ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ՏԵՂԵԿԱԳԻՐ
ИЗВЕСТИЯ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

Տեխնիկական գիտություններ, սերիա XXXVI, № 1, 1983 Серия технических наук

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

С. С. МУСАЕЛЯН

ПОСТРОЕНИЕ НЕЛИНЕЙНЫХ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАКСИМАЛЬНОЙ ДЛИНЫ

I. *Введение.* Последовательностью де Брейна или нелинейной последовательностью максимальной длины [1] называют двоичную последовательность $\{a_i\}$ периода 2^n, в которой всевозможные векторы $a_j, a_{j-1}, \ldots, a_{j-n+1}$ длины n при любом j встречаются только один раз. Существование таких последовательностей для любого n было показано де Брейном [2], который доказал, что связный ориентированный граф с 2^n вершинами, каждая из которых имеет два входящих и два выходящих ребра, насчитывает $N = 2^{2^{n-1}-n}$ различных путей обхода максимальной длины.

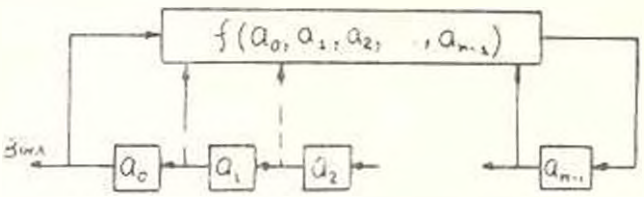

Рис. 1. n-каскадный регистр сдвига с обратной связью.

С другой стороны n-каскадный регистр сдвига с обратной связью, изображенный на рис. 1, порождает рекуррентные последовательности, максимальный период которых равен 2^n. В этом случае исчерпываются всевозможные состояния регистра. Пути прохождения состояний могут быть различными и, согласно вышесказанному, их число равно N. Различным последовательностям соответствуют различные функции обратной связи регистра сдвига. В [1, 3] приводятся некоторые алгоритмы построения лексикографически упорядоченной последовательности де Брейна и ее модификаций без описания функций обратной связи.

В данной работе предлагаются способы построения функций обратной связи n-каскадного регистра сдвига, позволяющие охватить широкий класс последовательностей де Брейна.

II. *Основные понятия.* Пусть обратная связь n-каскадного регистра сдвига описывается булевой функцией $f(a_0, a_1, \ldots, a_{n-1})$,

где $a_i \in B = \{0, 1\}$. При подаче токового импульса в регистре происходит смена состояний. Старое значение вектора заполнения $a = (a_0, a_1, \ldots, a_{n-1}) \in B^n$ заменяется новым $b = (b_0, b_1, \ldots, b_{n-1}) \in B^n$ посредством оператора $F: B^n \to B^n$, $b = Fa$, где

$$b_0 = a_1, \quad b_1 = a_2, \ldots, b_{n-2} = a_{n-1}, \quad b_{n-1} = f(a_0, a_1, \ldots, a_{n-1}). \qquad (1)$$

Нас будут интересовать только циклические последовательности, т. е. случай, когда множество всевозможных значений B^n разбивается на непересекающиеся, циклические замкнутые подмножества без каких-либо ветвлений. В [1] доказано, что выходная последовательность n-каскадного регистра сдвига является циклической только тогда, когда функция обратной связи имеет вид:

$$f(a_0, a_1, \ldots, a_{n-1}) = a_0 \oplus g(a_1, a_2, \ldots, a_{n-1}). \qquad (2)$$

При этом $Fa = Fb$ тогда, когда $a = b$. В дальнейшем циклически замкнутые подмножества B^n будем называть циклами.

Определение 1. [4] Векторы $a = (a_0, a_1, \ldots, a_{n-1})$ и $\bar{a} = (\bar{a}_0, a_1, \ldots, a_{n-1})$ называются сопряженными, если $\bar{a}_i = a_i \oplus 1$.

Теорема 1. [4] Цикл C можно разложить на два цикла C_1 и C_2, если поменять местами векторы, следующие за парой сопряженных векторов a и $\bar{a}$, принадлежащих C. И наоборот, C_1 и C_2 можно объединить в цикл C, если поменять местами векторы, следующие за парой сопряженных векторов $a \in C_1$ и $\bar{a} \in C_2$.

Теорему 1 поясняет граф состояний регистра сдвига с функцией обратной связи $f(a_0, a_1, a_2) = a_0 \oplus a_1 \oplus a_2 \oplus 1$, изображенный на рис. 2а. Граф состоит из двух циклов длины 4, в которых пара векторов (001) и (010) одного цикла имеют в другом цикле сопряженные векторы (101) и (110), соответственно. Меняя местами векторы, следующие за сопряженной парой, скажем (010) и (110), получаем цикл длины восемь, граф состояний которого представлен на рис. 2б. Теперь сопряженные векторы (001) и (101) принадлежат уже одному циклу, и если поменять местами следующие за ними векторы, то получатся два цикла длины шесть и длины два, граф состояний которых представлен на рис. 2в.

Эффект замены векторов, следующих за сопряженными парами, достигается прибавлением к уравнению обратной связи (2) дополнительного члена, который принимает значение 1 только для выбранной пары сопряженных векторов, а во всех остальных случаях равен нулю. Уравнение обратной связи примет вид:

$$h(a_0, a_1, \ldots, a_{n-1}) = a_0 \oplus g(a_1, a_2, \ldots, a_{n-1}) \oplus a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_{n-1}^{\alpha_{n-1}}, \qquad (3)$$

где $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) \in B^{n-1}$, а a_i^1 и a_i^0 равны a_i и $\bar{a}_i$, соответственно. Из (3) видно, что $h(a)$ отличается от $f(a)$ только для сопряженных

векторов $a = (a_0, a_1, \ldots, a_{n-1})$ и $\bar{a} = (\bar{a}_0, a_1, \ldots, a_{n-1})$, что позволяет делать необходимую замену не затрагивая остальные векторы.

Определение 2. Цикл, порожденный n-каскадным регистром сдвига с обратной связью (2), будем называть неполным, если его длина меньше чем 2^n.

Теорема 2. Любой неполный цикл содержит хотя бы один вектор, сопряженный к которому находится вне заданного цикла.

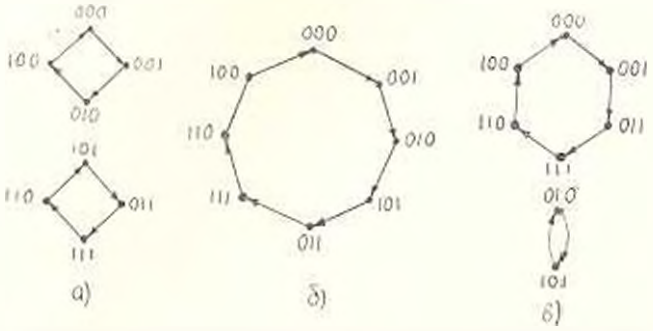

Рис. 2. Графы состояний регистра сдвига с обратной связью до и после замены векторов, следующих за сопряженными парами.

Доказательство. Допустим, что неполный цикл состоит только из векторов $a = (a_0, a_1, \ldots, a_{n-1}) \in B^n$, чьи сопряженные находятся в том же цикле. Для сопряженных векторов a и $\bar{a}$ справедливы следующие соотношения:

$$f(a) = a_0 \oplus g(a_1, a_2, \ldots, a_{n-1}) = a_n;$$
$$f(\bar{a}) = a_0 \oplus 1 \oplus g(a_1, a_2, \ldots, a_{n-1}) = \bar{a}_n = a_n \oplus 1. \qquad (4)$$

Определим векторы, следующие за произвольной парой сопряженных векторов $a = (a_0, a_1, \ldots, a_{n-1})$ и $\bar{a} = (\bar{a}_0, a_1, \ldots, a_{n-1})$. Согласно (1) и (4) этими векторами будут $a_1, a_2, \ldots, a_{n-1}, a_n$ и $a_1, a_2, \ldots, a_{n-1}, \bar{a}_n$ и без ограничения общности можно принять $a_n = 1$, $\bar{a}_n = 0$. Эти векторы отличаются только в последнем символе и, согласно нашему допущению должны иметь сопряженные в том же цикле, совместно с которыми снова порождают две пары векторов. Нетрудно заметить, что все четыре полученных вектора различны. Действительно, векторы каждой пары, например $a_2, a_3, \ldots, a_{n-1}, 1,1$ и $a_2, a_3, \ldots, a_{n-1}, 1,0$, отличаются друг от друга в последнем символе, т. к. порождены парой сопряженных векторов $a_1, a_2, \ldots, a_{n-1}, 1$ и $\bar{a}_1, a_2, \ldots, a_{n-1}, 1$, а от векторов другой пары $a_2, a_3, \ldots, a_{n-1}, 0,1$ и $a_2, a_3, \ldots, a_{n-1}, 0,0$ они отличаются в $n-1$-ом символе в силу того, что их предшественники отличались в n-ом символе. Эти четыре вектора совместно со своими сопряженными порождают 2^3 различных вектора и т. д. Таким образом, рассмотренный цикл должен содержать 2^{n-1} различных

векторов, совпадающих в первом символе, которые совместно со своими сопряженными представляют 2^n различных вектора, принадлежащих циклу. Получили противоречие, т. е. цикл, состоящий только из пар сопряженных векторов, который должен иметь максимальную длину, что доказывает теорему.

Следствие. Циклы, на которые разбивается множество B^n порождаемые n-каскадным регистром сдвига с обратной связью, всегда можно объединить в цикл максимальной длины.

III. *Построение циклов максимальной длины.* Рассмотрим построение циклов максимальной длины для случаев, когда неполные циклы, объединяемые в цикл длины 2^n, порождены n-каскадным регистром сдвига с линейной обратной связью.

1. Пусть имеется примитивный полином степени n

$$p(x) = \sum_{i=0}^{n} p_i x^i,$$

коэффициенты p_i которого принадлежат полю $GF(2)$ и $p_0 = p_n = 1$. Известно [5], что рекуррентное соотношение

$$a_n = f(a_0, a_1, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} p_i a_i, \qquad (5)$$

соответствующее этому полиному, порождает два неполных линейных цикла длины $T_1 = 2^n - 1$ и $T_2 = 1$. Число примитивных над $GF(2)$ полиномов степени n есть $\varphi(2^n - 1)/n$, где φ — функция Эйлера. Для получения циклов длины 2^n ко всем циклам длины T_1, соответствующим этим полиномам, необходимо присоединить нулевой вектор (цикл длины T_2) $00\ldots0$, сопряженный к которому будет $10\ldots0$. Выражение (5) примет вид:

$$a_n = h(a_0, a_1, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} p_i a_i \oplus \bar{a}\bar{a}_2 \ldots \bar{a}_{n-1}.$$

2. Пусть далее $z(x) = p_1(x)\,p_2(x)$ — полином степени n, где $p_1(x)$ и $p_2(x)$ примитивные полиномы с взаимно простыми степенями n_1 и n_2 ($n_1 > n_2 > 0$) и коэффициентами из $GF(2)$.

Утверждение 1. Циклы, порожденные n-каскадным регистром сдвига ($n = n_1 + n_2$), обратная связь которого описывается полиномом $z(x)$, можно объединить $[(2^{n_1} - 1)(2^{n_2} - 1) - 1]$ способами в различные циклы длины 2^n.

Случай, когда обратная связь n-каскадного регистра сдвига описывается полиномом $z(x)$, рассмотрен в [6], где показано, что множество векторов B^n разбивается на непересекающиеся подмножества B_1^n, B_2^n, $B_{1,2}^n$ и 0, каждое из которых представляет собой неполный цикл длины $T_1 = 2^{n_1} - 1$, $T_2 = 2^{n_2} - 1$, $T_{1,2} = (2^{n_1} - 1)(2^{n_2} - 1)$ и 1,

соответственно. Согласно следствию теоремы 2 эти циклы можно объединить в цикл длины 2^n. Покажем, что циклы длины T_1 и T_2 не имеют ни одного вектора, сопряженный к которому находится в том же цикле. Действительно, последовательности этих циклов должны удовлетворять рекуррентным соотношениям:

$$a_{n_1} = \sum_{i=0}^{n_1-1} p_{1_i} a_i \quad \left(p_1(x) = \sum_{i=0}^{n_1} p_{1_i} x^i\right); \tag{6}$$

$$a_{n_2} = \sum_{i=0}^{n_2-1} p_{2_i} a_i \quad \left(p_2(x) = \sum_{i=0}^{n_2} p_{2_i} x^i\right). \tag{7}$$

Но ни одна пара сопряженных векторов $a_0, a_1, \ldots, a_{n_1}, \ldots, a_{n_1}, \ldots, a_{n-1}$ и $\bar{a}_0, \ldots, a_{n_2}, \ldots, a_{n_1}, \ldots, a_{n-1}$ не удовлетворяет соотношениям (6) или (7). Следовательно, ни один из векторов циклов длины T_1 и T_2 не имеют сопряженного вектора в своем цикле. Определим местонахождение векторов, сопряженных к векторам этих циклов. В силу взаимной простоты степеней n_1 и n_2 векторы цикла длины $T_{1,2}$ являются результатом сложения по mod 2 всевозможных пар векторов, один из которых принадлежит циклу длины T_1, а другой — циклу длины T_2. Заметим, что вектор 100 ... 0 принадлежит циклу длины $T_{1,2}$, т. к. он не удовлетворяет ни одному из соотношений (6) и (7). С другой стороны он является результатом сложения по модулю два одной (сопряженной) пары векторов из циклов длины T_1 и T_2. Следовательно, все векторы этих циклов, кроме одного в каждом, имеют сопряженные векторы в цикле длины $T_{1,2}$. Откуда следует, что все три цикла совместно с нулевым (0,0 ... 0) можно объединить в цикл максимальной длины $|(2^{n_1}-1)\cdot(2^{n_2}-1)-1|$ способами.

Пусть число пар взаимно простых чисел, сумма которых равна n, есть l, т. е.

$$n_{1_i} + n_{2_i} = n, \ (n_{1_i}, n_{2_i}) = 1, \qquad i = 1, 2, \ldots, l,$$

тогда число различных полиномов $z(x)$ будет:

$$S = \sum_{i=1}^{l} \frac{\varphi(2^{n_{1_i}}-1)}{n_{1_i}} \cdot \frac{\varphi(2^{n_{2_i}}-1)}{n_{2_i}}. \tag{8}$$

Утверждение 2. Различным полиномам $z(x)$ из числа S в (8), описывающим обратную связь n-каскадного регистра сдвига, соответствуют различные (непересекающиеся) множества, состоящие из $|(2^{n_1}-1)\cdot(2^{n_2}-1)-1|$ объединенных циклов длины 2^n.

Заметим, что в тех случаях, когда единственная пара сопряженных векторов a и $\bar{a}$, принадлежащая циклам длины T_1 и T_2, не используется для объединения циклов, эти циклы раздельно объединяются с циклом длины $T_{1,2}$, как это условно изображено на рис. 3а. Порядок следования векторов циклов длины T_1 и T_2 в этих случаях не нарушается и все объединенные циклы длины 2^n будут различными. В случаях, когда

векторы a и $\hat{a}$ используются для объединения циклов, циклы длины T_1 и T_2 предварительно объединяются в цикл длины T_1+T_2, который затем присоединяется к циклу длины $T_{1,2}$. Условное изображение такого объединения приведено на рис. 3б. Цикл длины T_1+T_2 состоит из двух участков, описывающихся рекуррентными соотношениями соответствующих полиномов $p_1(x)$ и $p_2(x)$. Поэтому различным полиномам соответствуют различные циклы длины T_1+T_2, а следовательно различные циклы максимальной длины. Таким образом, во всех случаях различные полиномы из числа S порождают (после объединения циклов) различные множества циклов максимальной длины. При этом каждое из множеств, согласно утверждению 1, насчитывает $|(2^{n_1}-1)\cdot(2^{n_2}-1)-1|$ циклов длины 2^n.

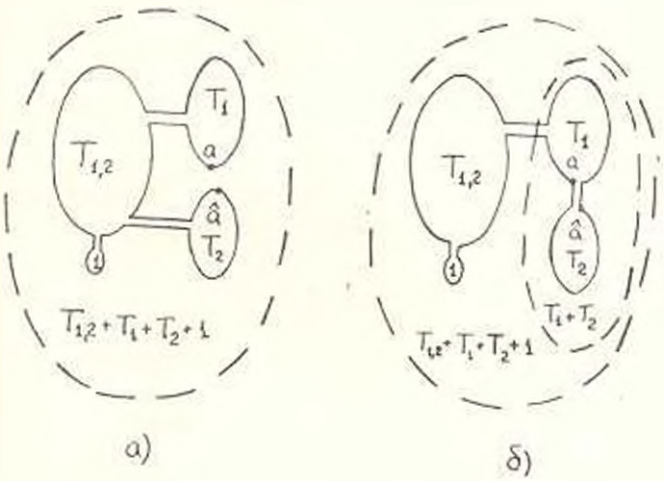

Рис. 3. Условное представление объединения неполных циклов в цикл максимальной длины.

Число циклов длины 2^n, полученных в результате объединения неполных циклов, порожденных n-каскадными регистрами сдвига, обратные связи которых описываются полиномами $z_j(x)$, $j=1, 2, \ldots, S$, есть

$$K=\sum_{i=1}^{t}\frac{\varphi(2^{n_{1_i}}-1)}{n_{1_i}}\cdot\frac{\varphi(2^{n_{2_i}}-1)}{n_{2_i}}\cdot|(2^{n_{1_i}}-1)(2^{n_{2_i}}-1)-1|,$$

а общее число циклов длины 2^n, полученных в разделах 1 и 2, будет:

$$K'=K+\frac{\varphi(2^n-1)}{n}.$$

3. Пары сопряженных векторов a, $\hat{a}$ и b, $\hat{b}$ назовем сцепленными, если в цикле они чередуются в следующем порядке $\ldots a \ldots b \ldots \ldots \hat{a} \ldots \hat{b} \ldots$ С помощью сцепленных пар исходного цикла можно получить новые циклы той же длины.

Пусть число сцепленных пар в цикле длины $T_{1,2}$ для каждого $z_j(x)$, $j = 1, 2, \ldots, S$ равно m_j, тогда общее число циклов длины 2^n будет

$$K^n = \sum_{j=1}^{S}(m_j + 1)\left[(2^{n_{1j}} - 1)(2^{n_{2j}} - 1) - 1\right] + \frac{\varphi(2^n - 1)}{n}.$$

Заключение. Двоичные нелинейные последовательности максимальной длины представляют большой практический интерес, в частности для задач помехоустойчивого кодирования и идентификации. Приведенный метод легко распространяется на случай произведения произвольного числа примитивных полиномов над $GF(2)$ с попарно взаимно простыми степенями.

Ин-т проблем управления
АН СССР

15.VI.1981

Ս. Ս. ՄՈՒՍԱԵԼՅԱՆ

ԵՐԿԱԿԻ ՈՉԳԾԱՅԻՆ ԱՌԱՎԵԼԱԳՈՒՅՆ ԵՐԿԱՐՈՒԹՅԱՄԲ ՀԱՋՈՐԴԱԿԱՆՈՒԹՅՈՒՆՆԵՐԻ ԿԱՌՈՒՑՈՒՄ

Ամփոփում

Առաջարկվում է առավելագույն պարբերությամբ երկուական ոչգծային հաջորդականությունների կառուցման ձև։ Որպես օրինակ դիտարկվում են նման կառուցումներ գծային հաջորդականություններից, որոնք նկարագրվում են մեկ հասարակ բազմանդամով կամ $GF(2)$ *դաշտում երկու հասարակ բազմանդամների արտադրյալով։*

ЛИТЕРАТУРА

1. *Golomb S. W.* Shift register sequences. — San-Francisco: 1967. — 214 p.
2. *de Bruijn N. G.* A combinatorial problem. — Proc. Kon. Ned. Akad. Wetensch., 1946, v. 49, p. 758—764.
3. *Fredricksen H.* A class of nonlinear de Bruijn cycles. — J. Combin. Theory, 1975, 19A, p. 192—199.
4. *Yoeli M.* Counting with nonlinear binary feedback shift registers. — IEEE Tran. Elec. Computers, 1963, v. 12, n. 4, p. 357—361.
5. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976. — 600 с.
6. *Варшамов Р. Р., Тененгольц Г. М.* Об одном классе циклических кодов. — Проблемы кибернетики, 1970, т. 2, с. 157—166.