УДК 621.391.82

И. И. СНЫТКИН, канд. техн. наук

АЛГОРИТМИЧЕСКИЕ МЕТОДЫ ФОРМИРОВАНИЯ КОДОВЫХ СЛОВАРЕЙ НЕЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, СУЩЕСТВУЮЩИХ В РАСШИРЕННЫХ ПОЛЯХ ГАЛУА $GF(p^n)$

В работах [1—4], связанных с теорией и практикой ШПС, рассматриваются вопросы формирования и выбора оптимальных по корреляционным свойствам кодовых рекуррентных последовательностей (КРП), не генерируемых регистрами сдвига с линейными обратными связями и называемых нелинейными рекуррентными последовательностями (НЛРП). В работе [1] представлен весьма ограниченный класс НЛРП в виде полных кодовых колец, существующих в полях $GF(2^n)$ и обладающих тем самым рядом недостатков, не позволяющих их широко использовать, особенно в специальных системах [4]. Среди НЛРП особое место, занимает класс НЛРП в виде характеристических кодов, существующих в расширенных полях $GF(p^n)$, где простое число $p>2$, для четных длительностей $L=p^n-1=4\cdot t,\ 4\cdot t+2;\ t=1,\ 2,\ 3\ldots$ [2]. Данные НЛРП помимо оптимальных корреляционных свойств обладают свойствами симметрии числа 1 и —1, большой мощностью кодирования и потенциально не раскрываемой (не восстанавливаемой) внутренней структурой, что имеет неоценимое значение для специальных систем с ШПС [4]. В работе [3] освещаются вопросы формирования НЛРП в виде характеристических кодов, однако существующих лишь в простых полях $GF(p)$ и для $L\leqslant 136$. В работе [2] исследуется метод «ручного» формирования НЛРП в рас-

ширенных полях $GF(p^n)$ ограниченного числа и с максимально формируемой длительностью $L=124$ в $GF(5^3)$. Однако данный метод неэффективен и практически не алгоритмизируем, так как основан на построении и использовании сопровождающих матриц громоздких таблиц сложения элементов полей $GF(p^n)$, их индексов, что требует огромных временных затрат при ручной работе [2] и делает невозможным формирование таких НЛРП с $L>100$.

Формирование больших по объему систем НЛРП больших ($L>1000$) и сверхбольших ($L>10000$) длительностей является весьма актуальной задачей в теории и практике систем с ШПС [1; 2; 4].

Правило построения НЛРП в расширенных полях $GF(p^n)$. В соответствии с работой [2] правило построения данных НЛРП имеет вид

$$GF(p^n)=\{a_i:\theta^i(\mathrm{mod}\, df(x),\ p)\};\ L=p^n-1=4\cdot t,\ 4\cdot t+2;$$

$$t=0,\ 1,\ 2,\ ...;$$

$$\begin{cases} V=\{V_i:i=0,\ 1,\ ...,\ p^n-2\}; \\ V_i=\psi(\theta^i+1),\ \theta^i+1\not\equiv 0(\mathrm{mod}\, df(x),\ p); \\ V_i=\pm 1,\quad \theta^i+1\equiv 0(\mathrm{mod}\, df(x),\ p), \end{cases} \tag{1}$$

где θ — первообразный элемент поля $GF(p^n)$, $f(x)$ — первообразный неприводимый над $GF(p)$ полином степени n, a_i—i-й элемент поля, $\psi(\cdot)$ — двузначный характер мультипликативной группы [2]:

$$\psi(a)=\exp(j\pi u)=\begin{cases} 1, & u\equiv 0(\mathrm{mod}\,2); \\ -1, & u\equiv 1(\mathrm{mod}\,2), \end{cases} \tag{2}$$

где u — индекс элемента a при выполнении условия

$$a\equiv\theta^u(\mathrm{mod}\, df(x),\ p). \tag{3}$$

Как видно из правила (1) и соотношений (2), (3), основные трудности при формировании таких НЛРП заключаются в вычислении элементов a_i, индексов, характеров и в определении соответствий между ними согласно (1).

Ниже на основе установленных автором и приводимых систематических комбинационно-логических соотношений в теории расширенных полей $GF(p^n)$ исследуются эффективные программные методы и алгоритмы, положенные в основу программного обеспечения ЦВМ, микроЭВМ и микропроцессоров при формировании в реальном масштабе времени систем НЛРП, существующих в расширенных полях Галуа $GF(p^n)$ при простом числе $p>2$.

Новые соотношения в теории расширенных полей $GF(p^n)$. Соотношения приводятся без доказательств вследствии их громоздкости, в их объективности можно удостовериться с использованием примера построения НЛРП в поле $GF(3^2)$, помещенного в табл. 1.

Таблица 1

i	x^{i-1}	$F_{k;i}(x) \equiv x^{i-1} (\mathrm{mod} f(x), p)$	V_i	i	x^{i-1}	$F_{k,i}(x) \equiv x^{i-1} (\mathrm{mod} f(x), p)$	V_i
1	x^0	1	1	5	x^4	2	1
2	x^1	x	1	6	x^5	$2 \cdot x$	−1
3	x^2	$x+1$	−1	7	x^6	$2 \cdot x + 2$	−1
4	x^3	$2 \cdot x + 1$	1	8	x^7	$x + 2$	−1

Лемма 1. *Расширенное поле $GF(p^n)$ представляет собой множество, состоящее из всевозможных элементов-многочленов (полиномов) степени k*

$$F_k(x) = \alpha_k \cdot x^k + \alpha_{k-1} \cdot x^{k-1} + \ldots + \alpha_1 \cdot x + \alpha_0, \qquad (4)$$

определяемых всевозможными обращениями как порядок следования, так и самих значений коэффициентов α_i, принимающих всевозможные значения элементов простого поля $GF(p) = \{0,1 \ldots, p-1\}$, при этом $k = 0, 1, \ldots, n-1$, а $\alpha_k \neq 0$ при $k \neq 0$.

Следствие. *Для определения множества элементов расширенного поля $GF(p^n)$ достаточно в многочлене $F_k(x)$ (4) фиксировать значение $k = 0, 1, 2, \ldots, n-1$, а коэффициентам α_i придавать всевозможные размещения по $(k+1)$ элементов из множества $GF(p)$. При этом многочлены $F_k(x)$ будут представлять собой вычеты поля $GF(p^n)$, число таких многочленов равно порядку p^n. Следовательно, для определения множества элементов поля $GF(p^n)$ не требуется знания первообразного неприводимого над $GF(p)$ полинома степени n.*

Лемма 2. *Произвольному элементу-полиному $F_{k,i}(x)$ вида (4), где i — его номер, поля $GF(p^n)$ однозначно соответствует степень x^{i-n}, удовлетворяющая сравнению $x^{i-1} \equiv F_{k,i}(x) \times \times (\mathrm{mod}\, df(x), p)$, если $f(x)$ — первообразный неприводимый над $GF(p)$ полином степени n, а $i = 1, \ldots, p^n - 1$ и является номером элемента-полинома $F_{k,i}(x)$.*

Лемма 3. *С точностью до изоморфизма индексом $\mathrm{Ind}(F_{k,i}(x))$ элемента-полинома $F_{k,i}(x)$ расширенного поля $GF(p^n)$ является число $(i-1)$, если i является номером элемента $F_{k,i}(x)$ и принимает значения $1, 2, \ldots, p^n - 1$ так, что справедливо сравнение*

$$x^{i-1} \equiv F_{k,i}(x) (\mathrm{mod}\, df(x),\ p). \qquad (5)$$

Леммы 1—3 имеют важное значение для алгоритмизации процедуры формирования НЛРП в $GF(p^n)$, основывающихся на формулируемых ниже теоремах.

Теорема 1. *Если i является номером позиции элемента-полинома $F_{k,i}(x)$ расширенного поля $GF(p^n)$ и принимает рекуррентно значения $i = 1, 2, \ldots, p^n - 1$, а $f(x)$ — первообразный неприводимый над $GF(p)$ полином степени n, то с точностью до изоморфизма*

элементы-полиномы $F_{k,i}(x)$, *их индексы* $\operatorname{Ind} F_{k,i}(x)$) *и номера позиций связаны рекуррентным соотношением*

$$F_{k,l=\operatorname{Ind}F_{k,l}(x)+1}(x) \equiv (F_{k,l-1=\operatorname{Ind}F_{k,l-1}(x)+1}(x))\, x \pmod{df(x),\ p}. \quad (6)$$

Теорема 2. *Если элемент-полином* $F_{k,i}(x)$ *расширенного поля* $GF(p^n)$ *представить в виде*

$$F_{k,i}(x) = \alpha_{k,i-1} \cdot x^k + \alpha_{k-1,i-1} \cdot x^{k-1} + \ldots + \alpha_{1,i-1} \cdot x^1 + \alpha_{0,i-1}, \quad (7)$$

где $k = 0, 1, 2, \ldots, n-1$, $\alpha_k \neq 0$ *при* $k \neq 0$, $\alpha = \pm\{0, 1, \ldots, p-1\}$, *а первообразный неприводимый над* $GF(p)$ *полином степени* n *записать как*

$$f(x) = x^n + \beta_{n-1} \cdot x^{n-1} + \ldots + \beta_1 \cdot x^1 + \beta_0,$$

где $\beta = \pm\{0, 1, \ldots, p-1\}$, *тогда*

а) если в (7) $\alpha_{k,i-1} = 0$, *или* $\alpha_{k,i-1} = \alpha_{k-1,i-1} = 0$, *или* $\alpha_{k,i-1} = \alpha_{k-1,i-1} = \alpha_{k-2,i-1} = 0$, *или* ..., *или* $\alpha_{k,i-1} = \ldots = \alpha_{1,i-1} = 0$, *то последующий элемент* $F_i(x)$ *поля* $GF(p^n)$ *есть соответственно*

$$F_i(x) = F_{k,i}(x) = \alpha_{k-1,i-1} \cdot x^k + \alpha_{k-2,i-1} x^{k-1} + \ldots + \alpha_{0,i-1} \cdot x^1,$$

или

$$F_i(x) = F_{k-1,i}(x) = \alpha_{k-2,i-1} \cdot x^{k-1} + \alpha_{k-3,i-1} \cdot x^{k-2} + \ldots + \alpha_{0,i-1} \cdot x^1, \ldots$$

или, ..., *или* $F_i(x) = F_{1,i}(x) = \alpha_{0,i-1} x^1$;

б) если в (7) $\alpha_{k\,i-1} = 0$, *то последующий элемент* $F_i(x)$ *равен*

$$F_i(x) = F_{k,i}(x) \equiv (F_{k,i-1}(x) - \alpha_{k,i-1} \cdot f(x)) \bmod p. \quad (8)$$

Теорема 3. *В расширенном поле* $GF(p^n)$ *всегда могут быть найдены два элемента-полинома вида (4), удовлетворяющие условию*

$$F_{k,l=\operatorname{Ind}F_{k,i}+1}(x) \equiv (F_{k,j=\operatorname{Ind}F_{k,j}+1}(x) + 1) \bmod p,$$

если $i \neq j$, i, j *принимают значения* $0, 1, \ldots, p^n-1$ *и являются номерами позиций соответствующих элементов-полиномов* $F_{k,i}(x)$, $F_{k,j}(x)$ *расширенного поля* $GF(p^n)$.

С помощью методов, определяемых теоремами 1—3, можно легко, даже вручную, с точностью, до изоморфизма вычислять последовательности элементов расширенного поля и соответствующие им индексы. Действительно, при использовании теорем 1—3 этот процесс сводится к проведению арифметических операций с коэффициентами первообразного неприводимого полинома $f(x)$. Первыми n элементами этой последовательности будут элементы $0, 1, x, x^2, \ldots, x^{n-1}$, а остальные элементы вычисляются с использованием коэффициентов предыдущего элемента, начиная с x^{n-1}, и полинома $f(x)$. Данные методы легко алгоритмизируются и эффективно осуществляются при синтезе НЛРП в расширенных полях $GF(p^n)$. Так, при применении теорем 1—3 формирование

данных НЛРП сводится к последовательности операций, определяемой следующим утверждением.

Утверждение 1. Пусть $I\,[1:L]$ — массив индексов элементов-полиномов $F_{k,i}(x)$ поля $GF(p^n)$, а $\alpha_0, \alpha_1, ..., \alpha_{n-1}$ $[1:L]$ — массивы коэффициентов при соответствующих степенях $x^0, x^1, ..., x^{n-1}$ элементов-полиномов $F_{k,i}(x)$. Тогда НЛРП в расширенном поле $GF(p^n)$ по правилу (1) можно сформировать следующим образом:

а) из массива $I\,[:L]$ формировать массивы номеров-индексов элементов поля, имеющих равные коэффициенты α_{n-1}, таких массивов будет $p:\alpha_{n-1,0};\ \alpha_{n-1,1};\ \alpha_{n-1;2};\ ...,\ \alpha_{n-1,p-1}\,[1:L/p]$;

б) для каждого массива $\alpha_{n-1,i}\ [1:L/p]$ формировать массивы номеров-индексов элементов поля, имеющих равные коэффициенты α_{n-2}, таких массивов будет $p:\alpha_{n-2,1,0};\ \alpha_{n-2;1;1};\ ...;$ $[1:L/p^2]$ и т. д.;

в) для каждого массива $\alpha_{2,n-(n-3),...,i}$ формировать массивы номеров-индексов элементов поля, имеющих равные коэффициенты α_1, таких массивов будет $p:\alpha_{1,n-(n-2)},...,0;\ \alpha_{1,n-(n-2)},...,1,\ ...;$ $\alpha_{1,n-(n-2)},...,p-1\ [1:L/p^{n-1}]$;

г) для каждого номера-индекса элемента поля из массива $\alpha_{1,...,i}\ [1:L/p^{n-1}]$ ставить в соответствие номер-индекс другого элемента поля из того же массива так, чтобы коэффициент α_0 последнего превышал на единицу коэффициент α_0 первого элемента; тем самым формируется массив $I^*\ [1:L]$;

д) анализируя масив $I^*\ [1:L]$ на четность согласно (2), формируется НЛРП.

В табл. 1 с фактическими данными на простом примере поля $GF\,(3^2)$, для которого первообразный неприводимый над GF (3) полином $f(x)=x^2-x-1$, можно проследить справедливость выше приведенных лемм, теорем, утверждения и построение НЛРП с $L=3^2-1=8$.

Формирование кодовых словарей НЛРП фиксированной L связан, как известно [2], с авто- и изоморфными преобразованиями соответствующих разностных множеств $A=\{a_1, a_2, ..., a_k\}$, где a_i — номер позиций НЛРП с символами 1, вида

$$A_t \equiv t\cdot A\,(\mathrm{mod}\,L) \equiv \{t\cdot a_1,\ t\cdot a_2,\ ...,\ t\cdot a_k\}(\mathrm{mod}\,L),$$

где $t\in T$, содержащее $\varphi(L)$ чисел взаимно простых с L, $\varphi(L)$ — функция Элера. В работе [2] метод формирования множества T — сложный и громоздкий. В соответствии с ниже приводимым утверждением этот процесс значительно упрощается.

Утверждение 2. Испытывая число L на делимость на множество чисел $\{2, 3, ..., L/2\}$, определяется множество простых сомножителей $\{l_i\}: L=l_1^{\alpha_1}\cdot l_2^{\alpha_2}\ldots l_i^{\alpha_i}$. Затем из множества чисел $\{1, 2, 2, ..., L-1\}$ выбрасываются числа, делящиеся на $l_1, l_2, ..., l_i$ методом «решета Эратосфена» [5]. Тем самым формируется множество чисел T. Затем испытывая сумму каждых двух любых чисел множества T на выполнение условия $t_i+t_k \equiv 0\ (\mathrm{mod}\,L)$, $i\neq k$, отыскиваются наименьшие числа, подчиняющиеся данному усло-

вию. Тем самым формируется множество неинверсно-изоморфных коэффициентов $T_и$. Используя $t \in T_и$, можно получать неинверсно-изоморфные множества A_t, несущие в себе изменения тонкой внутренней структуры соответствующих им НЛРП. Вычисление автоморфных и инверсно-изоморфных разностных множеств A_t не

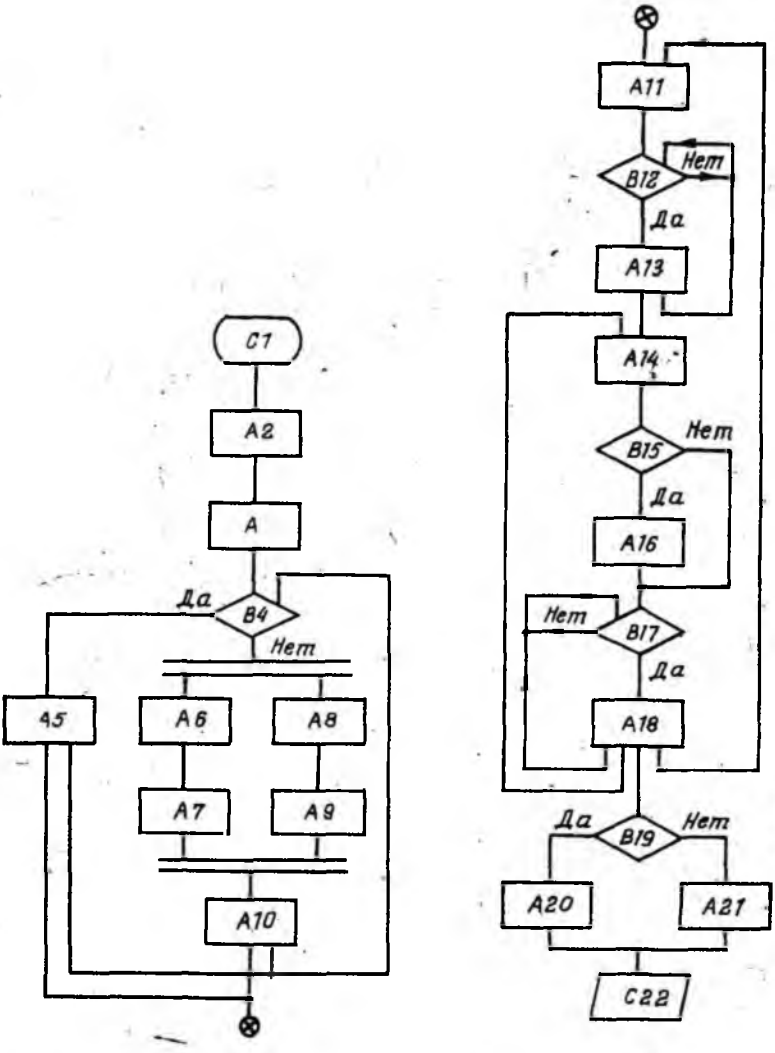

Рис. 1

имеет смысла, потому что, как показано в работе [2], автоморфным A_t соответствуют циклические сдвижки символов НЛРП, а инверсно-изоморфным A_t — зеркальные отображения с циклическим сдвигом символов НЛРП.

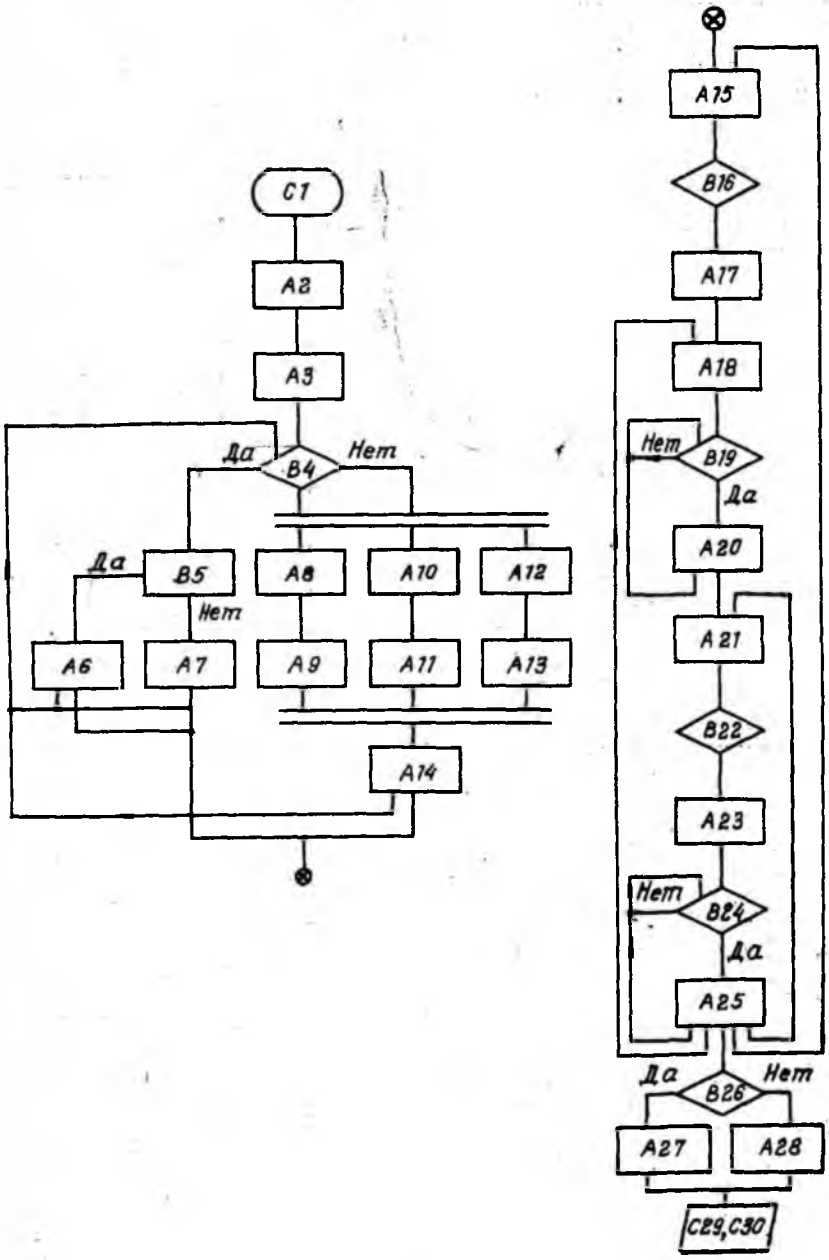
C1
A2
A3
B4
Да
Нет
B5
Да
Нет
A6
A7
A8
A9
A10
A11
A12
A13
A14
A15
B16
A17
A18
Нет
B19
Да
A20
A21
B22
A23
Нет
B24
Да
A25
Да
B26
Нет
A27
A28
C29,C30

Рис. 2

Таблица 2

Алгоритм РП1 формирования НЛРП в $GF(p^2)$, $f(x)=x^2+A\cdot x+B$

C1	Начало программы процедуры.
A2	Описание заглавия процедуры, ее формальных параметров РП1(L, p, A, B, V), описание параметров тела процедуры с размерностью массивов V, A, B, [1 : L].
A3	Формирование коэффициентов первого элемента поля $GF(p^2)$: $A1$ [1] = 0, $B1$ [1] = 1; $A1$, $B1$ — массивы коэффициентов элементов поля при степенях соответственно x^1, x^0 размерностью [1 : L]. Проверка условия равенства нулю коэффициентов A1.
B4	Формирование коэффициентов следующего элемента поля путем
A5	циклической сдвижки коэффициентов предыдущего.
A6—A7	Операторы формирования коэффициента A1 последующего элемента поля $GF(p^2)$ согласно утверждению 1.
A8—49	Операторы формирования коэффициента B1 последующего элемента поля $GF(p^2)$ согласно утверждению 1.
A10	Оператор приведения коэффициентов A1 и B1 по модулю p.
A11	Приравнивание параметра номера элемента поля к нулю.
B12	Проверка условия равенства массива коэффициентов A1 каждому из возможных значений.
A13	Оператор формирования массива номеров элементов, имеющих равные (одному из возможных) значения A1.
A14	Оператор увеличения на 1 коэффициента B1 очередного элемента поля, имеющего равные значения A1.
B15	Проверка условия равенства увеличенных коэффициентов модулю p.
A16	Приравнивание коэффициента модулю p.
B17	Проверка условия равенства B1 элемента поля и очередного увеличенного коэффициента.
A18	Формирование элемента массива AA [1 : p] индексов элементов поля, равного уменьшенному на 1 номеру элемента, имеющего коэффициент, равный очередному, увеличенному коэффициенту оператора A14.
B19	Проверка условия на четность массива индексов элементов поля $GF(p^2)$.
A20	Присвоение кодовой последовательности V_i символа 1.
A21	Присвоение кодовой последовательности V_i символа —1.
C22	Оператор вывода на печать и останова.

В соответствии с рассмотренными положениями ниже приводятся эффективные программные алгоритмы, обеспечивающие формирование кодовых словарей НЛРП в расширенных полях Галуа $GF(p^n)$ в соответствии с утверждениями 1 и 2, рассчитанные на языки высокого уровня.

Алгоритмы формирования НЛРП в $GF(p^n)$. На рис. 1, 2 приведены функциональные схемы алгоритмов-процедур соответственно «РП1», «РП2», а в табл. 2, 3 помещены комментарии к ним. Алгоритмы «РП1», «РП2» позволяют при любых задаваемых значениях модуля p и первообразных неприводимых над $GF(p)$ полиномах соответственно 2- и 3-й степеней формировать НЛРП в полях $GF(p^n)$ с порядками полей p^2, p^3. Данные алгоритмы являются формализованно-унифицированными, что позволяет разрабатывать аналогичные алгоритмы в полях $GF(p^n)$ с $n>3$.

Таблица 3

	Алгоритм РП2 формирования НЛРП в $GF(p^3)$, $f(x)=x^3+A\cdot x^2+B\cdot x+D$
C1	Начало программы процедуры.
A2	Описание заглавия тела процедуры, ее фактических параметров РП2 (L, p, A, B, D, V), параметров тела.
A3	Формирование коэффициентов первого элемента поля $GF(p^3)$: $A1\,[1]=0$, $B1\,[1]=0$, $D1\,[1]=1$; $A1$, $B1$, $D1$ — массивы коэффициентов элементов поля при степенях соответственно x^2, x^1, x^0 размерностью $[1:L]$.
B4	Проверка условия равенства нулю коэффициента $A1$ очередного элемента поля $GF(p^3)$.
B5	Проверка условия равенства нулю коэффициента B1 очередного элемента поля $GF(p^3)$.
A6	Формирование коэффициентов последующего элемента поля путем двух циклических сдвигов влево коэффициентов очередного элемента поля.
A7	Формирование коэффициентов последующего элемента поля путем одного сдвига влево коэффициентов очередного элемента поля.
A8—A10, A12	Умножение на коэффициент A1 очередного элемента поля коэффициентов соответственно А, В, Д первоочередного полинома.
A9, A11	Вычитание результатов умножения соответственно из коэффициентов B1, Д1 очередного элемента поля.
A13	Присвоение отрицательного знака последнему сомножителю.
A14	Приведение результатов по модулю p и формирование тем самым коэффициентов последующего элемента поля $GF(p^3)$.
A15	Присвоение нуля параметру номера элемента поля.
B16	Проверка условия равенства коэффициента B1 очередного элемента та поля очередному возможному значению.
A17	Формирование элемента массива АА номеров элементов поля, имеющих равные очередному возможному значению коэффициенты А1.
A18	Присвоение нуля параметру номера элемента поля.
B19	Проверка условия равенства коэффициента B1 очередного элемента поля из очередного массива АА очередному возможному значению.
A20	Формирование элемента массива ВВ номеров элементов поля из очередного массива АА, имеющих равные очередному возможному значению коэффициенты B1.
A21	Увеличение на 1 коэффициента Д1 очередного из массива ВВ элемента поля.
B22	Проверка условия равенства модулю p, увеличенного на 1 коэффициента.
A23	Приравнивание нулю коэффициента, равного при увеличении на 1 модулю p.
B24	Проверка условия равенства увеличенного на 1 коэффициента коэффициентам Д1 элементов поля с номерами из массива ВВ.
A25	Формирование элемента массива индексов элементов поля уменьшением на 1 номера элемента поля из массива ВВ, при условии B24.
B26	Проверка условия на четность массива индексов элементов поля $GF(p^3)$.
A27—A28	Присвоение кодовой последовательности V_i символов 1 и —1.
C29—C30	Вывод на печать и оператор останова.

Опыт показывает, что формирование кодовых словарей НЛРП в расширенных полях $GF(p^n)$ для $1000 < L < 10000$ с использованием данных алгоритмов на языке ПЛ-1 и ЭВМ серии «ЕС» занимает единицы минут. Это позволяет широко использовать данные алгоритмы в теории и практике формирования и исследования свойств НЛРП в расширенных полях $GF(p^n)$.

Список литературы: 1. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. М., 1985. 384 с. 2. *Свердлик М. Б.* Оптимальные дискретные сигналы. М., 1975. 200 с. 3. *Пелехатый М. И., Голубев Е. А.* Автокорреляционные свойства некоторых типов двоичных последовательностей//Проблемы передачи информации. 1972. Т. 8, № 1. С. 92—99. 4. *Диксон Р. К.* Широкополосные системы/Пер. с англ. Под ред. В. И. Журавлева. М., 1979. 302 с. 5. *Виноградов И. М.* Теория чисел. М., 1972. 105 с.

Поступила в редколлегию 11.05.88