(x)} = a(x)$. Звідси випливає, що період послідовності на виході регістру Галуа дорівнює m . Оскільки $x^m \pmod{c(x)} = 1$, то $(x^m + 1) \pmod{c(x)} = 0$, або $c(x)$ ділить $x^m + 1$.

У випадку, коли $m = 2^r - 1$, x породжує усю мультиплікативну групу, і період на виході регістру досягає максимального значення, а поліном $c(x)$ називають примітивним.

Будемо називати регістр Фібоначчі та регістр Галуа еквівалентними, якщо на їх виходах утворюються однакові послідовності. Розглянемо зв'язок між поліномами $g(x) = x^r \oplus g_{r-1}x^{r-1} \oplus g_{r-2}x^{r-2} \oplus \dots \oplus g_1x \oplus 1$ та $c(x) = x^r \oplus c_{r-1}x^{r-1} \oplus c_{r-2}x^{r-2} \oplus \dots \oplus c_1x \oplus 1$, що відповідають еквівалентним регістрам RG та RF . Коефіцієнти цих поліномів задовольняють умові

$$g_i = c_{r-i}, \quad i = \overline{1, r-1}.$$

Вище було показано, що на виході еквівалентних регістрів утворюється послідовність з максимальним періодом, що дорівнює $2^r - 1$, тоді і тільки тоді, коли поліном $g(x)$ примітивний. Покажемо, що цій же умові задовольняє і поліном $c(x)$. Для цього розглянемо регістр Фібоначчі RF^l , у якого відводи c^l_i , задовольняють умові

$$c^l_i = g_i = c_{r-i}, \quad i = \overline{1, r-1}.$$

Схема регістру показана на рис. 5.

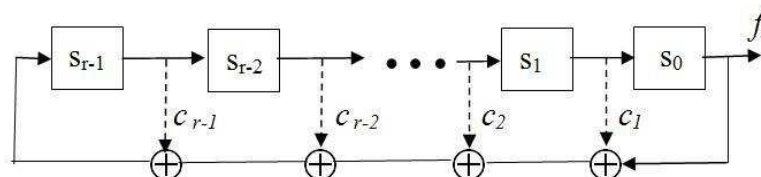


Рис. 5. Схема регістру RF^l .

На виході цього регістру утворюється послідовність максимального періоду тоді і тільки тоді, коли поліном $c(x)$ примітивний. Зіставимо послідовності на виході регістрів RF та RF^l . Нехай, у такті t ($t > r$) стан регістру RF - $(a_{r-1}^t, a_{r-2}^t, \dots, a_1^t, a_0^t)$, а регістру RF^l - $(a_0^t, a_1^t, \dots, a_{r-2}^t, a_{r-1}^t)$. У регістрі RF^l a_0^t міститься у комірці s_{r-1} , a_1^t - у s_{r-2} , і так далі, a_{r-1}^t - у s_0 . Тоді у наступних r тактах на виходах регістрів формуються взаємно інверсні послідовності (для кожного елементу наступний у одній послідовності дорівнює попередньому для цього елемента у іншій послідовності). Наприклад, у послідовності на виході регістру RF наступним елементом після $a_0^t \in a_1^t$, і на виході регістру RF^l елементу a_0^t передє a_1^t .

Для того, щоб показати, що з взаємної інверсії станів у деякому такті t впливає повна взаємна інверсія послідовностей на виході регістрів, достатньо показати, що елемент на виході регістру RF у такті $t+r$ дорівнює елементу на виході регістру RF^l у такті $t-1$.

Визначимо значення x , що міститься у комірці s_0 регістру RF^l у такті $t-1$. У цьому такті a_{r-1}^t міститься у комірці s_1 , a_{r-2}^t - у s_2 , і так далі, a_1^t - у s_{r-1} . Тому

$$a_0^t = c_{r-1} a_{r-1}^t \oplus c_{r-2} a_{r-2}^t \oplus \dots \oplus c_2 a_{r-2}^t \oplus c_1 a_{r-1}^t \oplus x.$$

Звідки

$$x = a_0^t \oplus c_{r-1} a_{r-1}^t \oplus c_{r-2} a_{r-2}^t \oplus \dots \oplus c_2 a_{r-2}^t \oplus c_1 a_{r-1}^t.$$

У регістрі RF (рис. 1)

$$a^{t+r}_0 = a^{t+1}_{r-1} = a^t_0 \oplus c_{r-1} a^t_1 \oplus c_{r-2} a^t_2 \oplus \dots \oplus c_2 a^t_{r-2} \oplus c_1 a^t_{r-1}.$$

Таким чином a^{t+r}_0 у регістрі RF дорівнює a^{t-1}_0 у регістрі RF^l . Як наслідок, послідовності на виході регістрів RF та RF^l взаємно інверсні. А звідси випливає, що поліном $c(x)$ – примітивний тоді і тільки тоді, коли $g(x)$ – примітивний.

Розглянемо роботу регістрів RF та RF^l , з якими асоційовані примітивні поліноми $c(x) = x^4 \oplus x^3 \oplus 1$ і $g(x) = x^4 \oplus x \oplus 1$ відповідно. Послідовності станів обох регістрів представлені у табл. 3, де стани комірок регістру RF^l позначені буквою b .

Таблиця 3

Такт	регістр RF				регістр RF^l			
	a_3	a_2	a_1	a_0	b_3	b_2	b_1	b_0
0	1	1	0	0	0	0	1	1
1	0	1	1	0	1	0	0	1
2	1	0	1	1	0	1	0	0
3	0	1	0	1	0	0	1	0
4	1	0	1	0	0	0	0	1
5	1	1	0	1	1	0	0	0
6	1	1	1	0	1	1	0	0
7	1	1	1	1	1	1	1	0
8	0	1	1	1	1	1	1	1
9	0	0	1	1	0	1	1	1
10	0	0	0	1	1	0	1	1
11	1	0	0	0	0	1	0	1
12	0	1	0	0	1	0	1	0
13	0	0	1	0	1	1	0	1
14	1	0	0	1	0	1	1	0
15	1	1	0	0	0	0	1	1

У поданій таблиці $a^{i \bmod 15}_0 = b^{(3-i) \bmod 15}_0$: $a^0_0 = b^3_0$, $a^1_0 = b^2_0$, $a^2_0 = b^1_0$, ..., $a^{13}_0 = b^5_0$, $a^{14}_0 = b^4_0$, що свідчить про те, що послідовності на виходах регістрів взаємно інверсні.

Література

1. Сمارт Н. Криптографія. – М.: Техносфера, 2005.
2. Шнайер Б. Прикладная криптография. Издание 2-е. Протоколы, алгоритмы и исходные тексты на языке Си. – М.: Триумф, 2002.
3. Мао В. Современная криптография: теория и практика. – М.: Изд. дом «Вильямс», 2005.

Секція «Будівництво та архітектура»:

ЛУЖНІ ШЛАКОПОРТЛАНДЦЕМЕНТИ, МОДИФІКОВАНІ ОРГАНІЧНИМИ КОМПЛЕКСОУТВОРЮЮЧИМИ ДОБАВКАМИ

Бондаренко О.П.

Україна, м. Київ,

Київський національний університет будівництва і архітектури

Abstract. In work made a selection additives as well as the features of the kinetics of increasing strength of alkali Blast-furnace cements modified with complex additives.

Keywords: Blast-furnace cement, activation, complex additive, durability.

На сьогоднішній день широкий інтерес до бетонів та бетонних сумішей з регульованими технологічними та експлуатаційними характеристиками обумовлює розвиток монолітного будівництва. При цьому однією з найважливіших є задача зниження матеріальних, енергетичних і трудових ресурсів, що в значній мірі досягається за рахунок розробки нових в'язучих речовин з максимальним вмістом відходів металургійної промисловості. Враховуючи існуючі екологічні