УДК 621.391.82

И. И. СНЫТКИН, канд. техн. наук

МЕТОДЫ И АЛГОРИТМЫ ФОРМИРОВАНИЯ СИСТЕМ НЕЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, СУЩЕСТВУЮЩИХ В ПРОСТЫХ ПОЛЯХ ГАЛУА *GF(p)*

В теории ШПС термин «нелинейные рекуррентные последовательности» (НЛРП) относится ко всем кодовым рекуррентным последовательностям (КРП), которые не генерируются посредством регистров сдвига с линейными обратными связями. Вопросы формирования и выбора НЛРП с потенциально неулучшаемыми автокорреляционными свойствами рассматривались в работах [1—5]. Так, в работе [3] изучались вопросы формирования и исследования свойств НЛРП в виде кодов квадратичных вычетов для длительностей $L \leqslant 709$, а в работе [4] — тех же кодов для $L \leqslant 1009$ и характеристических для $L \leqslant 136$. Исследования в этой области были расширены и дополнены рассмотрением вопросов построения систем (или кодовых словарей) данных НЛРП на основе их авто- и изоморфных преобразований [1]. Однако, как показывает практика, формирование и исследование свойств данных НЛРП больших ($L > 1000$) и сверхбольших ($L > 10000$) длительностей чрезвычайно затруднительно, так как используемые методы [1; 3; 4] и процедуры формирования НЛРП не эффективны, трудоемки и требуют больших затрат времени даже с применением самых мощных ЭВМ, уже начиная с $L \geqslant 100$. Это связано с тем, что они, с одной стороны, базируются на использовании таблиц первообразных корней θ по простым модулям p и таблиц индексов простых чисел p [6] для небольшого их числа $p \leqslant 109$, и поэтому трудно алгоритмизируемы, а с другой — связаны с оценкой величины θ', которая даже при $\theta < 10$ и $i > 100$ ($i = \overline{1, L}$) оказывается настолько большой, что с ней нельзя оперировать даже используя самые мощные ЭВМ. Формирование же больших объемов кодовых словарей НЛРП больших, сверхбольших длительностей [2; 5], является актуальной задачей при построении помехозащищенных систем связи с ШПС, особенно специального назначения.

На основе установленных автором и приводимых без доказательств систематических комбинационно-логических соотношений в теории чисел и конечных полей рассматриваются эффективные программные методы и алгоритмы, положенные в основу программного обеспечения ЭВМ, микроЭВМ и микропроцессоров при формировании в реальном масштабе времени систем НЛРП, существующих в простых полях Галуа $GF(p)$, больших и сверхбольших длительностей.

Правила построения НЛРП в полях $GF(p)$. Построение НЛРП нечетной длительности $L = p$ в виде кодов квадратичных вычетов и четной длительности $L = p - 1$ в виде характеристических кодов V базируется на использовании свойств двузначного характера $\psi(\cdot)$ мультипликативной группы $G(p-1)$ полей $GF(p)$ [1]. Так, для первого случая правило имеет вид

$$GF(p) = \{a_i : i = 0,\ 1,\ \ldots,\ p-1\};\ L = p = 4\cdot t + 1,\ 4—t + 3;$$
$$t = 0,\ 1,\ 2\ldots;\ v = \{v_i : i = 0,\ 1,\ \ldots,\ p-1\};$$
$$v_0 = \pm 1,\ v_i = \psi(a_i) = \psi(i),\ i \neq 0 \pmod p, \qquad (1)$$

а для второго — соответственно

$$GF(p) = \{a_i : i = 0,\ 1,\ \ldots,\ p-1\};\ L = p - 1 = 4\cdot t,\ 4\cdot t + 2;$$
$$t = 0,\ 1,\ 2,\ 3\ldots;\ v = \{v_i : i = 0,\ 1,\ \ldots,\ p-2\};$$
$$v_i = \psi(\theta^i + 1),\ \text{при}\ \theta^i + 1 \neq 0 \pmod p;$$
$$v_i = \pm 1,\ \text{при}\ \theta^i + 1 = 0 \pmod p. \qquad (2)$$

Здесь a_i — i-й элемент поля $GF(p)$; θ — первообразный элемент поля $GF(p)$; $\psi(\cdot)$ — характер, который при выполнении условия [6] $a = \theta^u \pmod p$ (3), где u — индекс числа a ($\mathrm{ind}\ a$) по модулю p оценивается как

$$\psi(a) = \exp(j\pi u) = \begin{cases} 1, & u \equiv 0 \pmod 2; \\ -1, & u \equiv 1 \pmod 2. \end{cases} \qquad (4)$$

Как видно из правил (1), (2), соотношений (3), (4) и работы [1], основные трудности построения НЛРП такого типа заключаются непосредственно в вычислении первообразных элементов θ, характеров $\psi(a)$ и индексов u ($\mathrm{ind}\ a$) согласно (3), (4), в определении между u ($\mathrm{ind}\ a$) и номерами i элементов необходимых соответствий согласно (1) и (2).

В дальнейшем вопросы построения НЛРП на основе кодов Якоби и Холла рассматривать не будем, поскольку данные коды — это частный случай оптимальных КРП для весьма ограниченного числа некоторых из длительностей L кодов квадратичных вычетов [1; 7; 8].

Новые положения в теории чисел и теории полей $GF(p)$. Строгие математические доказательства приводимых положений опущены вследствии их громоздкости, с доказательствами можно ознакомиться в работах [7; 8]. Однако справедливость и очевидность данных положений будут продемонстрированы на примере.

Л е м м а 1. *Сумма любого простого числа a (кроме 2) с числом 2 является нечетным несоставным или составным числом, а с любым*

другим простым числом $p>2$ — четным составным числом, т. е. число $(a+p)$ всегда разложимо на простые сомножители

$$x_i : a+p = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n},\ i = \overline{1,\ n}.$$

Лемма 2. *Индекс* ind a *числа* a, *взаимно простого с простым модулем* p *поля* $GF(p)$, $(a,\ p) = 1$ *и* $a < p$, *равен сумме, приведенной по модулю* $(p-1)$ *индексов чисел, разлагающих на сомножители число* $(a+p)$, *т. е.* $\text{ind}\, a \equiv (\text{ind}\, x_1^{\alpha_1} + \text{ind}\, x_2^{\alpha_2} + \ldots + \text{ind}\, x_n^{\alpha_n}) \pmod{(p-1)}$.

Пример: $GF(p=13) = \{0,\ 1,\ 2,\ \ldots,\ 12\}$, $\theta = 2$, $\text{ind}\, 1 = 0$, $\text{ind}\, 2 = 1$, $\text{ind}\, 3 = \text{ind}\,(3+13) = \text{ind}\, 2^4 = 4 \cdot \text{ind}\, 2 = 4$, $\text{ind}\, 4 = \text{ind}\, 2^2 = 2 \cdot \text{ind}\, 2 = 2$, $\text{ind}\, 5 = \text{ind}\,(5+13) = \text{ind}\,(2 \cdot 3^2) = \text{ind}\, 2 + 2 \cdot \text{ind}\, 3 = 9$, ..., и т. д.

Если значения индексов рассчитывать в соответствии с (3), то можно убедиться в справедливости примера и лемм 1, 2. Методика, определяемая леммами 1, 2, исключает необходимость использования, как это делается в работе [1], таблиц индексов простых чисел, приводимых в работе [6], освобождает от трудоемких операций, определяемых выражением (3) и весьма эффективна при ручном формировании НЛРП с $L < 100$.

Лемма 3. *В простых полях* $GF(p)$ *элемент* $a = 1$ *имеет два значения индекса*: 0 и $(p-1)$.

Лемма 4. *Индексом элемента* a_i *мультипликативной группы поля* $GF(p)$ *является число* $(i-1)$, *т. е.* $\text{ind}\, a_i = i-1$, *если* i — *номер элемента* a_i, $i = 1, 2, \ldots, p-1$.

Следствие. Независимо от того, с применением какого именно первообразного элемента θ вычислен элемент мультипликативной группы a_i, имеющий номер i, и какое численное значение он имеет, индекс элемента a_i равен $i-1$.

Лемма 5. *Любой фиксированный элемент* a *мультипликативной группы поля* $GF(p)$ *имеет число* $\varphi(p-1)$ *изоморфных индексов, где* $\varphi(p-1)$ — *функция Эйлера от* $(p-1)$, *разбивающихся на два непересекающихся класса: инверсные и неинверсные.*

Лемма 6. *Если* $c = \varphi(p-1)$, *а* $\theta_1 \equiv \theta_1^1$, $\theta_2 \equiv \theta_1^{k_2} \pmod{p}$, $\theta_3 \equiv \theta_1^{k_3} \pmod{p}$, ..., $\theta_c \equiv \theta_1^{k_c} \pmod{p}$ — *изоморфные первообразные элементы поля* $GF(p)$, *то изоморфные индексы* μ_1, γ_2, ... γ_c *любого фиксированного элемента* a *мультипликативной группы* $G(p-1)$ *и показатели степеней при* θ_1, *т. е.* k_2, k_3, ..., k_c *связаны следующим соотношением:*

$$\gamma_1 \equiv k_2 \cdot \gamma_2 \equiv k_3 \cdot \gamma_3 \equiv \ldots \equiv k_c \cdot \gamma_c \pmod{(p-1)}. \qquad (5)$$

Следствие. Если известно множество $\{c\} = \{\varphi(p-1)\} = \{k_i\}$ и индекс γ_1 числа $a \in G(p-1)$ при основании θ_1, тогда для вычисления всех изоморфных индексов γ_2, ..., γ_c числа a необходимо решать сравнение (5).

Теорема 1. *Если* i *является номером элемента* a_i *мультипликативной группы* $G(p-1)$ *поля* $GF(p)$ *и принимает рекуррентно значе-*

ния $i = 1, 2, \ldots, p-1$, а θ_k есть любой к-й изоморфный первообразный элемент поля GF (p), то с точностью до изоморфизма элементы a_i ($i = 1, 2, \ldots, G(p-1)$), их индексы ind a_i *и номера позиций i связаны рекуррентным соотношением*

$$a_{(i-\text{ind}\,a_i+1)} \equiv (a_{(i-1-\text{ind}\,a_{i-1}+1)})\,\theta_k \pmod p. \qquad (6)$$

На основании теоремы 1 вычисление последовательности элементов a_i и их индексов при любом первообразном $\theta_к$ существенно упрощается и сводится к решению рекуррентного соотношения (6), каждый из сомножителей правой части которого не превышает модуля p. При этом не требуется, как и в случае леммы 2, использовать таблицы индексов чисел, решать постоянно соотношение (3). Кроме того, соотношение (6) легко алгоритмизируется, что позволяет успешно применять его для программного обеспечения при формировании НЛРП.

На приведенном в табл. 1 конкретном примере построения элементов a_i поля GF (13) и вычисления индексов элементов можно проследить справедливость лемм 3—6 и теоремы 1.

При формировании НЛРП в простых полях $GF(p)$, как следует из (1) — (3), (6), требуется знание первообразного элемента θ. С этой целью в работе [1] используется таблица первообразных корней (элементов), приводимая в работе [6], так как вычисление θ для каждого конкретного поля $GF(p)$ является трудоемкой задачей [6]. Действительно, согласно работе [6], для того чтобы число θ, взаимно простое с p, т. е. $(\theta, p) = 1$, было первообразным корнем по модулю p, необходимо и достаточно, чтобы это θ не удовлетворяло ни одному из сравнений

$$\theta^{\frac{c}{g_1}} \not\equiv 1 \pmod p;\ \theta^{\frac{c}{g_2}} \not\equiv 1 \pmod p,\ \ldots;\ \theta^{\frac{c}{g_k}} \not\equiv 1 \pmod p, \qquad (7)$$

где $c = \varphi(p)$; $\varphi(p)$ — функция Эйлера, $g_1, g_2, \ldots, g_k$ — различные простые делители числа c.

Методику вычисления θ можно свести к следующему легко алгоритмизируемому утверждению.

Утверждение 1. Так как $\varphi(p) = p - 1$, то, возводя последовательно числа натурального ряда $g = 2, 3, 4\ldots$ в степени $x = (p-1), (p-1)/K_1, \ldots, (p-1)/K_l$ с помощью рекуррентного соотношения $a^{x-1} \equiv l \cdot a \pmod p$, $l \equiv a^{x-2} \pmod p$, где K_i — вычисляемые простые сомножители числа $(p-1)$, и анализируя результаты согласно условию (7), получаем значение θ.

Методика формирования НЛРП в соответствии с правилами (1) и (2) сводится к следующему.

Утверждение 2. Для формирования НЛРП в соответствии с правилом (I) необходимо вычислить первообразный элемент θ согласно утверждению I, затем вычислить последовательность элементов a_i поля $GF(p)$ согласно соотношению (6) при $i = 0, 1, 2, \ldots, p-1$. Поскольку в этом случае i есть индекс a_i (согласно теореме 1), то последовательность значений характера $\psi(a_i)$ (в соответствии с (4)) будет представлять собой чередование (меандр) символов (1, —1). Для обеспечения равенства $\psi(a_i) = \psi(i)$ достаточно с помощью цикла перестановочного соответствия последовательности чисел $i = 0, 1, \ldots,$

Таблица 4

$p = 13$; $GF(13) = \{0, 1, 2, \ldots, 12\}$;
$\varphi(p-1) = \{K_1 = 1,\ K_2 = 5,\ K_3 = 7,\ K_4 = 11\}$

$\theta_1^{K_1} = 2,\ a_i = \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\},\ i = 1, 2, 3, \ldots, 12,$
$\gamma_1 = \mathrm{ind}_{\theta_1} a_i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$\theta_2 \equiv \theta_1^{K_2} \equiv 6 \pmod{13},\ a_i = \{1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11\},$
$\gamma_2 = \mathrm{ind}_{\theta_2} a_i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\},\ i = 1, 2, 3, \ldots, 12$

$\theta_3 \equiv \theta_1^{K_3} \equiv 11 \pmod{13},\ = 1, 11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6,$
$\gamma_3 = \mathrm{ind}_{\theta_3} a_i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\},\ i = 1, 2, 3, \ldots, 12$

$\theta_4 \equiv \theta_1^{K_4} \equiv 7 \pmod{13},\ = 1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2,$
$\gamma_4 = \mathrm{ind}_{\theta_4} a_i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\},\ i = 1, 2, 3, \ldots, 12$

a_i	$a_i \equiv \theta_1^{\gamma_1} \equiv \theta_2^{\gamma_2} \equiv \theta_3^{\gamma_3} \equiv \theta_4^{\gamma_4} \pmod{p = 13}$
1	$1 \equiv 2^0 \equiv 6^0 \equiv 11^0 \equiv 7^0 \bmod 13$
2	$2 \equiv 2^1 \equiv 6^5 \equiv 11^7 \equiv 7^{11} \bmod 13$
3	$3 \equiv 2^4 \equiv 6^8 \equiv 11^4 \equiv 7^8 \bmod 13$
4	$4 \equiv 2^2 \equiv 6^{10} \equiv 11^2 \equiv 7^{10} \bmod 13$
5	$5 \equiv 2^9 \equiv 6^9 \equiv 11^3 \equiv 7^3 \bmod 13$
6	$6 \equiv 2^5 \equiv 6^1 \equiv 11^{11} \equiv 7^7 \bmod 13$
7	$7 \equiv 2^{11} \equiv 6^7 \equiv 11^5 \equiv 7^1 \bmod 13$
8	$8 \equiv 2^3 \equiv 6^3 \equiv 11^9 \equiv 7^9 \bmod 13$
9	$9 \equiv 2^8 \equiv 6^4 \equiv 11^8 \equiv 7^4 \bmod 13$
10	$10 \equiv 2^{10} \equiv 6^2 \equiv 10^{10} \equiv 7^2 \bmod 13$
11	$11 \equiv 2^7 \equiv 6^{11} \equiv 11^1 \equiv 7^5 \bmod 13$

Пример.

$$a = 3 \equiv 2^4 \equiv (2^5)^8 \equiv (2^7)^4 \equiv (2^{11})^8 \bmod 13.$$

$$\gamma_1 = 4 \equiv (K_2\gamma_2 = 40) \equiv (K_3\gamma_3 = 28) \equiv (K_4\gamma_4 = 88) \bmod 12.$$

$p-1$ поставить такую последовательность $\psi(a_i)$, при которой $a_i = 1$. Тем самым будет сформирована НЛРП в виде кодов квадратичных вычетов.

Утверждение 3. Для формирования НЛРП согласно правилу (2) необходимо вычислить первообразный элемент θ (согласно утверждению 1), затем вычислять $a_i \equiv \theta^i + 1 \pmod p$ и соответствующие характеры $\psi(a_i)$ по следующей методике: из свойств сравнений следует, что если $x_i \equiv \theta^i \pmod p$, то $x_i + 1 \equiv \theta^i + 1 \pmod p$. Следовательно, вычисляя x_i согласно (6) и прибавляя к x_i единицу; получаем a_i. Для x_i значение i является индексом, тогда для a_i индексом будет такое число z, при котором $x_z = a_i$, т. е. $a_z \equiv \theta^z \pmod p$.

Таким образом, с помощью цикла перестановочного соответствия, ставя в соответствие каждому a_i из массива $[a_i]$ такое значение $i = z$, при котором $a_i = x_z$, формируется массив индексов $[u_i]$ для $[a_i]$. Однако в массиве $[x_i]$ всегда отсутствует число p, а в массиве $[a_i]$ — число 1. Учитывая лемму 3 и тот факт, что значение позиции НЛРП $v_i = 1$ справедливо для $a_i \equiv 0 \pmod p$ и $u_i \equiv 0 \pmod 2$, можно утверждать, что замена числа p в массиве $[a_i]$ на 1, обеспечивает соответствие массивов $[a_i]$ и $[x_i]$ по набору чисел и однозначное соответствие массивов $[u_i]$ и $[a_i]$. Анализируя массив $[u_i]$ согласно (4) на четность, формируют НЛРП в виде характеристических кодов.

Для формирования кодовых словарей НЛРП фиксированной длительности необходимо, согласно [1], вычислять авто- и изоморфные коэффициенты разностных множеств НЛРП $A = \{a_1, a_2, \ldots, a_k\}$, где a_k номер позиций НЛРП с символами 1, т. е. определять все разностные множества вида

$$A_t \equiv tA \pmod L \equiv \{ta_1,\ ta_2\ \ldots\ ,\ ta_k\} \pmod L. \qquad (8)$$

Здесь $t \in T$ содержит $\varphi(L)$ чисел взаимно простых с L.

Методика вычисления множества T [1] неэффективна, так как связана с большим объемом вычислений и трудно алгоритмизируется. Более простая методика [7] заключается в следующем утверждении.

Утверждение 4. Испытывая число L (длительность НЛРП) на делимость на множество чисел $2, 3, \ldots, L/2$, определяем множество простых сомножителей $\{l_i\}: L = l_1^{\alpha_1} \cdot l_2^{\alpha_2}, \ \ldots\ , \ l_i^{\alpha_i}$. Затем из множества чисел $\{1, 2, 3, \ldots, L-1\}$ выбрасываются числа, делящиеся на $l_1, l_2, \ldots, l_i$ методом «решета Эратосфена» [6]. Тем самым формируется множество чисел T. Затем, испытывая сумму каждых двух любых чисел множества T на выполнение условия $t_i + t_k \equiv 0 \pmod L$, $i \neq k$, отыскивают наименьшие числа, подчиняющиеся данному условию. Тем самым формируется множество неинверсно-изоморфных коэффициентов $T_н$, используя которое, получают неинверсно-изоморфные множества A_t согласно (8) несущие в себе изменения тонкой внутренней структуры соответствующих им НЛРП.

Вычисление автоморфных и инверсно-изоморфных разностных множеств A_t не имеет смысла потому, что в соответствии с работой [1] автоморфным A_t отвечают циклические сдвижки символов НЛРП, а инверсно-изоморфным A_t — зеркальные отображения с циклическим сдвигом символов НЛРП.

Таблица 2

*C*1	Оператор начала процедуры.
*A*2	Описание заглавия и формальных параметров процедуры ВЫЧЕТ (θ, p, L, v).
*A*3	Описание параметров тела процедуры.
*A*4	Формирование первого и второго элементов поля $GF(p)$.
*A*5	Оператор формирования A_i элемента поля $GF(p)$ по соотношению $A_i = a_{i-1}\theta$.
*A*6	Деление A_i на модуль p.
*A*7	Нахождение остатка частного от деления.
*A*8	Умножение на модуль остатка частного от деления и нахождение целого от произведения и формирование массива элементов поля $GF(p)$.
*B*9	Проверка условия равенства ряда натуральных чисел элементу a_i.
*A*10	Формирование массива индексов элементов a_i.
*B*11	Проверка условия на четность индекса элемента a_i.
*B*12	Присвоение 1 кодовой позиции v_i.
*A*13	Присвоение — 1 кодовой позиции v_i.
*A*14	Присвоение 1 первой кодовой позиции v_1.
*C*15	Оператор вывода на печать.

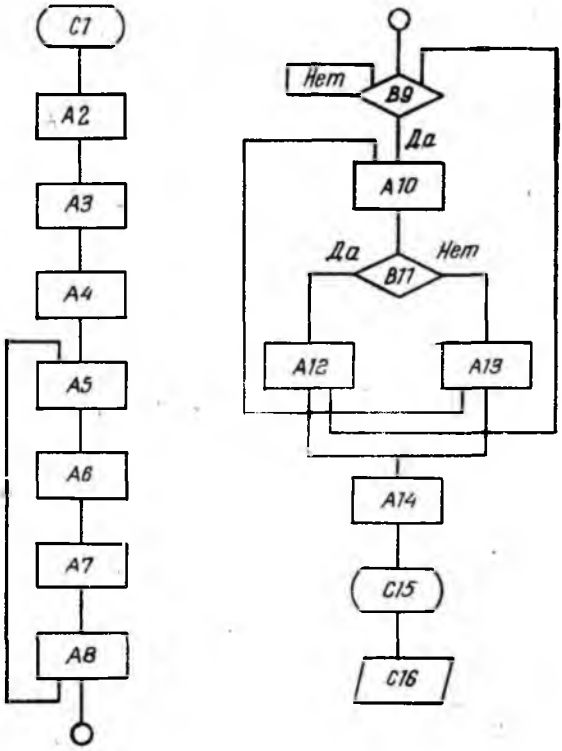

Рис. 1

Рассмотренные методики положены в основу алгоритмов формирования НЛРП.

Алгоритмы формирования НЛРП в полях GF (p). На рис 1 приведен, а в табл. 2 раскрыт алгоритм «ВЫЧЕТ», позволяющий при задаваемых значениях первообразного элемента θ и длительности $L = p = 4t + 1, 4t + 3$ формировать НЛРП нечетной длительности L в виде кодов квадратичных вычетов.

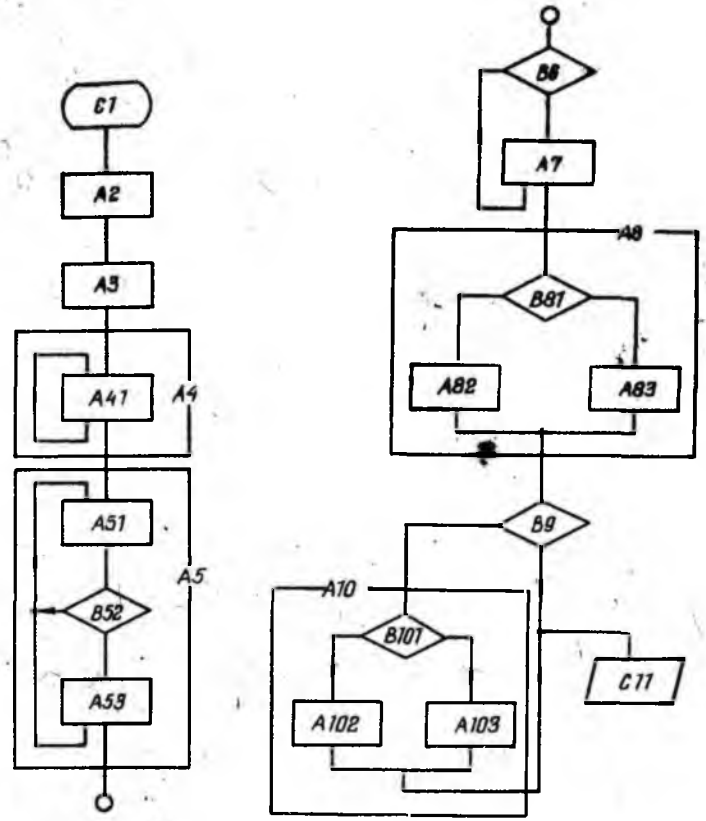

Рис. 2

На рис. 2 представлен, а в табл. 3 раскрыт алгоритм «ХАРА», позволяющий при задаваемых значениях первообразного элемента θ и длительности $L = p - 1 = 4t$, $4t + 2$ формировать НЛРП четной длительности L в виде характеристических кодов.

Данные алгоритмы, ориентированные на языки высокого уровня, являются эффективным программным обеспечением для ЦВМ, микроЭВМ и микропроцессоров для формирования в реальном масштабе времени кодовых словарей НЛРП любых длительностей $L = p, p - 1,$

Таблица 3

C1	Начало процедуры.
A2	Описание заголовка процедуры и формальных параметров «ХАРА» (θ, p, L, v).
A3	Описание параметров тела процедуры.
A4, *A41*	Формирование массива элементов a_i согласно рекуррентному выражению $a_i \equiv a_{i-1}\theta \pmod p$.
A5	Формирование массива элементов $a_i \equiv \theta^i + 1 \equiv a_i + 1 \pmod p$.
A51	Увеличение на 1 элементов a_i, т. е. $a_i^* = a_i + 1$.
B52	Проверка условия $\psi(a_i) = p$.
A53	Присвоение $\psi(a_i) = 1$.
B6	Проверка условия $\psi(a_i) = \psi(a_i^*)$.
A7	Формирование массива индексов элементов a_i^*.
A8	Формирование кодовой последовательности V.
B81	Проверка условия на четность массива индексов элементов a_i^*.
A82	Присвоение $v_i = 1$.
A83	Присвоение $v_i = -1$.
B9	Проверка условия $v[L] = 1$.
A10	Формирование кодовой последовательности.
B101	Проверка условия $v_i = 1$.
A102	Присвоение $v_i = -1$.
A103	Присвоение $v_i = 1$.
C11	Оператор конца процедуры.

где p — простое число. Как показал опыт, данные алгоритмы с использованием средних по мощности ЦВМ серии «ЕС» позволяют формировать кодовые словари НЛРП длительностями $L > 1000$ за единицы минут.

Список литературы: 1. *Свердлик М. Б.* Оптимальные дискретные сигналы. М., 1975. 200 с. 2. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. М., 1985. 384 с. 3. *Пелехатый М. И.* О последовательностях квадратичных вычетов. с наилучшими автокорреляционными свойствами // Радиотехника и электрон. 1971. Т. 16, № 5. С. 125—134. 4. *Пелехатый М. И., Голубев Е. А.* Автокорреляционные свойства некоторых типов двоичных последовательностей // Пробл. передачи информации. 1972 . Т. 8, № 1. С. 92—99. 5. *Диксон Р. К.* Широкополосные системы: Пер. с англ. / Под ред. В. И. Журавлева. М., 1979. 304 с. 6. *Виноградов И. М.* Теория чисел. М., 1972. 105 с. 7. *Сныткин И. И.* К вопросу теоретико-числовых методов построения рекуррентных последовательностей // Вестн. Харьк. политехн. ин-та. 1980. Вып. 8. № 7. С. 31—34.

Поступила в редколлегию 11.04.88