DOI 10.17223/20710410/2/4
УДК 519.7

ПОСТРОЕНИЕ НОРМАЛЬНЫХ ПЕРИОДИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ИЗ ЦИКЛИЧЕСКИ МИНИМАЛЬНЫХ ЧИСЕЛ

А.Г. Поздеев

Томский государственный университет

E-mail: anatoliy.pozdeev@vitasw.com

Предлагается алгоритм с вычислительной сложностью $O(2^n/n)$, позволяющий по задаваемым значениям параметра путем склеивания циклов, порожденных циклически минимальными числами, строить двоичные нормальные периодические последовательности порядка n так, что при разных значениях параметра с равной вероятностью строятся попарно неэквивалентные последовательности из множества большой мощности. В случае простого n указываются выражения для вычисления последней и размера параметра.

***Ключевые слова*:** *нормальные периодические последовательности*, *последовательности де Брейна*, *циклически минимальные числа.*

Нормальные периодические последовательности (НПП), они же – последовательности де Брейна, они же – нормальные рекуррентные последовательности [1], интересны для криптографии в качестве гамм или ключевых потоков в поточных шифрах. Для этого важно уметь порождать их с равной вероятностью из достаточно большого множества по случайно выбираемым значениям ключевого параметра (ключа). Судя по обзору методов построения НПП [1], к настоящему времени эта проблема еще не нашла удовлетворительного решения и требует дальнейшего исследования. В данной заметке демонстрируется подход к ее решению, основанный на построении НПП путем склеивания циклов, порожденных циклически минимальными числами. Изложению результатов предшествуют необходимые определения и сведения о работах других авторов в этом направлении.

Для любого натурального n элементы в множестве $\{0, 1\}^n$ рассматриваются как булевы векторы (слова) длиной n или как n-значные (двоичные) числа.

Последовательность $s = s_1s_2\ldots$, где $s_i \in \{0, 1\}$ для каждого $i \geq 1$, называется *периодической*, или *циклом*, если для некоторого натурального m и любого $i \geq 1$ в ней $s_{i+m} = s_i$; в этом случае пишут $s = <s_1s_2\ldots s_m>$, а наименьшие m с указанным свойством называют *периодом* последовательности s. Через $W_n(s)$ обозначается множество всех n-значных двоичных чисел, содержащихся в цикле $s = <s_1s_2\ldots s_m>$, а именно: $W_n(s) = = \{s_is_{i+1}\ldots s_{i+n-1}: i = 1, 2, \ldots, m\}$. Наименьшее n, при котором все числа $s_is_{i+1}\ldots s_{i+n-1}$ для $i = 1, 2, \ldots, m$ различны, называется *порядком* цикла s. Цикл порядка n и периода $m = 2^n$ называется *НПП порядка n*. Две НПП $< a >$ и $< b >$ называются *эквивалентными*, если a получается из b некоторым циклическим сдвигом.

Два цикла $a = <a_1a_2\ldots a_m>$ и $b = <b_1b_2\ldots b_r>$ называются *n-смежными*, если они не имеют общего n-значного числа, т.е. $W_n(a) \cap W_n(b) = \varnothing$, но имеют общее $(n-1)$-значное число, т.е. $W_{n-1}(a) \cap W_{n-1}(b) \neq \varnothing$. Результатом *склеивания n-смежных циклов a и b по общему числу* $a_ia_{i+1}\ldots a_{i+n-2} = b_jb_{j+1}\ldots b_{j+n-2}$ в $\{0, 1\}^{n-1}$ является цикл $c = <c_1c_2\ldots c_{m+r}> = <a_1a_2\ldots a_ia_{i+1}\ldots a_{i+n-2}b_{j+n-1}b_{j+n}\ldots b_rb_1b_2\ldots b_jb_{j+1}\ldots b_{j+n-2}a_{i+n-1}a_{i+n}\ldots a_m>$. По построению последнего, период последовательности c равен сумме периодов a и b, $W_n(a) \cup W_n(b) = W_n(c)$ и, как следствие, $W_{n-1}(a) \cup W_{n-1}(b) = W_{n-1}(c)$.

Множество циклов C называется *цикловым разбиением* множества $\{0, 1\}^n$, если различные циклы в нем не имеют общих n-значных чисел и любое n-значное число содержится в некотором цикле из C. Исходя из любого такого множества циклов, можно путем последовательного склеивания n-смежных циклов построить некоторую НПП порядка n. Выбирая разные исходные цикловые разбиения множества $\{0, 1\}^n$ и варьируя порядок выбора циклов и в них общих чисел для склеивания, можно таким способом построить любую из возможных НПП заданного порядка. Впервые этот метод построения НПП предложил А.Н. Радченко [2]. (Его полное изложение можно найти в [1].) Позднее операция склеивания смежных циклов возникала в работах других авторов, в частности в [3 – 6], где с ее помощью НПП заданного порядка строятся рекурсивно из НПП меньшего порядка – склеиванием НПП порядка n в НПП порядка $n+1$ для $n \geq 2$. В [7] представлен алгоритм со сложностью реализации $O(2^n)$ битовых операций, позволяющий таким образом порождать попарно неэквивалентные НПП заданного порядка n, выбирая их из некоторого множества мощности 2^{n-2} с равной вероятностью по значению параметра из множества $\{0, 1\}^{n-2}$.

Пусть далее для $a = a_1\ldots a_n \in \{0, 1\}^n$ и $i \in \{1, 2, \ldots, n\}$ через $a << i$ обозначается результат циклического сдвига числа a на i знаков влево: $(a << i) = a_{i+1}\ldots a_na_1\ldots a_i$. По определению $(a << n) = a$. Число $a \in \{0, 1\}^n$ называется *циклически минимальным*, если $a \leq (a << i)$ для каждого $i = 1, 2, ..., n-1$. Множество всех циклически минимальных чисел в $\{0, 1\}^n$ обозначается далее CM_n.

Ниже показывается, что множество $< CM_n >$ всех циклов $< a >$ для $a \in CM_n$ является цикловым разбиением множества $\{0, 1\}^n$, и предлагается алгоритм с вычислительной сложностью $O(2^n/n)$, позволяющий по значению параметра длиной $(|CM_n|-3)\lceil \log(n-1) \rceil$ бит путем склеивания циклов в $< CM_n >$ в определенном порядке построить некоторую НПП порядка n так, что при разных значениях параметра с равной вероятностью строятся попарно неэквивалентные НПП из множества, мощность которого в случае простого n равна $\prod_{m=1}^{n-1} m^{C_n^m / n}$. Длина параметра в этом случае аппроксимируется числом $2^n(\log n)/n$ бит.

Лемма 1. $\forall a, b \in CM_n\ (a \neq b \Rightarrow \neg\exists\, i \in \{1, 2, \ldots, n\}(a = (b << i)))$.

Доказательство. Предположив противное, будем иметь $b \le (b << i) = a$, $a \le (a << (n-i)) = b$ и $a = b$, что не так. ■

Следствие. $\forall a, b \in CM_n\ (a \neq b \Rightarrow W_n(< a >) \cap W_n(< b >) = \varnothing)$. ■

Лемма 2. $\forall a \in \{0, 1\}^n \exists\, j \in \{1, 2, \ldots, n\}((a << j) \in CM_n)$.

Доказательство. Определим $j \in \{1, 2, \ldots, n\}$ из условия: $(a << j)$ есть минимальное из чисел $(a << i)$ для всех $i \in \{1, 2, \ldots, n\}$. ■

Следствие. $\bigcup_{a \in CM_n} W_n(< a >) = \{0, 1\}^n$. ■

Объединяя утверждения следствий из лемм 1 и 2, получаем следующее

Утверждение 1. $< CM_n >$ есть цикловое разбиение множества $\{0, 1\}^n$. ■

Лемма 3. Пусть $i, j \in \{1, 2, \ldots, n\}$, $a = a_1 \ldots a_{i-1} 1 a_{i+1} \ldots a_n \in \{0, 1\}^n$ и $b = (a_1 a_2 \ldots a_{i-1} 0 a_{i+1} \ldots a_n << j)$. Тогда

1) циклы $< a >$ и $< b >$ n-смежные, и $a_{i+1} \ldots a_n a_1 a_2 \ldots a_{i-1}$ есть их общее $(n-1)$-значное число;

2) $\exists\, j \in \{1, 2, \ldots, n\}(b \in CM_n\ \&\ b < a)$.

Доказательство. 1) $a_{i+1} \ldots a_n a_1 a_2 \ldots a_{i-1} \in W_{n-1}(< a >) \cap W_{n-1}(< b >)$ и, кроме того, $W_n(< a >) \cap W_n(< b >) = \varnothing$, так как вес (число единиц) любого слова в $W_n(< a >)$ на 1 больше веса любого слова в $W_n(< b >)$;

2) по лемме 2 $\exists\, j \in \{1, 2, \ldots, n\}(b \in CM_n)$ и для такого j имеем $b \le (b << n - j) = a_1 a_2 \ldots a_{i-1} 0 a_{i+1} \ldots a_n < a$. ■

Обозначим $w(a)$ вес вектора $a \in \{0, 1\}^n$. Пусть $CM_n = \{r_0, r_1, \ldots, r_k\}$ и $r_0 < r_1 < \ldots < r_k$. Тогда $r_0 = 00\ldots0$, $r_1 = 0\ldots01$ и $r_k = 11\ldots1$. Для любого $t = 0, 1, \ldots, k$ определим r_t' из условий: $< r_t' > = < r_t >$ и длина r_t' есть период последовательности $< r_t >$, и положим $P_t = \{1, 2, \ldots, w(r_t')\}$. В частности, $r_0' = 0$, $r_k' = 1$, $r_1' = r_1$, $P_0 = \varnothing$, $P_1 = \{1\}$, $P_k = \{1\}$. Элементы в $P(n) = P_2 \times \ldots \times P_{k-1}$ будем называть *параметрами*.

Алгоритм *Z*. Выберем произвольный параметр $p = (p_2, \ldots, p_{k-1}) \in P(n)$, положим $p_1 = p_k = 1$ и построим последовательность $s(p)$ как результат последовательного склеивания циклов $< r_0 >, < r_1 >, \ldots, < r_k >$, выполненного по правилу: результат $< s >$ склеивания циклов $< r_0 >, < r_1 >, \ldots, < r_t >$ для каждого $t = 0, 1, \ldots, k-1$ склеивается с циклом $< r_{t+1} >$ по общему числу $\alpha(p_{t+1}) = a_{i+1} \ldots a_n a_1 a_2 \ldots a_{i-1}$, такому, что $r_{t+1} = a_1 \ldots a_{i-1} 1 a_{i+1} \ldots a_n$ и $p_{t+1} = w(a_1 \ldots a_{i-1} 1)$.

Корректность алгоритма *Z*. Нужно убедиться в том, что число $a_{i+1} \ldots a_n a_1 a_2 \ldots a_{i-1}$ действительно общее для циклов $< s >$ и $< r_{t+1} >$. По 2 в лемме 3 найдется $j \in \{1, 2, \ldots, n\}$, что $(a_1 \ldots a_{i-1} 0 a_{i+1} \ldots a_n << j) = b \in CM_n$, $b < r_{t+1}$ и, следовательно, $b = r_l$ для некоторого $l \in \{1, 2, \ldots, t\}$. По 1 в лемме 3 $a_{i+1} \ldots a_n a_1 a_2 \ldots a_{i-1}$ является общим числом циклов $< r_l >$ и $< r_{t+1} >$, поэтому $a_{i+1} \ldots a_n a_1 a_2 \ldots a_{i-1} \in \bigcup_{i=1}^{t} W_{n-1}(< r_i >) = W_{n-1}(< s >)$, и корректность Z доказана.

Ввиду утверждения 1 справедливо

Утверждение 2. Последовательность $s(p)$, порождаемая алгоритмом Z, есть НПП порядка n. ■

Пример. Пусть $n = 3$. Тогда $k = 3$, $r_0 = 000$, $r_1 = 001$, $r_2 = 011$, $r_3 = 111$, $r_0' = 0$, $r_1' = 001$, $r_2' = 011$, $r_3' = 1$, $P_2 = \{1, 2\}$, $P(3) = P_2 = \{1, 2\}$. Следуя алгоритму Z, можно построить две (и это будут все возможные для данного порядка неэквивалентные) НПП: $s(1)$ и $s(2)$. Построим первую. Имеем: $p = p_2 = 1$, $p_1 p_3 = 11$ и $< s > = < r_0 >$. Поскольку $r_1 = a_1 a_2 a_3 = 001$ и $p_1 = 1 = w(001)$, то $i = 3$ и $< s >$ и $< r_1 >$ склеиваются по общему числу $a_1 a_2 = 00$, давая результатом $< s > = <0001>$. Поскольку $r_2 = a_1 a_2 a_3 = 011$ и $p_2 = 1 = w(01)$, то $i = 2$ и $< s >$ и $< r_2 >$ склеиваются по общему числу $a_3 a_1 = 10$, давая результатом $< s > = <0001011>$. Наконец $< s >$ и $< r_3 >$ склеиваются по $a_2 a_3 = 11$, поскольку $r_3 = a_1 a_2 a_3 = 111$, $p_3 = 1 = w(1)$ и $i = 1$. Результатом этого склеивания является НПП $s(1) = <00010111>$. Аналогичным образом строится НПП $s(2)$, а именно: $< r_0 >$ и $< r_1 >$ склеиваются по числу 00 в цикл <0001>, который по 01 склеивается с $< r_2 >$ в цикл <0001101>, который по 11 склеивается с $< r_3 >$ в НПП $s(2) = <00011101>$.

Лемма 4. $p \neq p' \Rightarrow s(p) \neq s(p')$.

Доказательство. Пусть $p = p_2 \ \ldots\ p_{k-1}$ и $p = p'_2 \ \ldots\ p'_{k-1}$. Тогда, по построению в алгоритме Z, имеем $p_{t+1} \neq p'_{t+1} \Rightarrow \alpha(p_{t+1}) \neq \alpha(p'_{t+1}) \Rightarrow s(p) \neq s(p')$. ■

Утверждение 3. НПП, порождаемые алгоритмом Z с различными параметрами, не эквивалентны.

Доказательство. Поскольку НПП, порождаемые алгоритмом Z, начинаются с одного и того же слова – $00\ldots0$, то утверждение верно в силу леммы 4. ■

Лемма 5. Пусть n – простое число и $CM_n = \{r_0, r_1, \ldots, r_k\}$. Тогда

$$| CM_n| = (2^n–2)/n +2 \text{ и } \prod_{t=1}^{k-1} w(r_t) = \prod_{m=1}^{n-1} m^{C_n^m/n} . \quad (1)$$

Доказательство. В соответствии с утверждением 1 множество $\{0, 1\}^n$ при простом n разбивается на k+1 = $|CM_n|$ классов $C_0, C_1, \ldots, C_k$, где $C_0 = \{r_0\}$, $C_k = \{r_k\}$ и C_t для $t = 1, 2, \ldots, k–1$ состоит из n различных чисел ($r_t << j$), $j = 1, 2, ..., n$. Следовательно, для любого $m \in \{1, 2, \ldots, n–1\}$ среди чисел $r_1, \ldots, r_{k–1}$ будет ровно C_n^m/n чисел веса m, и произведение весов последних равно $m^{C_n^m/n}$, поэтому, во-первых, верно второе равенство в (1) и, во-вторых, $|CM_n| = 2 + \sum_{m=1}^{n-1} C_n^m / n = 2 + (2^n–2)/n$. ■

Утверждение 4. Количество всех НПП простого порядка n, порождаемых алгоритмом Z, равно

$$\prod_{m=1}^{n-1} m^{C_n^m/n} .$$

Доказательство. По лемме 4 количество всех НПП, порождаемых Z, равно $|P(n)|$. Пусть n простое. Тогда $r_t = r'_t$ для любого $r_t \in CM_n – \{r_0, r_k\}$ и, так как $w(r_1) =1$, то $|P(n)| = w(r_1)\cdot w(r_2)\cdot\ldots\cdot w(r_{k–1})$. Утверждение следует теперь из второго равенства в (1). ■

Утверждение 5. Для простого n длина параметра в $P(n)$ в битах равна $((2^n–2)/n –1) \lceil \log (n–1) \rceil$ и для большого n аппроксимируется числом $2^n(\log n)/n$.

Доказательство. По определению $P(n)$ длина $L(n)$ элемента $p = (p_2, \ldots, p_{k–1}) \in P(n)$ в битах равна $(k–2)\lceil \log(n–1) \rceil$, где k+1 = $|CM_n|$, поэтому $L(n) = (|CM_n|–3) \lceil \log(n–1) \rceil$. Подставляя сюда при простом n выражение для $|CM_n|$ из (1), получим требуемую формулу. ■

ЛИТЕРАТУРА

1. *Агибалов Г.П.* Нормальные рекуррентные последовательности // Вестник ТГУ. Приложение. 2007. № 23. С. 4 – 11.
2. *Радченко А.Н.* Методы синтеза кодовых колец // Радиотехника и электроника. 1959. № 11. С. 1782 – 1795.
3. *Lempel A.* On a Homomorphism of the De Bruijn Graph and Its Applications to the Design of Feedback Shift Registers // IEEE Trans. Computers. 1970. V. C-19. No. 12. P. 1204 – 1209.
4. *Mykkeltveit J.*, *Siu M.K.*, *Tong P.* On the cycle structure of some nonlinear shift register sequence // Information and Control. 1979. V. 43. P. 202 – 215.
5. *Siu M.K.*, *Tong P.* Generation of some de Bruijn sequences // Discrete Mathematics. 1980. V. 31. P. 97 – 100.
6. *Games R.A.* A generalized recursive construction for de Bruijn sequences // IEEE Trans. Inform. Theory. 1983. V. IT-29. No. 6. P. 843 – 850.
7. *Annexstein F.S.* Generating De Bruijn Sequences: An Efficient Implementation// IEEE Trans. Computers. 1997. V. C-46. No. 2. P. 198 – 200.