NIELINIOWE REJESTRY PRZESUWNE I ŁĄCZENIE SKRZYŻOWANYCH PAR STANÓW

Johannes Mykkeltveit[*], **Janusz Szmidt**[**]

[*] International Research Institute, Bergen, Norway
[**] Wojskowy Instytut Łączności, Zegrze, Poland
j.szmidt@wil.waw.pl

Streszczenie. Wyjaśniamy pochodzenie funkcji sprzężenia zwrotnego dla Nieliniowych Rejestrów Przesuwnych ze Sprzężeniem Zwrotnym (*NFSR*), które generują binarne ciągi de Bruijna. Funkcje te powstają przez zastosowanie operacji łączenia skrzyżowanych par stanów do wybranego rejestru przesuwnego generującego ciąg binarny o maksymalnym okresie; np. rejestru liniowego, który zawsze istnieje dla danego rzędu n. Otrzymany wynik pozwala konstruować wszystkie nieliniowe rejestry przesuwne generujące ciągi binarne o okresie $2^n - 1$.
Słowa kluczowe: nieliniowe rejestry przesuwne ze sprzężeniem zwrotnym, ciągi de Bruijna, metoda łączenia skrzyżowanych par stanów.

1. Wprowadzenie

Celem tej pracy jest przedstawienie konstrukcji funkcji Boolowskich sprzężenia zwrotnego dla nieliniowych rejestrów przesuwnych (*NFSR - ang. Nonlinear Feedback Shift Registers*), które generują ciągi binarne o maksymalnym okresie. W szczególności rozpatrywany jest problem czy dowolny binarny ciąg de Bruijna może być otrzymany z ustalonego ciągu de Bruijna tego samego rzędu przez zastosowanie operacji łączenia skrzyżowanych par stanów. Problem ten został postawiony na konferencji z Kodowania i Kryptologii (WCC 2013, Bergen, Norwegia) i pozytywnie rozwiązany wspólnie z Johannesem Mykkeltveitem. W terminach funkcji Boolowskich otrzymany wynik wskazuje jakie operacje algebraiczne mają być zastosowane do ustalonej funkcji Boolowskiej, aby otrzymać wszystkie funkcje sprzężenia zwrotnego nieliniowych rejestrów przesuwnych generujących ciągi de Bruijna tego samego rzędu.

Rejestry przesuwne ze sprzężeniem zwrotnym są użyteczne do generowania binarnych ciągów okresowych i w tym celu są stosowane w telekomunikacji i kryptografii. Liniowe rejestry przesuwne (*LFSR - ang. Linear Feedback Shift Registers*) i *NFSR* są głównymi elementami, z których budowane są szyfry strumieniowe. Algorytmy Mickey [1], Trivium [4], Grain [15], Achterbahn [11] i modyfikacje naprzemiennego generatora krokowego [27] są przykładami szyfrów strumieniowych, w których zastosowano *NFSR*.

Teoria rejestrów typu *LFSR* jest dobrze ugruntowana matematycznie. Badanie *NFSR* zostało rozpoczęte w pionierskiej monografii Golomba [12] i kontynuowane w następnych latach. W zastosowaniach kryptograficznych *NFSR* generujące tzw. zmodyfikowane ciągi de Bruijna są ważne, ponieważ w pewnych przypadkach algebraiczna postać normalna (*ANF - ang. Algebraic Normal Form*) odpowiadających funkcji sprzężenia zwrotnego jest dość prosta i dogodna do implementacji; patrz np. [11, 22].

Operacje łączenia i rozłączania cykli generowanych przez nieosobliwe rejestry przesuwne były rozpatrywane w książce Golomba [12]. Następnie istnienie tzw. skrzyżowanych par stanów (*ang. cross-join pairs*) było wykorzystane w serii prac [6, 9, 10, 23, 28] do konstrukcji nowych *NFSR*. Helleseth i Kløve [16] udowodnili ważny wynik, który podaje liczbę skrzyżowanych par stanów dla m-ciągów (ciągi o maksymalnym okresie generowane przez *LFSR*). Dubrowa w pracy [6] zastosowała operację łączenia skrzyżowanych par stanów do konstrukcji rejestrów typu Galois generujących ciągi o maksymalnym okresie.

Metody znajdowania *NFSR* z funkcją sprzężenia o prostej *ANF* były badane w pracach [3, 5, 7, 11, 17, 26]. Gong i Mandal [21] stosując metody z pracy Mykkeltveit *et al.* [24] podali metodę rekurencyjną konstruowania *NFSR* o maksymalnym okresie. Chan, Games i Rushanan [3] postawili hipotezę o istnieniu tzw. kwadratowych m-ciągów dla każdego rzędu n. W pracy [5] hipoteza ta została zweryfikowana eksperymentalnie do rzędu $n = 29$ i zostały znalezione *NFSR* o prostej *ANF* generujące kwadratowe m-ciągi. W niniejszej pracy przedstawiamy związek między *NFSR* generującymi kwadratowe m-ciągi a operacją łączenia skrzyżowanych par. Podany jest przykład rejestru rzędu 7 generującego zmodyfikowany ciąg de Bruijna, który został skonstruowany w wyniku zastosowania operacji łączenia skrzyżowanych par. Dowód Twierdzenia 3 został opublikowany w pracy [25].

2. Nieliniowe rejestry przesuwne

Niech $\mathbb{F} = \{0, 1\}$ oznacza ciało binarne, zaś $\mathbb{F}_2^n$ niech będzie n-wymiarową przestrzenią nad ciałem $\mathbb{F}_2$. Elementami przestrzeni $\mathbb{F}_2^n$ są ciągi binarne o długości n. Przykładowo taki ciąg (wektor) będziemy oznaczać $x = (x_0, x_1, \ldots, x_{n-1})$, gdzie $x_i \in \mathbb{F}_2$, $i = 0, 1, \ldots, n-1$. Przesuwy rejestr binarny ze sprzężeniem zwrotnym (*FSR - ang. Feedback Shift Register*) rzędu n (lub n-stanowy) jest odwzorowaniem $\mathfrak{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ postaci

$$\mathfrak{F}(x_0, \ldots, x_{n-1}) = (x_1, x_2, \ldots, x_{n-1}, f(x_0, \ldots, x_{n-1})),$$

gdzie f jest funkcją Boolowską od n zmiennych. Rejestr przesuwny jest określony jako nieosobliwy jeśli przekształcenie $\mathfrak{F}$ jest wzajemnie jednoznaczne, tzn. $\mathfrak{F}$ jest bijekcją na zbiorze $\mathbb{F}_2^n$.

Wykazuje się (patrz [12]), że rejestr przesuwny $\mathfrak{F}$ jest nieosobliwy wtedy i tylko wtedy, gdy funkcja Boolowska f jest postaci

$$f(x_0, \ldots, x_{n-1}) = x_0 + F(x_1, \ldots, x_{n-1}), \tag{1}$$

gdzie F jest funkcją Boolowską od $n-1$ zmiennych. Rejestry nieosobliwe jako przekształcenia przestrzeni $\mathbb{F}_2^n$ generują zamknięte cykle elementów tej przestrzeni. Największą liczbę cykli generuje tzw. rejestr czysto cykliczny rzędu n oznaczany PCR_n (*ang. Pure Cyclic Register*), gdzie funkcja $F \equiv 0$, tzn. funkcja sprzężenia zwrotnego f ma postać

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0.$$

PCR_n dokonuje rozkładu przestrzeni na liczbę cykli równą

$$Z(n) = \frac{1}{n} \sum_{d|n} \varphi(d) 2^{n/d},$$

gdzie $\varphi(.)$ jest funkcją Eulera, zaś suma jest po wszystkich dodatnich dzielnikach liczby n. Dla innych rejestrów nieosobliwych liczba generowanych cykli jest mniejsza.

FSR jest nazywany liniowym, (*LFSR - ang. Linear Feedback Shift Register*) jeśli funkcja Boolowska jest liniowa oraz nieliniowym, jeśli funkcja f jest nieliniowa, tzn. w algebraicznej postaci normalnej tej funkcji występują iloczyny argumentów. W dalszym ciągu będziemy zajmowali się generowaniem binarnych ciągów okresowych o pewnych specjalnych właściwościach przez nieliniowe i liniowe rejestry przesuwne.

Definicja 1. Ciągiem de Bruijna rzędu n nazywamy ciąg binarny (s_i) długości 2^n (rozpatrywany jako zamknięty cykl), w którym wszystkie układy n kolejnych bitów występują dokładnie jeden raz.

Zostało udowodnione przez Flue Sainte-Marie [8] w roku 1894 oraz niezależnie przez de Bruijna [2] w roku 1946, że liczba wszystkich cyklicznie nierównoważnych ciągów spełniających Definicję 1 jest równa

$$B_n = 2^{2^{n-1}-n}.$$

W zastosowaniach kryptograficznych występują tzw. zmodyfikowane ciągi de Bruijna, które nie zawierają podciągu kolejnych n zer.

Definicja 2. Zmodyfikowanym ciągiem de Bruijna rzędu n nazywamy ciąg o długości 2^n-1 (lub odpowiednio ciąg o okresie 2^n-1) otrzymany z ciągu de Bruijna rzędu n przez usunięcie jednego zera z podciągu kolejnych n zer, patrz [22].

Na podstawie Definicji 1 i 2 istnieje wzajemnie jednoznaczna odpowiedniość między ciągami de Bruijna rzędu n a zmodyfikowanymi ciągami de Bruijna tego samego rzędu. W szczególności mając zmodyfikowany ciąg de Bruijna długości (o okresie) 2^n-1 i dodając jedno zero do podciągu kolejnych $n-1$ zer otrzymujemy ciąg de Bruijna rzędu n. Liczba cyklicznie nierównoważnych zmodyfikowanych ciągów de Bruijna rzędu n wyraża się również wzorem (2). Ciągi de Bruijna generowane są przez pewne funkcje Boolowskie postaci (1). Liczba wszystkich funkcji postaci (1) jest równa liczbie wszystkich funkcji Boolowskich od $n-1$ zmiennych i wyraża się wzorem $2^{2^{n-1}}$.

Związek między ciągami de Bruijna a nieliniowymi rejestrami przesuwnymi wyraża następujące:

Twierdzenie 1. *Niech (s_t) będzie ciągiem de Bruijna (lub zmodyfikowanym ciągiem de Bruijna). Wtedy istnieje funkcja Boolowska $F(x_1,\ldots,x_{n-1})$ taka, że*

$$s_{t+n} = s_t + F(s_{t+1},\ldots,s_{t+n-1}), \quad t = 0,1,\ldots,2^n-n-1. \tag{3}$$

Dowód tego twierdzenia można znaleźć w książce Golomba [12]. Zatem ciągi de Bruijna generowane są przez pewne nieliniowe rekurencje. Na podstawie wzoru (2) prawdopodobieństwo tego, że losowo wybrana funkcja Boolowska postaci (1) będzie generować ciąg de Bruijna (lub odpowiednio ciąg zmodyfikowany) równe jest $2^{-(n-1)}$. Prawdopodobieństwo to można zwiększyć do $2^{-(n-3)}$ korzystając z pewnych własności funkcji generujących ciągi de Bruijna. W przypadku ciągów zmodyfikowanych istnieją funkcje Boolowskie liniowe

$$F(x_0,x_1,\ldots,x_{n-1}) = x_0 + c_1c_1 + \ldots + c_{n-1}x_{n-1}, \tag{4}$$

gdzie $c_i \in \mathbb{F}_2$ dla $i = 1,\ldots,n-1$, które generują ciągi binarne o maksymalnym okresie 2^n-1. Warunkiem dostatecznym jest aby wielomian jednej zmiennej

$$\varphi(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1x + 1 \tag{5}$$

był wielomianem pierwotnym w pierścieniu $\mathbb{F}_2[x]$. Wielomiany pierwotne określone są jako takie, których pierwiastki (miejsca zerowe: $\varphi(x) = 0$)

w ciele Galois $GF(2^n)$ są elementami pierwotnymi (generatorami) grupy multiplikatywnej $GF(2^n)^*$. Liczba wszystkich wielomianów pierwotnych stopnia n równa jest

$$\frac{\varphi(2^n-1)}{n}, \tag{6}$$

gdzie $\varphi(.)$ oznacza funkcję Eulera. Liczba ze wzoru (6) dla ustalonej wartości n jest znacznie mniejsza niż liczba (2) wszystkich zmodyfikowanych ciągów de Bruijna (generowanych przez funkcje Boolowskie liniowe i nieliniowe). Ciągi o maksymalnym okresie 2^n-1 generowane przez funkcje liniowe postaci (4) zwane są w literaturze m-ciągami, a odpowiadające rejestry nazywane są maksymalnymi liniowymi rejestrami ze sprzężeniem zwrotnym. Teoria m-ciągów jest dobrze ugruntowana matematycznie; w szczególności wiadomo jak konstruować wielomiany pierwotne (a zatem jak generować m-ciągi) dla dowolnego stopnia n. Powyższe fakty omawiane są szeroko w literaturze [13, 19]. Natomiast teoria nieliniowych rejestrów przesuwnych (*NFSR*) jest znacznie mniej rozbudowana. W zasadzie brak jest algorytmów, które pozwalałyby efektywnie konstruować, dla możliwie dużych wartości rzędu n, funkcje Boolowskie dogodne w implementacji generujące zmodyfikowane ciągi de Bruijna.

3. Skrzyżowane pary stanów

Przedstawimy teraz pewną technikę konstruowania nowych *NFSR* o maksymalnym okresie 2^n lub 2^n-1 z danego rejestru (liniowego lub nieliniowego) generującego ciąg o maksymalnym okresie. Technika ta wykorzystuje istnienie tzw. skrzyżowanych par stanów (*ang. cross-join pairs*). Wpierw przedstawimy sposób łączenia lub rozłączania cykli stanów generowanych przez nieosobliwe rejestry przesuwne.

Niech S_i, $i=0,\ldots,2^n-1$, $S_i \in \mathbb{F}_2^n$, będzie ciągiem stanów generowanych przez rejestr opisany funkcją Boolowską f postaci (1). Niech

$$S_i = (x_0, x_1, \ldots, x_{n-1})$$

będzie wybranym stanem tego rejestru. Stan

$$\hat{S}_i = (\widehat{x_0}, x_1, \ldots, x_{n-1}),$$

gdzie $\widehat{x_0} = x_0 + 1$, nazywamy stanem sprzężonym do stanu S_i. Jeśli para stanów S_i, $\hat{S}_i$ leży na jednym cyklu generowanym przez rejestr opisany

funkcją f, to zamieniając między sobą stany następujące po S_i i $\hat{S}_i$ otrzymamy dwa nowe cykle. Operacja ta związana jest z zanegowaniem funkcji F w punkcie $(x_1, \ldots, x_{n-1})$. Jeśli taka para stanów S_i, $\hat{S}_i$ leży na dwóch cyklach generowanych przez rejestr przesuwny, to podobna operacja prowadzi do połączenia tych cykli.

Definicja 3. Dwie pary stanów sprzężonych nieosobliwego rejestru przesuwnego określonego przez funkcję sprzężenia f :

$$\alpha = (a_0, a_1, \ldots, a_{n-1}), \quad \widehat{\alpha} = (\overline{a}_0, a_1, \ldots, a_{n-1}),$$

$$\beta = (b_0, b_1, \ldots, b_{n-1}), \quad \widehat{\beta} = (\overline{b}_0, b_1, \ldots, b_{n-1}),$$

stanowią skrzyżowaną parę stanów dla ciągu generowanego przez ten rejestr, jeśli stany te pojawiają się w kolejności $\alpha, \beta, \widehat{\alpha}, \widehat{\beta}$ w czasie generacji tego ciągu.

Twierdzenie 2. *Niech (s_t) będzie ciągiem de Bruijna spełniającym rekurencję (3). Niech*

$$(u, U), (v, V), \quad (\widehat{u}, U), (\widehat{v}, V)$$

będzie skrzyżowaną parą stanów dla ciągu (s_t) i niech $G(x_1, \ldots, x_{n-1})$ będzie otrzymana z $F(x_1, \ldots, x_{n-1})$ przez zanegowanie wartości $F(U)$ i $F(V)$. Wtedy $G(x_1, \ldots, x_{n-1})$ generuje ciąg de Bruijna *(u_t). Mówimy, że ciąg (u_t) jest otrzymany z ciągu (s_t) przez operację łączenia skrzyżowanych par.*

4. Konstrukcja ciągów de Bruijna

Twierdzenie 3. *Niech (u_t), (v_t) będą różnymi ciągami de Bruijna rzędu n. Wtedy ciąg (v_t) może być otrzymany z ciągu (u_t) przez wielokrotne zastosowanie operacji łączenia skrzyżowanych par.*

Ponieważ istnieje wzajemnie jednoznaczna odpowiedniość między ciągami de Bruijna rzędu n, które mają okres 2^n, a zmodyfikowanymi ciągami de Bruijna tego samego rzędu, które mają okres $2^n - 1$, to Twierdzenie 3 jest również prawdziwe dla ciągów zmodyfikowanych. Jako bezpośredni wniosek z Twierdzenia 3 otrzymujemy następujący:

Lemat 1. *Dla każdego ciągu de Bruijna (zmodyfikowanego ciągu de Bruijna) istnieje para skrzyżowanych stanów.*

W pracy Hellesetha i Kløve [16] zostało wykazane, że liczba różnych skrzyżowanych par stanów dla m-ciągów rzędu n jest równa

$$(2^{n-1}-1)(2^{n-1}-2)/6. \tag{7}$$

Dla zmodyfikowanych ciągów de Bruijna rzędu n generowanych przez *NFSR* nie mamy dokładnych wzorów na liczbę różnych skrzyżowanych par, ale przeprowadzone eksperymenty dla małych rzędów $n = 4, 5, 6$ wskazują, że liczby te są bliskie wartości (7) dla danego rzędu n. Algebraiczna postać normalna (*ANF*) funkcji sprzężenia zwrotnego danego ciągu de Bruijna rzędu n jest różna od takiej funkcji dla odpowiadającego zmodyfikowanego ciągu de Bruijna. Jeśli $f(x_0, x_1, \ldots, x_{n-1})$ jest funkcją generującą zmodyfikowany ciąg de Bruijna rzędu n, wtedy funkcja sprzężenia dla odpowiadającego ciągu de Bruijna jest równa

$$f(x_0, x_1, \ldots, x_{n-1}) + \bar{x}_1\bar{x}_2\cdots\bar{x}_{n-1}. \tag{8}$$

Po obliczeniu

$$\bar{x}_1\bar{x}_2\cdots\bar{x}_{n-1} = (x_1+1)(x_2+1)\cdots(x_{n-1}+1) \tag{9}$$

otrzymujemy, że *ANF* funkcji (8) zawiera składnik $x_1x_2\cdots x_{n-1}$, który ma stopień algebraiczny $n-1$. W ogólności funkcje Boolowskie reprezentujące ciągi de Bruijna rzędu n mają stopień $n-1$; wtedy wyrażenie (9) dla stanu zerowego $(0, \ldots, 0)$ równe jest 1. Natomiast funkcje sprzężenia reprezentujące zmodyfikowane ciągi de Bruijna mają stopień algebraiczny co najwyżej $n-2$, ale mogą mieć też mniejszy stopień algebraiczny. W praktycznych zastosowaniach w kryptografii interesuje nas znalezienie *NFSR* generujących zmodyfikowane ciągi de Bruijna, dla których funkcje sprzężenia mają niski stopień algebraiczny i możliwie małą liczbę składników.

5. Zastosowania Twierdzenia 3

W paragrafie tym będziemy rozpatrywali zmodyfikowane ciągi de Bruijna i odpowiadające im funkcje Boolowskie sprzężenia zwrotnego. Niech $f(x_0, x_1, \ldots, x_{n-1})$ będzie taką funkcją generującą zmodyfikowany ciąg de Bruijna rzędu n. Niech $\alpha, \beta, \hat{\alpha}, \hat{\beta}$ będzie skrzyżowaną parą stanów dla tego ciągu, gdzie

$$\alpha = (a_0, a_1, \ldots, a_{n-1}), \quad \beta = (b_0, b_1, \ldots, b_{n-1}).$$

Wtedy funkcja

$$f(x_0, x_1, \ldots, x_{n-1}) + (x_1 + \bar{a}_1) \cdots (x_{n-1} + \bar{a}_{n-1}) + (x_1 + \bar{b}_1) \cdots (x_{n-1} + \bar{b}_{n-1})$$

generuje nowy zmodyfikowany ciąg de Bruijna rzędu n powstały z ciągu wyjściowego przez zastosowanie operacji łączenia skrzyżowanych par stanów.

5.1. NFSR rzędu 4

Konstrukcja wszystkich funkcji Boolowskich, które generują zmodyfikowane ciągi de Bruijna rzędu 4 była punktem wyjścia do dalszych badań nad zastosowaniem metody łączenia skrzyżowanych par. Bierzemy funkcje sprzężeń dla *LFSR* rzędu 4:

$$x_0 + x_1, \quad x_0 + x_3, \tag{10}$$

które odpowiadają dwóm wielomianom pierwotnym stopnia 4. Każdy z ciągów o okresie 15 generowanych przez funkcje (10) ma zgodnie ze wzorem (7) po 7 różnych par skrzyżowanych stanów. Stosując konstrukcję łączenia par skrzyżowanych stanów otrzymujemy z każdego *LFSR* postaci (10) po 7 nowych *NFSR* wśród których dwie pary są identyczne, czyli otrzymaliśmy łącznie 12 różnych *NFSR*. Wybranie dwóch *NFSR* i znalezienie po jednej skrzyżowanej parze stanów dla każdego z nich pozwala skonstruować brakujące dwa *NFSR* do kompletnej listy 16 funkcji sprzężeń dla zmodyfikowanych ciągów de Bruijna. Poniżej podajemy tą listę z zastosowanymi operacjami algebraicznymi wynikającymi z metody łączenia skrzyżowanych par.

1. $x_0 + x_1$
2. $x_0 + x_3$
3. $x_0 + x_1 + \overline{x}_1 x_2 x_3 + \overline{x}_1 x_2 \overline{x}_3 = x_0 + x_1 + x_2 + x_1 x_2$
4. $x_0 + x_3 + \overline{x}_1 x_2 x_3 + \overline{x}_1 x_2 \overline{x}_3 = x_0 + x_2 + x_3 + x_1 x_2$
5. $x_0 + x_1 + (\overline{x}_1 x_2 x_3 + \overline{x}_1 x_2 \overline{x}_3) + (x_1 x_2 \overline{x}_3 + x_1 \overline{x}_2 x_3) = x_0 + x_1 + x_2 + x_1 x_3$
6. $x_0 + x_3 + (\overline{x}_1 x_2 x_3 + \overline{x}_1 x_2 \overline{x}_3) + (x_1 x_2 \overline{x}_3 + x_1 \overline{x}_2 x_3) = x_0 + x_2 + x_3 + x_1 x_3$
7. $x_0 + x_3 + \overline{x}_1 x_2 \overline{x}_3 + \overline{x}_1 \overline{x}_2 x_3 = x_0 + x_2 + x_1 x_2 + x_1 x_3$
8. $x_0 + x_1 + \overline{x}_1 x_2 \overline{x}_3 + \overline{x}_1 \overline{x}_2 x_3 = x_0 + x_1 + x_2 + x_3 + x_1 x_2 + x_1 x_3$
9. $x_0 + x_1 + x_1 x_2 \overline{x}_3 + \overline{x}_1 x_2 \overline{x}_3 = x_0 + x_1 + x_2 + x_2 x_3$
10. $x_0 + x_3 + x_1 x_2 \overline{x}_3 + \overline{x}_1 x_2 \overline{x}_3 = x_0 + x_2 + x_3 + x_2 x_3$
11. $x_0 + x_1 + \overline{x}_1 x_2 x_3 + x_1 x_2 \overline{x}_2 = x_0 + x_1 + x_1 x_2 + x_2 x_3$
12. $x_0 + x_1 + x_1 \overline{x}_2 \overline{x}_3 + \overline{x}_1 \overline{x}_2 x_3 = x_0 + x_3 + x_1 x_2 + x_2 x_3$

13. $x_0 + x_1 + x_1\overline{x}_2\overline{x}_3 + \overline{x}_1x_2\overline{x}_3 = x_0 + x_2 + x_1x_3 + x_2x_3$
14. $x_0 + x_3 + x_1\overline{x}_2\overline{x}_3 + x_1\overline{x}_2x_3 = x_0 + x_1 + x_2 + x_3 + x_1x_3 + x_2x_3$
15. $x_0 + x_1 + x_1\overline{x}_2x_3 + \overline{x}_1x_2\overline{x}_3 = x_0 + x_1 + x_2 + x_1x_2 + x_1x_3 + x_2x_3$
16. $x_0 + x_3 + x_1\overline{x}_2x_3 + \overline{x}_1x_2\overline{x}_3 = x_0 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3$

Rysunek 1 ilustruje graficznie drogę konstruowania 14 *NFSR* rzędu 4 zaczynając od dwóch *LFSR* tego rzędu. Natomiast Rysunek 2 przedstawia drogę konstruowania 14 różnych *NFSR* i jednego *LFSR* startując z drugiego *LFSR*; w szczególności dwukrotne zastosowanie operacji łączenia skrzyżowanych par stanów prowadzi od jednego *LFSR* do drugiego. Podobnych sposobów otrzymania wszystkich rejestrów maksymalnego rzędu opisanych przez grafy z Rysunków 1 i 2 jest wiele; zależy to od losowego wyboru skrzyżowanych par stanów dla poszczególnych rejestrów. W celu otrzymania funkcji sprzężenia zwrotnego generujących ciągi de Bruijna (w tym przykładzie dla $n = 4$) należy do każdego ze wzorów 1-16 z powyższej listy dodać wyrażenie algebraiczne

$$\bar{x}_1\bar{x}_2\bar{x}_3 = (x_1 + 1)(x_2 + 1)(x_3 + 1),$$

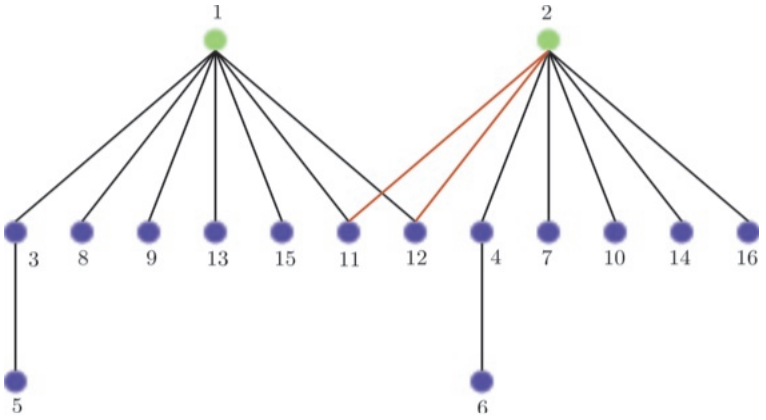
które odpowiada połączeniu cyklu o długości 15 z cyklem o długości 1 reprezentowanym przez stan (0,0,0,0). Otrzymamy wtedy listę wszystkich funkcji Boolowskich sprzężenia zwrotnego generujących ciągi de Bruijna rzędu 4 (odpowiednio o okresie 16).

Na każdym z grafów z Rysunków 1 i 2 możemy znaleźć drogę z dowolnego wierzchołka do każdego innego wierzchołka. Na przykładzie ciągów de Bruijna rzędu 4 mamy potwierdzenie tezy Twierdzenia 3. Wykonano również podobne obliczenia dla zmodyfikowanych ciągów de Bruijna rzędu 5, gdzie mamy $2^{11} = 2048$ nierównoważnych cyklicznie ciągów. Wygenerowano programowo wszystkie funkcje Boolowskie od 5 zmiennych, które są funkcjami sprzężenia zwrotnego dla rejestrów generujących te ciągi. W tym celu wykorzystano pakiet *SAGE* [30] i programowanie w języku *Python* [29].

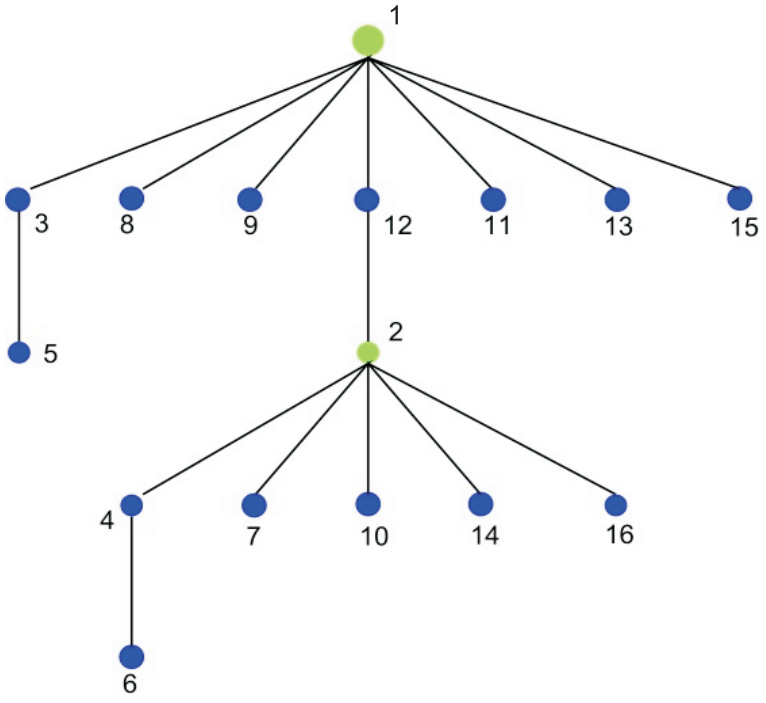
5.2. NFSR rzędu 7

Podamy konstrukcję nieliniowego rejestru rzędu 7 o prostej algebraicznej postaci normalnej wychodząc od rejestru liniowego i stosując metodę łączenia skrzyżowanych par stanów. Weźmy wielomian pierwotny stopnia 7 równy

$$p(x) = x^7 + x + 1.$$



Rysunek 1. Konstrukcja NFSR z dwóch *LFSR*



Rysunek 2. Konstrukcja NFSR i jednego *LFSR* z drugiego *LFSR*

Funkcja sprzężenia zwrotnego dla odpowiadającego *LFSR* równa jest $x_0 + x_6$. Bierzemy stan początkowy rejestru

$$s_0 = (x_0, x_1, \ldots, x_6) = (1, 0, \ldots, 0)$$

i generujemy wszystkie niezerowe stany tego rejestru $s_1, \ldots, s_{126}$. Rozpatrzmy stany dla których $x_2 = 1$ oraz $x_4 = 0$, których jest razem 32. Stany te zawierają 8 skrzyżowanych par stanów (po 4 stany w każdej parze), które łącznie pokrywają stany z warunkiem $(x_2, x_4) = (1, 0)$. Poniżej mamy listę tych skrzyżowanych par $(\alpha, \hat{\alpha}, \beta, \hat{\beta})$:

$$(10, 29; 17, 101),\ (20, 58; 21, 91),\ (25, 47; 32, 62),\ (37, 118; 113, 125),$$

$$(38, 107; 71, 119),\ (42, 55; 50, 94),\ (59, 82; 81, 90),\ (65, 97; 70, 106),$$

gdzie zastosowaliśmy reprezentację dziesiętną dla każdego stanu. Zastosowanie operacji łączenia skrzyżowanych par oddzielnie do każdej z tych 8 par, co jest możliwe, ponieważ wszystkie stany są rozłączne, prowadzi do konstrukcji *NFSR* rzędu 7:

$$\begin{aligned} f = {} & x_0 + x_6 + x_1x_2x_3\overline{x}_4x_5\overline{x}_6 + \overline{x}_1x_2\overline{x}_3\overline{x}_4x_5x_6 + \overline{x}_1x_2x_3\overline{x}_4\overline{x}_5x_6 \\ & + x_1x_2\overline{x}_3\overline{x}_4x_5x_6 + x_1x_2x_3\overline{x}_4x_5x_6 + \overline{x}_1x_2\overline{x}_3\overline{x}_4x_5\overline{x}_6 + \overline{x}_1x_2x_3\overline{x}_4\overline{x}_5\overline{x}_6 \\ & + \overline{x}_1x_2\overline{x}_3\overline{x}_4\overline{x}_5\overline{x}_6 + x_1x_2\overline{x}_3\overline{x}_4\overline{x}_5x_6 + x_1x_2\overline{x}_3\overline{x}_4\overline{x}_5\overline{x}_6 + \overline{x}_1x_2x_3\overline{x}_4x_5x_6 \\ & + \overline{x}_1x_2x_3\overline{x}_4x_5\overline{x}_6 + x_1x_2\overline{x}_3\overline{x}_4x_5\overline{x}_6 + x_1x_2x_3\overline{x}_4\overline{x}_5x_6 + \overline{x}_1x_2\overline{x}_3\overline{x}_4\overline{x}_5x_6 \\ & + x_1x_2x_3\overline{x}_4\overline{x}_5\overline{x}_6 = x_0 + x_6 + x_2 + x_2x_4. \end{aligned}$$

Otrzymaliśmy funkcję sprzężenia zwrotnego, która określa rejestr generujący zmodyfikowany ciąg de Bruijna o okresie $2^7 - 1 = 127$.

5.3. Pewne warunki konieczne

Wzorując się na podanym wyżej przykładzie sformułujemy pewne warunki na funkcję Boolowską od $n-1$ zmiennych, które mogą prowadzić do konstrukcji funkcji sprzężenia nieliniowego rejestru rzędu n, który generuje zmodyfikowany ciąg de Bruijna.

Rozpatrzmy przyszłą funkcję sprzężenia dla *NFSR* o maksymalnym okresie $2^n - 1$, która ma postać

$$f(x_0, x_1, \ldots, x_{n-1}) = g(x_0, x_1, \ldots, x_{n-1}) + h(x_1, \ldots, x_{n-1}), \qquad (11)$$

gdzie g jest funkcją postaci (4) określoną przez wielomian pierwotny stopnia n, zaś h jest funkcją Boolowską możliwie niskiego stopnia algebraicznego z możliwie małą liczbą składników. Liczba wszystkich składników funkcji f musi być parzysta. W naszej konstrukcji musimy znać zbiór S stanów $(x_0, x_1, \ldots, x_{n-1})$ dla których

$$h(x_1, \ldots, x_{n-1}) = 1$$

oraz liczba stanów w S musi być podzielna przez 4. Następnie znajdujemy zbiór J skrzyżowanych par (każda para składa się z czterech stanów) spełniających następujące warunki:

1. Wszystkie elementy zbioru J są rozłączne; żadne dwie pary nie zawierają wspólnych stanów.
2. Wszystkie stany należące do par ze zbioru J pokrywają zbiór S.

Warunki 1 i 2 są warunkami koniecznymi, żeby funkcja (11) generowała ciąg o maksymalnym okresie $2^n - 1$. Przykład zbioru skrzyżowanych par stanów spełniających powyższe warunki był podany w paragrafie 5.2. Warunki 1 i 2 nie są warunkami dostatecznymi na generowanie pełnego okresu przez funkcję f postaci (11). Kiedy te warunki są spełnione musimy dodatkowo sprawdzić, czy funkcja ta generuje ciąg o okresie $2^n - 1$.

W serii prac [12, 7, 9, 10, 14, 17, 18, 20] zastosowano metodę łączenia cykli dla nieosobliwych rejestrów *LFSR* w celu otrzymania ciągów binarnych o maksymalnym okresie generowanych przez *NFSR*. Metoda ta jest obiecująca o ile będziemy mieli kontrolę nad stopniem algebraicznym i ilością składników w algebraicznej postaci normalnej konstruowanych w ten sposób nieliniowych rejestrów przesuwnych. Aktualnie prowadzimy prace w tym zakresie dla wspomnianych wyżej rejestrów PCR_n.

Literatura

[1] S. Babbage, M. Dodd, *"The MICKEY stream ciphers", in New Stream Cipher Designs: The eSTREAM Finalists.* LNCS vol. 4986, pp. 191–209. Springer-Verlag, 2008.

[2] N. G. de Bruijn, *A combinatorial problem*, Indag. Math., 8(1946), pp. 461–467.

[3] A. H. Chan, R. A. Games, J. J. Rushanan, *On the quadratic m-sequences*, Proceedings of Fast Software Encryption, LNCS vol. 809, pp. 166–173. Springer-Verlag, 1994.

[4] C. Canniere, B. Preneel, *"Trivium", in New Stream Cipher Designs: The eSTREAM Finalists*, LNCS vol. 4986, pp. 244–266. Springer-Verlag, 2008.

[5] P. Dąbrowski, G. Łabuzek, T. Rachwalik, J. Szmidt, *Searching for nonlinear feedback shift registers with parallel computing*, Inform. Proc. Letters, 114(2014), pp. 268–272.

[6] E. Dubrova, *A scalable method for constructing Galois NLFSRs with period* $2^n - 1$ *using cross-join pairs*, IEEE Trans. on Inform. Theory, 59(1), 2013, pp. 703–709.

[7] J. C. Fletcher, M. Perlman, *Nonlinear nonsingular feedback shift registers*, United States Patent 3911330, 1975.

[8] C. Flye Sainte-Marie, *Solution to question nr. 48*. L'Intermédiaire des Mathématiciens, 1(1894). pp. 107–110.

[9] H. Fredricksen, *A class of nonlinear de Bruijn cycles*, J. of Combinatorial Theory (A), 19(1975), pp. 192–199.

[10] H. Fredricksen, *A survey of full length nonlinear shift register cycle algorithms*, SIAM Review, 24(2), 1982, pp. 195–221.

[11] B. M. Gammel, R. Goetffert, O. Kniffler, *Achterbahn 128/80*, The eSTREAM project, www.ecrypt.eu.org/stream/, www.matpack.de/achterbahn/

[12] S. W. Golomb, *Shift register sequences*. San Francisco, Holden-Day, 1967, revised edition, Laguna Hills, CA, Aegean Park Press, 1982.

[13] S. W. Golomb, G. Gong, *Signal Design for Good Correlation. For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, 2005.

[14] E. R. Hauge, T. Helleseth, *De Bruijn sequences, irreducible codes and cyclotomy*, Discrete Math., 159(1996), pp. 143–154.

[15] M. Hell, T. Johansson, A. Maximov, W. Meier, *"The Grain Family of Stream Ciphers"*, in New Stream Cipher Designs: The eSTREAM Finalists. LNCS vol. 4986, pp. 179–190. Springer-Verlag, 2008.

[16] T. Helleseth, T. Kløve, *The number of cross-join pairs in maximum length linear sequences*, IEEE Trans. on Inform. Theory, 31(1991), pp. 1731–1733.

[17] F. Hemmati, *A large class of nonlinear shift register sequences*, IEEE Trans. on Inform. Theory, vol. 28, pp. 355-359, 1982.

[18] C. J. A. Jansen, *Investigations on nonlinear streamcipher systems: Construction and evaluation methods*, Ph.D. Thesis, Technical University of Delft, 1989.

[19] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications (Revised Edition)*, Cambridge University Press, Cambridge, 1994.
[20] K. B. Magleby, *The synthesis of nonlinear feedback shift registers*, Technical Report no. 6207-1. Stanford Electronics Laboratories, 1963.
[21] K. Mandal, G. Gong, *Cryptographically strong de Bruijn sequences with large periods*. Selected Areas in Cryptography. L. R. Knudsen, K. Wu (Eds.). LNCS, vol. 7707, pp. 104–118. Springer-Verlag, 2012.
[22] G. L. Mayhew, S. W. Golomb, *Linear spans of modified de Bruijn sequences*, IEEE Trans. Inform. Theory, 36(5), 1990, pp. 1166–1167.
[23] J. Mykkeltveit *Generating and counting the double adjacencies in a pure cyclic shift register*, Trans. on Computers, C-24, 1975, pp. 299–304.
[24] J. Mykkeltveit, M-K. Siu, P. Tong, *On the cyclic structure of some nonlinear shift register sequences*, Inform. and Control, 43(1979), pp. 202–215.
[25] J. Mykkeltveit, J. Szmidt *On cross joining de Bruijn sequences*, Contemporary Mathematics, vol. 632, pp. 333–344, American Mathematical Society, 2015.
[26] T. Rachwalik, J. Szmidt, R. Wicik, J. Zabłocki, *Generation of nonlinear feedback shift registers with special purpose hardware*, Military Communications and Information Systems Conference, MCC 2012, IEEE Xplore Digital Library, 2012, pp. 151–154.
[27] R. Wicik, T. Rachwalik, *Modified alternating step generators*, Military Communications and Information Systems Conference, MCC 2013. IEEE Xplore Digital Library, 2013, pp. 203-215.
[28] M. S. Turan, *On the nonlinearity of maximum-length NFSR feedbacks*, Cryptography and Communications, 4(3-4), 2012, pp. 233-243.
[29] *Python Programming Language*, http://www.python.org
[30] *SAGE Mathematical Software*, Version 5.8. http://www.sagemath.org

NONLINEAR FEEDBACK SHIFT REGISTERS AND JOINING OF CROSS-PAIRS STATES

Abstract. We explain the origins of Boolean feedback functions of Nonlinear Feedback Shift Registers (*NFSR*) of fixed order n generating de Bruijn binary sequences. They all come into existence by cross joining operations starting from one maximum period feedback shift register, e.g., a linear one which always exists for any order n. The result obtained yields some constructions of *NFSR* generating maximum period $2^n - 1$ binary sequences.

Keywords: nonlinear feedback shift registers, de Bruijn sequencec, method of joining of cross-pairs states.