УДК 621.391

И. Д. ГОРБЕНКО, д-р техн. наук, *А. А. ЗАМУЛА*, канд. техн. наук,
В. Л. КУЛЕШОВ

ПРОГРАММНЫЕ СРЕДСТВА ФОРМИРОВАНИЯ НЕЛИНЕЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

В теории кодирования в различных областях электроники широко используются последовательности над конечными полями, каждый член которых, будучи элементом основного поля, некоторым простым образом зависит от предшествующих ему членов. Такие последовательности легко получить с помощью рекурсивных процедур. Кроме того, такие последовательности обладают полезными статистическими свойствами. Для большинства приложений в качестве основного поля выбирается поле $GF(2)$. Если l — натуральное число, a b, b_0, b_1, ... b_{l-1} — заданные элементы конечного поля GF(P) (где P — характеристика поля), то последовательность S_0, S_1, ... элементов поля $GF(P)$, удовлетворяющая соотношению

$$S_{n+l} = b_{l-1}S_{n+l-1} + b_{l-1}S_{n+l-2} + \ldots + b_0S_n + b, \quad n = 0, 1, \ldots,$$

называется линейной рекуррентной последовательностью (l-го порядка) над полем GF(P).

В ряде практических приложений интерес представляют нелинейные последовательности (НП) характеристического типа [1], построение которых базируется на вычислении двухзначного харак-

тера мультипликативной группы поля Галуа. Характер задается комплексно-значной функцией вида

$$\psi(S) = e^{j\pi U} = \begin{cases} 1, & \text{если } U \equiv 0 \pmod 2 \\ -1, & \text{если } U \not\equiv 0 \pmod 2, \end{cases} \quad (1)$$

где U определяется из условия

$$S \equiv \Theta U \,(\mathrm{modd}\, f(x),\ P). \quad (2)$$

В (1) U — индекс первообразного элемента поля Θ по модулю P и основанию S ($U = \mathrm{ind}_S \Theta \pmod P$), $f(x)$ — первообразный неприводимый над полем GF(P) полином. Множество НП, которое может быть построено в поле GF(P^k), определяется из соотношения $M = \varphi(P-1)/k$ (3).

Принципы построения НП, в частности принципы реализации операции сравнения вида (2), свойства НП изложены в работах [2; 3]).

Программные средства формирования НП, реализующие разработанные принципы построения НП [2], отличаются максимальной гибкостью с точки зрения возможности замены или передачи блоков системы математического обеспечения и поэтому представляют наибольший практический интерес.

Методика, использованная при создании комплекса программ формирования, исследования свойств НП, основывается на разработке оптимальных по точности и быстродействию алгоритмов и их программной реализации. Она основана на идее: каждой задаче — наилучшую программу ее решения и программу вычисления ее основных характеристик (точности, времени реализации и требуемой памяти ЭВМ).

Комплекс программ состоит из двух взаимосвязанных подсистем программных модулей: формирование нелинейных последовательностей в простых ($k=1$) и расширенных ($k>1$) полях Галуа (ФНП); исследования свойств НП (ИСНП). Подсистема ФНП состоит из 12 программных модулей, позволяющих вычислять данные (коэффициенты децимации, функции Эйлера, первообразные элементы поля, первообразные неприводимые над полем GF (P) полиномы степени k и на основе этих данных решать задачи по формированию НП.

Подсистема ИСНП включает 8 программных модулей, позволяющих производить оценки авто- и взаимно корреляционных функций, спектров НП их ансамблевых свойств, а также математического ожидания, дисперсии и среднеквадратичного отклонения.

Для эксплуатации комплекса программ формирования и исследования свойств НП необходимы следующие технические средства: устройство ввода, АЦПУ, накопители на магнитных лентах или дисках, процессор с объемом оперативной памяти не менее 32 К.

Программы комплекса написаны на языках Фортран и Ассемблер. Комплекс программ содержит управляющую программу и программные модули. Программы, написанные на языке Фортран, реализованы в виде подпрограмм типа SUBROUTIN. Обращение к подпрограммам комплекса осуществляется с помощью стандартного оператора CALL. Для проверки работоспособности и точности вычислений используются контрольные примеры, каждый из которых проверяет работу нескольких программ. Комплекс предназначен для эксплуатации на ЭВМ СМ-4 и ЕС. Комплекс программ позволяет пользователю в диалоге с ЭВМ изучить возможность решения задачи выбранной программой. При этом вычисляются оценки времени ее решения и необходимый объем оперативной памяти ЭВМ путем выбора через управляющую программу комплекса программы вычисления оценок характеристик. Если, судя по вычисленным априорным оценкам, ограничения на основные характеристики удовлетворяются, то комплекс гарантирует решение задачи с требуемым качеством. Каждая программа комплекса может работать либо в автономном режиме, либо с помощью управляющей программы комплекса. Комплекс программы может использоваться в других подпрограммах и комплексах в качестве программного модуля.

Оптимизация программ комплекса осуществляется за счет написания наиболее часто используемых фрагментов программы на языке Ассемблер.

Управляющие подпрограммы комплекса составлены на Фортране и Ассемблере для СМ-4 и обеспечивают выполнение следующих функций: печать выходных данных; печать информации о классах задач, решаемых комплексом (например: «Программа генерации НП характеристического типа POSL»); вызов программы решения задачи; вычисление оценок характеристик программы решения задачи (объем оперативной памяти, занимаемый программой, время решения задачи по формированию НП). Программа решения задачи состоит из следующих программных модулей (ПМ): ведущего, печати входных данных, решающего, печати выходных данных. Ведущий ПМ обеспечивает обращение к указанным выше модулям.

Одной из программ комплекса является программа ДЕС, обеспечивающая реализацию операции децимации исходного изоморфизма (НП, построенной по минимальному из первообразных элементов поля $GF(P^k)$. Операция над последовательностями, называемая децимацией или разрядкой [4], определяется следующим образом: если σ — последовательность элементов S_0, S_1, S_2... из поля $GF(P)$, а $c \in P-1$ — натуральное число, то децимированная последовательность $\sigma^{(c)}$ состоит из членов S_0, S_c, S_{2c}, ... т. е. $\sigma^{(c)}$ получается путем выбора каждого c-го члена исходной последовательности, начиная с S_0. При этом c должно отвечать условию: наибольший делитель c и $L=P-1$ равен 1. Применение децимации НП по всем c, для которых $(c, P-1)=1$, позволяет получить

все множество последовательностей M, определяемое из (3) для поля $GF(P^k)$.

Обращение к программе ДЕС производится с помощью стандартного оператора CALL: CALL DEC (L, KD, KOD, KODT), где L — период формируемой НП; KD — коэффициент децимации *(c)*; KOD — исходный изоморфизм; KODT — изоморфизм НП, полученный путем децимации.

Для реализации функции формирования НП в соответствии с алгоритмами, разработанными в [2], необходимо иметь ряд параметров. К таковым могут быть отнесены — минимальный первообразный элемент θ_{min} поля $GF(P)$, множество первообразных элементов $\{\theta\}$ поля $GF(P)$, множество коэффициентов, децимации $\{c\}$, множество первообразных неприводимых над полем $GF(P)$ полиномов $\{f(x)\}$, число элементов НП L.

Существуют различные алгоритмы расчета θ_{min}, однако их вычислительная сложность весьма значительна [4]. Более приемлемый алгоритм расчета θ_{min} заложен в определении первообразного или образующего элемента поля [1]. Элемент a, имеющий максимально возможный период $E=P-1$, называется первообразным элементом поля $GF(P)$ или другими словами, степени первообразного элемента $\theta^0, \theta^1, \ldots \theta^{P-2}$ различны и пробегают все ненулевые элементы поля. Из приведенного определения следует, что для определения θ_{min} необходимо и достаточно последовательно возводить в степени 0, 1, 2, ... $P-2$ числа $\theta=2, 3, \ldots$ Первое из чисел, имеющее максимальный период, и есть первообразный элемент.

Приведем и докажем утверждение, позволяющее уменьшить вычислительную сложность приведенного алгоритма расчета θ_{min}. Утверждение: $((P-1)/2+1)$-й элемент мультипликативной группы G равен $P-1$.

Доказательство. $((P-1)/2+1)$-й элемент мультипликативной группы определяется из соотношения: $a_{(P-1)/2+1} = \Theta_v^{(P-1)/2} \pmod P$. В свою очередь необходимым и достаточным условием разрешенности сравнения вида $x^q \equiv A \pmod P$ **(4)** является $A^{\frac{P-1}{q}} \equiv 1 \pmod P$ [4]. Если $(A, P)=1$, а $q>1$ и есть делитель $P-1$, то (4) при $n=(P-1)/2$, $A=P-1$, $x=\Theta_v$ будет иметь вид $\Theta_v^{(P-1)/2} \equiv P-1 \pmod P$ **(5)**. Для доказательства (5) необходимо показать, что $(P-1)^{\frac{P-1}{(P-1)/2}} \equiv 1 \pmod P$. После несложных преобразований последнего выражения получим

$$(P-1)^{\frac{P-1}{(P-1)/2}} = (P-1)^2 = (P^2-2P+1) \bmod P \equiv (\bmod P).$$

Поэтому $a_{\frac{P-1}{2}+1} \equiv (P-1) \bmod P$. Утверждение доказано.

Приведенное утверждение позволяет сделать вывод о том, что для определения θ_{min} необходимо и достаточно выполнить не $P-1$ операций возведения в степени числа θ, а $(P-1)/2$. Данная методика положена в основу программы TETMIN вычисления минимального первообразного элемента поля.

Из теории чисел известно, что если период элемента a в поле GF(P) есть E (E — максимальный период элемента поля) и наибольший общий делитель (β, E) = 1, то период элемента $a^\beta = E = P - 1$, а значит a^β — первообразный элемент поля. Находя числа β, для которых выполняется условие (β E) = 1 и, возводя a в степень β, можно получить множество первообразных элементов поля GF(P). Общее число первообразных элементов $M = \varphi(P - 1)$, где $\varphi(\cdot)$ — функция Эйлера.

Для построения множества НП необходимо осуществлять расчет коэффициентов децимации, для которых выполняется условие (c, P — 1) = 1. Для расчета β и c взаимно простых с $P - 1$ может быть использован алгоритм Эвклида.

Число элементов НП выбирается в зависимости от требуемой величины частотной избыточности и характера ее реализации. Например, при ФМШПС величина L равна базе B используемого сигнала $L = B = \Delta f \cdot T_c$ **(6)**, где Δf — полоса частот, занимаемой ФМШПС; T_c — длительность сигнала.

В случае применения ППРЧ ФМ сигнала величина L также определяется из соотношения (6), однако в этом случае T_c — есть время изучения сложного сигнала на одной частоте. При этом величина $L = B$ выбирается из условия $B \geqslant B_{доп}$, где $B_{доп}$ — минимально допустимый выигрыш при обработке сигнала.

Список литературы: 1. *Свердлик М. Б.* Оптимальные дискретные сигналы. М., 1975. 200 с. 2. *Горбенко И. Д., Замула А. А.* Ускоренные алгоритмы формирования систем характеристических дискретных сигналов // Радиотехника. Вып. 84. С. 69—72. 3. *Горбенко И. Д., Замула А. А., Кулешов В. Л.* Корреляционные свойства систем характеристических дискретных сигналов // Радиотехника. Вып. 85. С. 96—100. 4. *Лидл Р., Нидеррайтер Г.* Конечные поля. В 2-х т.: Пер. с англ., М., 1988. Т. 2. 822 с.

Поступила в редколлегию 30.03.80