DOI: 10.18372/2410-7840.22.14868
УДК 512.6, 519.165, 519.725

АЛГОРИТМ СИНТЕЗА НЕПРИВОДИМЫХ ПОЛИНОМОВ ЛИНЕЙНОЙ СЛОЖНОСТИ

Анатолий Белецкий, Арсен Ковальчук, Константин Новиков, Дмитрий Полторацкий

Неприводимые полиномы находят широкое применение в различных областях науки и техники. Несмотря на большую востребованность синтез неприводимых полиномов до настоящего времени представляет собой достаточно сложную задачу и, как отмечено В. Жельниковым, «нахождение неприводимых полиномов до сих пор покрыто мраком. Криптографические службы высокоразвитых стран работали и работают над поиском многочленов как можно более высокой степени, но свои результаты они почти не освещают в открытой печати». Известные алгоритмы синтеза неприводимых полиномов обладают существенным недостатком, который состоит в том, что их вычислительная сложность является, как правило, квадратической. Следовательно, построение полиномов больших степеней может быть реализовано лишь на вычислительных комплексах весьма высокой производительности. Предлагаемый алгоритм опирается на так называемые реперные сетки (лестницы), число ступенек в которых совпадает со степенью синтезируемых полиномов. На каждой ступеньке лестницы осуществляются простейшие рекуррентные однотипные модулярные вычисления, по завершении которых тестируемый полином однозначно классифицируется или как неприводимый, или как составной. Разработанный алгоритм относится к подклассу алгоритмов линейной сложности. Суть рекуррентных операций на множестве двоичных полиномов сводится к вычислению остатков по модулю тестируемого на неприводимость полинома, представленного в векторной форме (набором бинарных коэффициентов полинома), от квадрата вычета, образованного на предыдущей ступеньке преобразования и дополненного справа нулем. Если верхняя (пороговая) степень синтезируемых полиномов не велика, например, не превышает двух десятков, то формирование множества тестируемых полиномов может осуществляться методом полного перебора. В том случае, когда степень полинома превышает пороговое значение, то их генерацию удобнее реализовывать статистическим моделированием. В работе кратко изложен алгоритм синтеза неприводимых полиномов над простым полем Галуа характеристики.

Ключевые слова: *неприводимые и составные полиномы, сингулярные полиномы, реперные сетки, сравнимость по модулю.*

1. Введение и постановка задачи

Неприводимые полиномы (НП), часто называемые *многочленами*, находят широкое применение в различных областях математики, информационной техники, современной теории передачи информации, при синтезе шумоподобных кодовых последовательностей, в теории помехоустойчивого кодирования, криптографии и др. отраслях науки и техники [1-9]. Несмотря на большую востребованность синтез НП до настоящего времени представляет собой достаточно сложную задачу и, как отмечено в [10], «нахождение неприводимых полиномов до сих пор покрыто мраком. Криптографические службы высокоразвитых стран работали и работают над поиском многочленов как можно более высокой степени, но свои результаты они почти не освещают в открытой печати». Основная проблема заключается в том, что известным алгоритмам синтеза НП присуща ни менее чем квадратическая сложность вычислений. А из этого следует, что с увеличением степени НП существенно возрастают затраты вычислительных ресурсов, необходимых для их построения.

Неприводимые полиномы играют роль сходную с простыми числами, которые, как и НП, обладают лишь тривиальными делителями. НП представимы двумя формами. Первой их них является так называемая «полиномиальная форма», которую мы будем именовать *алгебраической формой*:

$$f(x)=\sum_{k=0}^{n}\alpha_k x^k=\alpha_n x^n+\alpha_{n-1}x^{n-1}+\ldots+\alpha_k x^k+\ldots+\alpha_1 x+\alpha_0, \quad (1)$$

а в качестве второй служит векторная форма, являющаяся совокупностью коэффициентов α_k полинома, включая нулевые коэффициенты отсутствующих мономов ряда (1):

$$f=\alpha_n\alpha_{n-1}\ldots\alpha_k\ldots\alpha_1\alpha_0. \quad (2)$$

Двойственным к исходному полиному f является полином $\tilde{f}$, образованный инверсией полинома в алгебраической форме (1) или коэффициентов α_k в векторной форме (2). Например, векторная форма двойственного полинома имеет вид:

$$\tilde{f}=\alpha_0\alpha_1\ldots\alpha_k\ldots\alpha_{n-1}\alpha_n.$$

Выражения (1) и (2) представляют собой *естественные формы* записи НП, повсеместно применяемые, например, в позиционных системах счисления, в которых старшие разряды располагаются в левой части числа. Полиномы характеризуются рядом основных параметров. Одним из таковых является *степень полинома*, равная максимальной степени входящего в полином монома с ненулевым коэффициентом. Степень полинома n обозначается $\deg(f(x))$ – для алгебраической и $\deg(f)$ – для векторной формы. Вторым важнейшим параметром НП является его порядок. *Порядок полинома*, называемый также *периодом* или *экспонентой* [2], это наименьшее натуральное число m, при котором $f(x)$ оказывается делителем двучлена x^m-1, что отображается так:

$$f(x)\,|\,x^m-1. \qquad (3)$$

Поскольку x есть полином первой степени, равный 10 в векторной записи, то делимость (3) для векторного изображения полиномов можно представить формулой:

$$f\,|\,(10)^m-1 = f\,|\,1(0)^{[m]}-1,$$

где $(0)^{[m]} = \underbrace{00\ldots00}_{m\ \text{раз}}$.

Порядок полинома обозначается как $\mathrm{ord}(f(x))$ или $\mathrm{ord}(f)$ для алгебраической и векторной форм соответственно.

Различают *примитивные полиномы* (ПрП) и полиномы, *не являющиеся примитивными*. Последние для удобства будем именовать *простыми неприводимыми полиномами* (ПНП). Подмножества $\boldsymbol{Q}_{\text{ПрП}}$ и $\boldsymbol{Q}_{\text{ПНП}}$ – непересекающиеся подмножества полного множества $\boldsymbol{Q}$ полиномов одной и той же степени n, т.е. $\boldsymbol{Q}=\boldsymbol{Q}_{\text{ПрП}}\cup\boldsymbol{Q}_{\text{ПНП}}$, причём $\boldsymbol{Q}_{\text{ПрП}}\cap\boldsymbol{Q}_{\text{ПНП}}=0$. Если нет необходимости в конкретизации: является ли полином ПрП или ПНП, для простоты будем называть его *неприводимым полиномом*. Каждый ПрП является НП, тогда как обратное не всегда имеет место.

Число $M_p(n)$ неприводимых полиномов над простым полем Галуа $GF(p)$, в котором $p\ge 2$ – характеристика поля, являющаяся простым числом, определяется выражением [9]:

$$M_p(n)=\frac{1}{n}\sum_{k|n}\mu(k)\,p^{n/k},$$

где $\mu(k)$ – функция Мёбиуса, заданная следующим образом:

$$\mu(k)=\begin{cases}1, & \text{если } k=1;\\ (-1)^l, & \text{если } k-\text{проиведение } l\\ & \text{различных простых чисел;}\\ 0, & \text{в остальных случаях.}\end{cases}$$

Первые 32 функции $\mu(k)$ приведены в табл. 1.

Таблица 1

Функции Мёбиуса

k	μ	k	μ	k	μ	k	μ
1	1	9	0	17	-1	25	0
2	-1	10	1	18	0	26	1
3	-1	11	-1	19	-1	27	0
4	0	12	0	20	0	28	0
5	-1	13	-1	21	1	29	-1
6	1	14	1	22	1	30	-1
7	-1	15	1	23	-1	31	-1
8	0	16	0	24	0	32	0

Результаты расчётов числа неприводимых полиномов над полем $GF(2)$ для ряда значений n сведены в табл. 2.

Таблица 2

Число НП малых степеней

n	M	n	M	n	M	n	M
1	2	9	56	17	7’710	25	1’342’176
2	1	10	99	18	14’532	26	2’580’795
3	2	11	186	19	27’594	27	4’971’008
4	3	12	335	20	52’377	28	9’586’395
5	6	13	630	21	99’858	29	18’512’790
6	9	14	1’161	22	190’557	30	35’790’267
7	18	15	2’182	23	364’722	31	69’273’666
8	30	16	4’080	24	698’870	32	134’215’680

Из беглого просмотра табл. 2 следует, что начиная с $n=2$ практически $M(n+1)\approx 2M(n)$; т.е. увеличение на единицу степени НП приводит приблизительно к удвоению числа неприводимых полиномов. *Сложность вычислений*, обозначаемая $O(\cdot)$, известных методов синтеза НП [11-13] в зависимости от степени полинома n, как правило, не ниже квадратической, т. е. имеет место $O(n^2)$. Обычно сложность вычислений того или иного алгоритма оценивается ресурсами (машинным временем, объемом оборудования и т. д.), затрачиваемыми на его реализацию. Совершенно очевидно, что с ростом степени синтезируемых полиномов затраты машинного времени на их определение существенно возрастают.

Отмеченная проблема как раз и предопределяет направление исследования (цель) данной статьи и состоит в разработке нового эффективного алгоритма синтеза неприводимых полиномов (в

том числе и над полем Галуа $GF(p)$ характеристики $p>2$), сложность вычислений которых $O(n)$ растёт в *линейной зависимости* от степени полиномов n.

2. Концептуальные основы синтеза неприводимых полиномов

Ниже приведены ряд простых зачастую очевидных положений, сформулированных в виде аксиом (для краткости будем обозначать их $\boldsymbol{Ak}$, где k – натуральные числа), полученные в основном по результатам эмпирически установленных фактов и существенно облегчающие процесс вычисления НП.

$\boldsymbol{A}1$. Векторные формы двоичных НП обрамляются слева и справа единицами, т. е. имеют вид:

$$f_n = 1\alpha_{n-1}\alpha_{n-2}\ldots\alpha_k\ldots\alpha_1 1,\ \ \alpha_k = F_2 = \{0,1\}.$$

$\boldsymbol{A}2$. Вес совокупности внутренних коэффициентов $\alpha_k \in GF(2)$ полинома f_n степени n должен быть нечётным числом, так как в противном случае f_n делится без остатка на полином первой степени $f_1 = 11$ и, тем самым, тестируемый полином оказывается приводимым.

$\boldsymbol{A}3$. Максимальный порядок $\hat{L}_n$ НП f_n, определяется выражением:

$$\hat{L}_n = 2^n - 1. \qquad (4)$$

$\boldsymbol{A}4$. Если f – неприводимый полином, то и двойственный ему полином $\tilde{f}$ тоже является неприводимым.

$\boldsymbol{A}5$. Примитивным является НП максимального порядка.

$\boldsymbol{A}6$. Порядок L_n неприводимого полинома f_n совпадает с порядком элемента $\theta = 10$ поля $GF(2^n)$, порождаемого НП f_n.

$\boldsymbol{A}7$. Порядок L_n неприводимого полинома f_n является делителем максимального порядка $\hat{L}_n$, то есть соблюдается соотношение

$$L_n \,|\, \hat{L}_n = (2^n - 1). \qquad (5)$$

Некоторые аксиомы (такие, например, как $\boldsymbol{A}2$ **и** $\boldsymbol{A}6$**)** скорее всего подпадают под определение лемм ($\boldsymbol{A}7$ – по определению является теоремой [2]), но их доказательство не вызывает особых затруднений и может быть выполнено непосредственной проверкой. Именно на этом основании они и отнесены к разряду аксиом.

Проиллюстрируем применение вышеприведенных аксиом для решения задачи синтеза НП в интервале степеней $\deg(f) = \overline{2,4}$. Полиномы $f_0 = 1$ и $f_1 = \{10,11\}$ относятся к подклассу *вырожденных* ПрП.

Общую форму полинома второй степени запишем в виде: $f_2 = 1\alpha_1 1,\ \alpha_1 \in \{0,1\}$. Единственным вариантом значения коэффициента α_1 в f_2, сохраняющим условие аксиомы $\boldsymbol{A}2$, является $\alpha_1 = 1$, при этом полином $f_2 = 111$ оказывается ПрП. Обратимся к общей форме полиномов третьей степени $f_3 = 1\alpha_2\alpha_1 1$, которой отвечают четыре варианта бинарных внутренних коэффициентов $\alpha_2\alpha_1 = \{00, 01, 10, 11\}$, но только лишь для двух из них, а именно $\alpha_2\alpha_1 = \{01, 10\}$, соблюдаются условия аксиомы $\boldsymbol{A}2$. Допустимые значения коэффициентов порождают полиномы $f_3^{(1)} = 1011$ и $f_3^{(2)} = 1101$, являющиеся ПрП.

И, наконец, рассмотрим процедуру синтеза НП четвёртой степени, общая форма которых имеет вид: $f_4 = 1\alpha_3\alpha_2\alpha_1 1$. Нечётным весом обладают только лишь такие комбинации внутренних коэффициентов $\alpha_3\alpha_2\alpha_1 = \{001, 010, 100, 111\}$. Проверим делимость всех четырёх полиномов на НП второй степени $f_2 = 111$. Первый полином $f_4^{(1)} = 10011$ из совокупности не делится без остатка на f_2 и в силу этого оказывается неприводимым. Таким же неприводимым будет и полином $f_4^{(3)} = 11001$, являющийся двойственным полиному $f_4^{(1)}$. Кроме того, оба полинома $f_4^{(1)}$ и $f_4^{(3)}$ примитивные, в чём можно убедиться, воспользовавшись аксиомами $\boldsymbol{A}6$ и $\boldsymbol{A}7$. Полином $f_4^{(2)} = 10101$ приводимый, поскольку делится без остатка на f_2. Оставшийся полином $f_4^{(4)} = 11111$ – неприводимый, причём $\mathrm{ord}\left(f_4^{(4)}\right) = 5$, то есть относится к подмножеству ПНП.

Рассмотренная технология синтеза НП имеет ограничения по степени n полиномов, поскольку уже при $n \geq 28$ объём вычислений возрастает настолько, что ресурсов ПК может оказаться недостаточным для определения всего множества неприводимых полиномов f_n. В частности, если $n = 32$, то потребуется подвергнуть тестированию все нечётные (по весу) полиномы, верхняя оценка

числа которых составляет порядка одного миллиарда. С учетом того, что тестирование сводится к проверке делимости на все неприводимые полиномы в интервале степеней от 2 до 16, становится очевидным, что для определения полного множества НП f_{32} требуются вычислительные средства весьма высокой производительности.

3. Алгоритм тестирования полиномов на неприводимость

Введём ряд числовых параметров (см. табл. 3), «увязав» их с характеристиками так называемой *реперной сетки* (рис. 1), состоящей из совокупности параллельных прямых линий (*ступенек сетки*). Число ступенек r лестницы совпадает со степенью n тестируемого на неприводимость полинома f_n.

Таблица 3

Вспомогательные числовые параметры

r	1	2	3	4	5	6	7	8	…
t_r	1	3	7	15	31	63	127	255	…
Δ_r	1	2-3	4-7	8-15	16-31	32-63	64-127	128-255	…

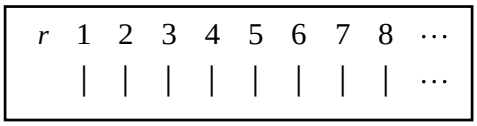

Рис. 1. Реперная сетка алгоритма синтеза НП

В табл. 3 приняты такие обозначения: r – номер ступеньки реперной сетки; t_r – степень двоичного полинома CV_r, назовём его *координатным вектором* (Coordinate Vector), левый разряд которого равен 1, а остальные заполнены нулями, то есть

$$CV_r = \underset{t_r}{100...0}.$$

Таким образом, t_r есть ни что иное, как порядок нулевого вектора полинома CV_r. Число нулевых разрядов полинома CV_r определяется формулой (6), то есть $t_r = 2^r - 1$. И, наконец, через Δ_r в табл. 3 обозначен диапазон изменений допустимых значений степеней тестируемых полиномов (ТП), отвечающих выбранному номеру r ступеньки реперной сетки. Нижняя $\Delta_{r,\,down}$ и верхняя $\Delta_{r,\,top}$ границы интервала Δ_r заданы функциями $\Delta_{r,\,down} = 2^{r-1}$ и $\Delta_{r,\,top} = 2^r - 1$ соответственно.

Взаимосвязь векторов CV_r с интервалами Δ_r степеней ТП для $r = 3$ можно проследить по табл. 4, в которой переменные $b \in \{0,1\}$ выбираются такими, чтобы их совокупный вес в полиномах равнялся (согласно аксиоме $\boldsymbol{A}2$) нечётному числу.

Таблица 4

К пояснению взаимосвязи параметров CV_3 и Δ_3

CV_3		1	0	0	0	0	0	0	0
		Структура ТП							
Δ_3	4	1	b	b	b	1			
	5	1	b	b	b	b	1		
	6	1	b	b	b	b	b	1	
	7	1	b	b	b	b	b	b	1

Тестирование полиномов на неприводимость сводится к выполнению ряда вычислительных операций, которые в необходимых случаях для наглядности мы будем подкреплять числовыми примерами. Алгоритм тестирования базируется на аксиоме $\boldsymbol{A}7$. Придадим $\boldsymbol{A}7$ форму, несколько отличную от той, что определена соотношением (5). С этой целью сформулируем следующее

Утверждение 1. Необходимым условием неприводимости двоичного полинома f_n степени n является выполнение сравнения

$$1(0)^{2^n-1} \equiv 1 \pmod{f_n},\ n \geq 2. \qquad (6)$$

Доказательство. Перепишем (6), представив сравнение в таком виде

$$(10)^{\hat{L}_n} \equiv 1 \pmod{f_n}. \qquad (7)$$

Левая компонента $(10)^{\hat{L}_{n,}}$ сравнения (7) представляет собой координатный вектор

$$CV_n = 1\underbrace{00\ldots0}_{2^n-1\ \text{бит}}. \qquad (8)$$

В свою очередь бинарный вектор, отвечающий порядку $\hat{L}_n$, состоит исключительно из n единиц. Назовем этот вектор *вектором единиц* (Unit Vector), как антипод *нулевому вектору* (то есть вектор, инициализированный единицами), и обозначим

$$UV_n = \underbrace{11\ldots11}_{2^n-1\ \text{бит}}. \qquad (9)$$

Сравнения (6) и (7) фактически являются аналогами аксиомы **A7**. Десятичное значение вектора (8) на единицу больше значения вектора (9). Поэтому если соблюдается условие (5), то тем самым подтверждается и сравнение (6). На этом заканчивается доказательство Утверждения 1. Как будет показано в п. 4, сравнение (6) является необходимым, но не для всех n обязательным условием неприводимости ТП.

Проиллюстрируем соотношения (6) и (7) числовым примером, выбрав в качестве тестируемого один из НП четвёртой степени. Пусть $f_4^{(1)} = 10011$, являющийся ПрП. Выпишем координатный вектор

$$CV_4 = 1\underbrace{00\ldots0}_{15\ бит}. \qquad (10)$$

Поделив правую часть вектора (10) на $f_4^{(1)}$, получим $Res(CV_4)_{f_4^{(1)}} = 1$, где обозначено $Res(a)_b = a \pmod b$ – вычет числа a по модулю b. Следовательно, согласно Утверждению 1, $f_4^{(1)}$ – неприводимый полином. К такому же результату приходим для варианта ПНП $f_4^{(3)} = 11111$, поскольку $Res(CV_4)_{f_4^{(3)}}$ так же как и $Res(CV_4)_{f_4^{(1)}}$ равен 1.

Обратимся к альтернативному варианту, выбрав в качестве ТП $f_4 = 10101$. Для анализируемого полинома $Res(CV_4)_{f_4} = 1000 \neq 1$, а из этого следует, что f_4 – приводимый (т.е. составной) полином.

Порядок координатных векторов CV_n, согласно (8), растёт экспоненциально в зависимости от степени n тестируемых полиномов f_n. И, как следствие, уже при $n \geq 30$ воспользоваться Утверждением 1 на стандартных ПК практически невозможно, поскольку на его реализацию требуются непреодолимо большие затраты машинного времени. Данную проблему можно обойти, применяя предлагаемый ниже линейный алгоритм тестирования полиномов.

Отобразим реперную сетку, соответствующую полиному f_n, вектором $1^{[n]}$, содержащим n единиц, т. е. пусть $1^{[n]} = \underbrace{11\ldots11}_{n\ бит}$. Каждая $r-$я единица в $1^{[n]}$ символизирует координатный вектор CV_r ($r-$ю ступеньку реперной сетки). Закон изменения порядков t_r нулевых разрядов векторов CV_r можно легко установить, анализируя данные средней строки в табл. 3, а именно:

$$t_r = 2 \cdot t_{r-1} + 1, \quad t_0 = 0, \quad r = \overline{1,n}. \qquad (11)$$

Введем ряд обозначений. Пусть $s_r = Res(CV_r)_f$ – вычет координатного вектора CV_r по модулю полинома f. Соотношения (11) составляют *фундаментальную основу* предлагаемого алгоритма тестирования двоичных полиномов на неприводимость, которое сводится к последовательности простых рекуррентных вычислений

$$\begin{gathered} s_r = Res(s_{r-1} \cdot s_k)_f, \\ s_0 = 1,\ s_r = s_{r-1}0, \\ r = \overline{1,n}, \end{gathered} \qquad (12)$$

где s_r – *расширенный* (дополненный справа нулем) вычет координатного вектора CV_{r-1}. При достижении индексом r последней $n-$й ступеньки реперной лестницы если окажется, что $s_n = 1$, то это будет означать, в соответствии с Утверждением 1, выполнение необходимых условий неприводимости ТП.

Придадим последовательности вычетов (12) простую интерпретацию. Согласно выражению (11), ассоциированному со значениями, перечисленными во второй строке табл. 3, координатный вектор CV_r, отвечающий $r-$й ступеньке реперной сетки, можно записать в виде

$$CV_r = CV_{r-1} \cdot CV_{r-1}0 = CV_{r-1}^2 0, \qquad (13)$$

которое на основании формулы (10) представим бинарным вектором

$$CV_r = 1\underbrace{00\ldots00}_{2^r-1\ бит} = 1\overbrace{\underbrace{00\ldots00}_{2^{r-1}-1\ бит}}^{CV_{r-1}}1\overbrace{\underbrace{00\ldots00}_{2^{r-1}-1\ бит}}^{CV_{r-1}}0. \qquad (14)$$

Вычисляя остатки по $\bmod f$ от компонент, обрамляющих равенство (14), приходим к оценке s_k:

$$\boldsymbol{S}_r = Res(CV_r)_f = Res(CV_{r-1}CV_{r-1}0)_f = Res(\boldsymbol{S}_{r-1}\boldsymbol{S}_{r-1}0)_f, \quad (15)$$

совпадающее с оценкой (12).

Развёртывание алгоритма (15) проиллюстрируем числовым примером, выбрав для тестирования априори неприводимый полином 12-й степени $f_{12}^{(1)} = 1000000001111$. Значения вычетов $\boldsymbol{S}_r$ векторов CV_r по модулю $f_{12}^{(1)}$ сведены в табл. 5.

Таблица 5

Последовательность вычетов, порождаемая полиномом $f_{12}^{(1)}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_5 = 101010011110;$	$\boldsymbol{S}_9 = 110111111100;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_6 = 110101111101;$	$\boldsymbol{S}_{10} = 110100000100;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_7 = 110101111110;$	$\boldsymbol{S}_{11} = 11111100010;$
$\boldsymbol{S}_4 = 1111000;$	$\boldsymbol{S}_8 = 110101110100;$	$\boldsymbol{S}_{12} = \mathbf{1}.$

Тот факт, что вычет $\boldsymbol{S}_{12}$ оказался равным 1, является свидетельством выполнения, по крайней мере, необходимых условий неприводимости полинома $f_{12}^{(1)}$.

Полезным для построения алгоритма синтеза НП является такое

Утверждение 2. Вычет координатного вектора CV_r по модулю НП f_n степени n достигает единицы только лишь при $r = n$, тогда как в противном случае, когда $r < n$,

$$CV_r \pmod{f_n} \neq 1.$$

Другими словами, если CV_r по модулю f_n на внутренней ступеньке реперной лестницы равен 1, то это будет означать, что f_n – составной полином.

К доказательству утверждения 2 легко приходим, опираясь на числовые примеры. В частности, если степень НП – двоично-рациональное число (см. п. 5), т.е. $n = 2^m$, где $m-$ натуральное число, то максимальный порядок $\hat{L}_n$ полинома f_n, которым обладает ПрП, может быть представлен произведением двучленов

$$\hat{L}_n = 2^n - 1 = (2^1+1)\cdot(2^2+1)\cdot(2^4+1)\cdot\ldots\cdot(2^k+1)\cdot\ldots\cdot(2^{n/2}+1). \quad (16)$$

Порядок L_n НП f_n, не являющегося примитивным, определяется произведением той или иной совокупности двучленов разложения (16), составляющих множество простых делителей (множителей) числа $\hat{L}_n$. Обратимся к табл. 3. Средняя строка таблицы содержит числа $t_r = 2^r - 1$, совпадающие с максимальным порядком полиномов f степени r. Совершенно очевидно, что не существует такого подмножества двучленов в (16), образованных *суммой* одночленов, произведение которых могло бы быть равным двучлену t_r, составленному *разностью* одночленов. А из этого однозначно следует, что если единичный вычет координатного вектора CV_r по модулю f_n появляется на $r-$й ступеньке реперной сетки r, то f_n является составным полиномом, причём степень одного из полиномов сомножителей равна r.

Для подтверждения сформулированного вывода рассмотрим числовой пример. Пусть $f_{10} = 11101000001$, которому отвечают вычеты, сведенные в табл. 6.

Таблица 6

Последовательность вычетов, порождаемая полиномом f_{10}

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_5 = 1110010;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_6 = 1110000110;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_7 = 1001001011;$
$\boldsymbol{S}_4 = 100110100;$	$\boldsymbol{S}_8 = 1.$

На основании данных табл. 6 приходим к такому результату: полином f_{10} является составным и степень одного их них равна восьми, а второго, естественно, двум. Полином f_8 также может оказаться составным, что, при необходимости, может уточняться отдельным тестированием. Так как $f_2 = 111$, то полином $f_8 = f_{10} / f_2 = 100011011$ оказывается неприводимым и, тем самым, отпадает потребность в дополнительном тестировании полинома f_8.

4. Синтез неприводимых полиномов малых степеней

К малым будем относить степени n полиномов f_n, не превышающие 64**.** Разобьём дополнительно совокупность полиномов малых степеней на две группы, включив в первую из них полиномы, степени которых принадлежат интервалу [2-32], а во вторую – интервалу [33-64]. Аналитические оценки числа $M(n)$ неприводимых полиномов малых степеней первой группы приведены выше в табл. 2.

Назовём *сингулярными* (исключительными) такие НП, степени которых являются: (*а*) простыми

числами, (*b*) степенями простых чисел или (*c*) произведением двух различных простых чисел. Сингулярные НП малых степеней первой группы выделены затенением в табл. 6, а второй группы – в табл. 7.

Таблица 6

Степени полиномов первой группы

	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

Таблица 7

Степени полиномов второй группы

33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

На основании компьютерных вычислений для сингулярных полиномов эмпирически установлена следующая

Теорема 1. Сингулярный полином f_n степени n неприводим тогда и только тогда, когда вычет S_n координатного вектора CV_n, отвечающий $n-$й ступеньке реперной сетки, по модулю f_n равен единице, то есть обеспечивается тождество $S_n \equiv 1$ (*необходимое условие*), причём ни при каких $r < n$ вычет S_r не может быть равным единице (*достаточное условие*).

Подкрепим теорему 1 числовыми примерами. В качестве первого рассмотрим тестирование априори НП 15-й степени $f_{15}^{(1)} = 1010011011000111$ (табл. 8).

Таблица 8

Последовательность вычетов, порождаемая полиномом $f_{15}^{(1)}$

$S_1 = 10;$	$S_6 = 100011110011101;$	$S_{11} = 11110100001101;$
$S_2 = 1000;$	$S_7 = 100000011001001;$	$S_{12} = 101110110101000;$
$S_3 = 10000000;$	$S_8 = 10110111011;$	$S_{13} = 10001100101111;$
$S_4 = 10011011000111;$	$S_9 = 1101010110100;$	$S_{14} = 11011101000110;$
$S_5 = 111111111000;$	$S_{10} = 100010100100011;$	$S_{15} = \mathbf{1}.$

Поскольку необходимые и достаточные условия теоремы 1 соблюдаются, то это означает, что полином $f_{15}^{(1)}$ является неприводимым.

Рассмотрим далее полином $f_{15}^{(2)} = 1010100101000011.$ Произведя вычисления остатков координатных векторов CV_r по модулю $f_{15}^{(2)}$, получим результаты в табл. 9.

Таблица 9

Последовательность вычетов, порождаемая полиномом $f_{15}^{(2)}$

$S_1 = 10;$
$S_2 = 1000;$
$S_3 = 10000000;$
$S_4 = 10100101000011;$
$S_5 = 1;$

Пятиэлементные второй и третий столбцы вычетов в табл. 9 повторяют элементы первого столбца и на этом основании они опущены. Достаточные условия теоремы 1 для полинома $f_{15}^{(2)}$ не выполняются, поскольку последовательность вычетов S_r, $r = \overline{1,15}$, содержит три единицы. Такими вычетами являются S_5, S_{10} и S_{15}. А это означает, что полином $f_{15}^{(2)}$ является приводимым. И, наконец, если ТП $f_{15}^{(3)}$ априори приводимый, например, образован произведением двух НП, то выполнив вычисления остатков, получим $S_{15} \neq 1$. Тем самым подтверждается, что $f_{15}^{(3)}$ – приводимый полином, как это и было предопределено изначально.

Полиномы, не являющиеся сингулярными, а к таковым, например, относятся полиномы, степени которых указаны в светлых ячейках табл. 6 и 7, обладают рядом специфических особенностей. Во-первых, оба условия (как необходимое, так и достаточное) теоремы 1 являются необходимыми условиями неприводимости *несингулярных полиномов* (НСП). И, во-вторых, достаточным условием неприводимости НСП, как это установлено эмпирически компьютерным моделированием, является отсутствие для таких полиномов так называемых «исключающих делителей». К *исключающим*

делителям будем относить такие НП, которые делят без остатка тестируемый несингулярный полином. Множество исключающих делителей тестируемых полиномов степени n будем обозначать $\tilde{d}_n$. Совокупность исключающих делителей НСП, содержащихся в табл. 6 и 7, приведена в табл. 10. Во втором столбце слева таблицы под знаком «=» представлены произведения простых множителей числа n вместе с их кратностями.

Таблица 10

Исключающие делители несингулярных полиномов

Степень ТП		Степени полиномов исключающих делителей								Степень ТП		Степени полиномов исключающих делителей							
n	=	2	3	4	5	6	7	8	9	n	=	2	3	4	5	6	7	8	9
12	$2^2\cdot 3$	+								44	$2^2\cdot 11$	+							
18	$3^2\cdot 2$		+							45	$3^2\cdot 5$		+						
20	$2^2\cdot 5$	+								48	$2^4\cdot 3$	+		+				+	
24	$2^3\cdot 3$	+		+						50	$5^2\cdot 2$				+				
28	$2^2\cdot 7$	+								52	$2^2\cdot 13$	+							
30	$2\cdot 3\cdot 5$	+	+		+					54	$3^3\cdot 2$		+						+
36	$2^2\cdot 3^2$	+	+			+				56	$2^3\cdot 7$	+		+					
40	$2^3\cdot 5$	+		+						60	$2^2\cdot 3\cdot 5$	+	+	+	+				
42	$2\cdot 3\cdot 7$	+	+				+			63	$3^2\cdot 7$		+						

На основании данных табл. 10 приходим к обобщениям, подтверждённых результатами компьютерного моделирования:

Утверждение 3. Множества исключающих делителей $\tilde{d}_n$ тестируемых на неприводимость несингулярных полиномов f_n степени n определяются выражениями:

$$\tilde{d}_n \in \begin{cases} \bigcup_{i=1}^{k-1} \overline{p}_1^{\,i}, \text{ если } n = p_1^k \cdot p_2, k \geq 2; \\ \bigcup_{i=1}^{k} \overline{p}_i, \text{ если } n = \bigcap_{i=1}^{k} p_i, k > 2; \\ \overline{p}_1 \cup \overline{p}_2 \cup \overline{p}_1 \cdot \overline{p}_2, \text{ если } n = p_1^k \cdot p_2^k, k \geq 2, \end{cases} \quad (17)$$

где p_i – простые числа, $\overline{p}_1^{\,i}$ – совокупность неприводимых полиномов степени p_1^i.

Разумеется, системой (17) не исчерпывается и малая доля многообразия вариантов разложения степеней n тестируемых полиномов f_n, каждому из которых отвечает собственный набор исключающих делителей $\tilde{d}_n$.

Но для приложений, например, в криптографии, как правило оказывается, что их вполне достаточно.

Эмпирически установлена следующая:

Теорема 2. Несингулярный полином f_n степени n неприводим тогда и только тогда, когда единственным вычетом координатного вектора CV_r по модулю f_n, равным единице, является вычет, отвечающий $n-$й ступеньке реперной сетки, то есть когда обеспечивается тождество $\boldsymbol{S}_n \equiv 1$ (*необходимое условие*), причём для тестируемого полинома не существует исключающих делителей (*достаточное условие*).

Обратимся к числовым примерам.

Пример 1. Рассмотрим несингулярный полином $f_{18}^{(1)} = 1010011010110101011$. Последовательность вычетов $\boldsymbol{S}_r$ координатных векторов CV_r по модулю $f_{18}^{(1)}$ представлена в табл. 11. Старшая половина последовательности вычетов (по значениям их индексов) повторяет младшую и на этом основании выброшена из таблицы.

Таблица 11

Последовательность вычетов, порождаемая полиномом $f_{18}^{(1)}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_4 = 1000000000000000;$	$\boldsymbol{S}_7 = 1101000000010110110;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_5 = 10100100100011100;$	$\boldsymbol{S}_8 = 1000111011011000;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_6 = 100000011111111001;$	$\boldsymbol{S}_9 = \mathbf{1}.$

Как следует из табл. 11, необходимое условие неприводимости ТП не соблюдается, а это означает, что $f_{18}^{(1)}$ — приводимый полином.

Пример 2. Пусть $f_{18}^{(2)} = 1010011011010011011$. Совокупность вычетов, отвечающая полиному $f_{18}^{(2)}$, сведена в табл. 12.

Таблица 12

Последовательность вычетов, порождаемая полиномом $f_{18}^{(2)}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_7 = 110100101100100011;$	$\boldsymbol{S}_{13} = 101111101101101001;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_8 = 111011111010100011;$	$\boldsymbol{S}_{14} = 10000110011010000;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_9 = 1111001100010000;$	$\boldsymbol{S}_{15} = 111001111110110000;$
$\boldsymbol{S}_4 = 1000000000000000;$	$\boldsymbol{S}_{10} = 100111101101101011;$	$\boldsymbol{S}_{16} = 10011000001001010;$
$\boldsymbol{S}_5 = 10111101110110100;$	$\boldsymbol{S}_{11} = 111011101101100;$	$\boldsymbol{S}_{17} = 111100100111000111;$
$\boldsymbol{S}_6 = 1101101100101000001;$	$\boldsymbol{S}_{12} = 1111001110010001;$	$\boldsymbol{S}_{18} = \boldsymbol{1}.$

Несмотря на то, что для $f_{18}^{(2)}$ необходимые условия неприводимости выполнены, полином $f_{18}^{(2)}$ не свободен от исключающего делителя $\tilde{d}_n$, которым, в соответствии с табл. 10, оказывается ПрП третьей степени $f = 1011$. Следовательно, $f_{18}^{(2)}$ – приводимый полином. Назовем полиномы несингулярной группы, поддерживающие необходимые условия неприводимости (по теореме 2), но для которых существуют исключающие делители, *ложно неприводимыми полиномами*. Таковым как раз и является полином $f_{18}^{(2)}$.

И, наконец, пусть $f_{18}^{(3)} = 1101010111001011001$. Множество вычетов, формируемое на реперной сетке полиномом $f_{18}^{(3)}$, представлено в табл. 13. У полинома $f_{18}^{(3)}$ нет исключающих делителей. Следовательно, $f_{18}^{(3)}$ – неприводимый полином.

Таблица 13

Последовательность вычетов, порождаемая полиномом $f_{18}^{(3)}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_7 = 101010100101010001;$	$\boldsymbol{S}_{13} = 1011111011111110;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_8 = 101110100000110110;$	$\boldsymbol{S}_{14} = 111000111010010110;$
$\boldsymbol{S}_3 = 10000000;$	$\boldsymbol{S}_9 = 110000000101001100;$	$\boldsymbol{S}_{15} = 101000110101101011;$
$\boldsymbol{S}_4 = 1000000000000000;$	$\boldsymbol{S}_{10} = 100111101101101111;$	$\boldsymbol{S}_{16} = 10010111110100;$
$\boldsymbol{S}_5 = 111010101100011001;$	$\boldsymbol{S}_{11} = 111110111000101001;$	$\boldsymbol{S}_{17} = 110110101101010;$
$\boldsymbol{S}_6 = 101100101010001011;$	$\boldsymbol{S}_{12} = 110001011011000101;$	$\boldsymbol{S}_{18} = \boldsymbol{1}.$

И в заключении раздела сформулируем признаки неприводимости полиномов f_n чётных степеней n, во всех разрядов которых содержатся единички. Подобные полиномы названы выше «векторами единиц». Очевидны следующие наблюдения:

Теорема 3. Единичный $(n+1)-$го порядка вектор $1^{[n+1]}$ является неприводимым полиномом f_n чётной степени n тогда и только тогда, когда $(n+1) \mid \hat{L}_n$ (*необходимые условия*), при том что $(n+1) \nmid \hat{L}_{n/2}$ (*достаточные условия*).

Результаты приложения теоремы 3 проиллюстрированы в табл. 14.

Таблица 14

Признаки неприводимости полиномов $f_n = 1^{[n+1]}$ чётных степеней

Первая группа НП малых степеней						Вторая группа НП малых степеней					
Степень	Н/У	Д/У	Степень	Н/У	Д/У	Степень	Н/У	Д/У	Степень	Н/У	Д/У
4	+	+	20	−		34	−		50	−	
6	−		22	+	−	36	+	+	52	−	
8	−		24	−		38	−		54	−	
10	+	+	26	−		40	+	−	56	−	
12	+	+	28	+	+	42	+	+	58	−	
14	−		30	+	−	44	−		60	−	
16	+	−	32	−		46	+	−	62	−	
18	+	+				48	−		64	−	

Затенением в табл. 14 выделены степени полиномов $f_n = 1^{[n+1]}$, для которых соблюдаются как необходимые (Н/У), так и достаточные (Д/У) условия неприводимости.

5. Синтез неприводимых полиномов двоично-рациональных степеней

К *двоично-рациональным* (термин заимствован из [14]) будем относить полиномы, степени которых n равны 2^k, где k – натуральные числа. Такие НП достаточно широко востребованы в криптографии и других разделах дискретной математики. Рассматриваемые полиномы f_n относятся к группе сингулярных НП. Их синтез базируется на теореме 1, согласно которой тестируемый полином неприводимый, если вычет координатных векторов CV_k по модулю f_n достигает единичного значения лишь на последней $n-$й ступеньке реперной сетки. Сингулярные полиномы двоично-рациональных степеней свободны от исключающих делителей. Перечисленные свойства полиномов значительно упрощают процедуру их синтеза. Однако сохраняется проблема, обусловленная не малыми затратами машинного времени при решении задачи оценки порядка полиномов и, соответственно, их классифицирования на примитивные (НП максимального порядка) и простые неприводимые (т. е. не являющиеся примитивными) полиномы. Обсуждение данной проблемы как раз и составляет содержание текущего раздела статьи.

Дополним аксиоматические основы синтеза НП, изложенные в п. 2, рядом полезных сведений, касающихся полиномов двоично-рациональных степеней. Обозначим:

1) $D_{1,n} = \{d_1, d_2, \ldots d_k, \ldots, d_m\}$ – упорядоченное подмножество *простых делителей* d_k, $d_k < d_{k+1}$, порядка $\hat{L}_n$ ПрП f_n, исключая тривиальные делители;

2) $D_{l,n} = \{\bullet\}$ – упорядочные подмножества *составных делителей* $\hat{L}_n$, образованные сочетаниями из m элементов подмножества $D_{1,n}$ по l, $l = \overline{2, m-1}$, исключая делитель $\hat{L}_n$. Параметр m равен числу простых делителей $\hat{L}_n$;

3) $\hat{D}_n = D_{1,n} \cup D_{l,n}$ – полное упорядоченное множество делителей $\hat{L}_n$, составленное из элементов подмножеств $D_{1,n}$ и $D_{l,n}$.

Полиномы двоично-рациональных степеней обладают замечательным свойством, суть которого состоит в следующем. Поскольку n — чётное число, то максимальный порядок $\hat{L}_n$ полиномов f_n может быть представлен в виде

$$\hat{L}_n = 2^n - 1 = \left(2^{n/2} - 1\right) \cdot \left(2^{n/2} + 1\right), \qquad (18)$$

где, в свою очередь, $n/2$ также является чётным числом, поскольку по определению $n = 2^k$.

Опираясь на приведенное свойство, легко выписать разложение числа $\hat{L}_n$ для полиномов двоично-рациональных степеней. Ниже показана цепочка разложения двучлена (18) на примере $n=32$:

$$\begin{gathered}\hat{L}_{32}=2^{32}-1=(2^{16}-1)\cdot(2^{16}+1)=\\(2^{8}-1)\cdot(2^{8}+1)\cdot(2^{16}+1)=\\(2^{4}-1)\cdot(2^{4}+1)\cdot(2^{8}+1)\cdot(2^{16}+1)=\\(2^{2}-1)\cdot(2^{2}+1)\cdot(2^{4}+1)\cdot(2^{8}+1)\cdot(2^{16}+1)=\\(2^{1}+1)\cdot(2^{2}+1)\cdot(2^{4}+1)\cdot(2^{8}+1)\cdot(2^{16}+1),\end{gathered}\qquad(19)$$

согласно которому *простые делители*, составленные из сомножителей нижней строки разложения (19),

$$D_{1,32}=3,5,17,257,65'537,\qquad(20)$$

образуют последовательность простых чисел Ферма [15]:

$$F_k=2^{2^k}+1,\ k=\overline{0,4}.\qquad(21)$$

Полное упорядоченное множество делителей максимального порядка $\hat{L}_{32}$ полиномов 32 степени таково:

$$\begin{gathered}\hat{D}_{32}=\{3,\ 5,\ 15,\ 17,\ 51,\ 85,\ 255,\ 257,\ 771,\ 1'285,\\3'855,\ 4'369,\ 13'107,\ 21'845,\ 65'535,\ 65'537,\\196'611,\ 327'685,\ 983'055,\ 1'114'129,\ 3'342'387,\\5'570'645,\ 16'711'935,\ 16'843'009,\ 50'529'027,\\84'215'045,\ 252'645'135,\ 286'331'153,\\858'993'459,\ 1'431'655'765\}.\end{gathered}\qquad(22)$$

Если f_n-НП степени n и на множестве $\hat{D}_n$ найдётся такой элемент $d\in\hat{D}_n$, при котором $f_n\,|\,(x^d-1)$, то f_n есть ПНП порядка d, иначе — ПрП.

Обобщённую форму (полную совокупность) простых делителей, как это следует из соотношений (20) и (21), можно представить в виде:

$$D_{1,2^{k+1}}=\bigcup_{i=0}^{k}F_i,\qquad(23)$$

причём начиная с $k=5$ числа Фибоначчи F_k оказываются составными.

Последовательность простых делителей (23) двучлена (18) обеспечивает возможность определения полного множества $\hat{D}_n$ делителей максимально порядка $\hat{L}_n$ НП f_n. Число компонентов N_n множества $\hat{D}_n$, для двоично-рациональных значений n определяется формулой

$$N_n=\sum_{k=1}^{\log_2 n-1}\binom{\log_2 n}{k}=n-2.$$

С ростом n увеличиваются затраты машинного времени, связанные с классифицированием тестируемых полиномов (вычислением их порядков и отнесением или к классам ПНП, или ПрП). Указанные затраты можно уменьшить, приняв во внимание следующее эмпирически установленное

Утверждение 4. Минимальный порядок НП f_n двоично-рациональной степени $n=2^k$ превышает порядок ПрП степени $\bar{n}=2^{k-1}$, то есть

$$ord_{\min}(f_n)>2^{\bar{n}}-1.\qquad(24)$$

В частности, на основании неравенства (24) подмножество делителей, выделенное затенением в последовательности (22), можно исключить из процедуры вычисления порядка тестируемых полиномов f_{32}.

Если степень n двоично-рациональных полиномов f_n не превышает 16, то синтез НП вполне может опираться на полный перебор возможных вариантов полиномов с последующим их тестированием на неприводимость. В том случае, когда $n\geq 32$, полный перебор, по крайней мере на ПК, становится практически не реализуемым. Единственным способом формирования таких полиномов становится их статистическое моделирование. Как показали результаты экспериментальной проверки для формирования одного НП степени 2 Кбит затраты машинного времени на компьютерах средней производительности составляют порядка 2.5 часов, что является вполне удовлетворительным результатом.

6. Синтез неприводимых полиномов над полем $GF(p)$, $p\geq 3$

В данном параграфе обобщаются результаты предыдущих разделов статьи и тем самым решается задача построения алгоритмов синтеза НП над полем Галуа характеристики $p\geq 3$. Числовые параметры, связанные с полиномами над $GF(p)$, $p\geq 3$, будем дополнительно снабжать ещё одним нижним индексом p.

Обратимся к табл. 3. В её средней строке параметр t_r определяет число нулей, содержащихся в двоичном координатном векторе CV_r, который соответствует $r-$й ступеньки реперной сетки. Для $p-$ичной системы счисления $t_{r,p}=p^r-1$ и, вследствие этого, например, если $p=3$, то табл. 3 трансформируется в нижеследующую табл. 15.

Таблица 15

Числовые параметры реперной сетки для характеристики $p=3$

r	1	2	3	4	5	6	7	8	…
$t_{r,3}$	2	8	26	80	242	728	2186	65600	…
$\Delta_{r,3}$	2	3-8	9-26	27-80	81-242	243-728	729-2186	2187-65600	…

Аппроксимация числовой последовательности $t_{r,p}$ имеет вид

$$t_{r,3}=3\cdot t_{r-1,3}+2,\quad t_{0,3}=0. \qquad (25)$$

На основании сопоставления выражений (11)-(13) и (25) приходим к таким обобщённым соотношениям

$$t_{r,p}=p\cdot t_{r-1,p}+(p-1),\quad t_{0,p}=0;$$

и

$$\boldsymbol{S}_{r,p}=Res(\boldsymbol{S}_{r-1,p}^{p}\underbrace{0...0}_{p-1})_f,\quad \boldsymbol{S}_{0,p}=1. \qquad (26)$$

Рассмотрим числовые примеры. Выберем в качестве тестируемого априори неприводимый над $GF(3)$ полином пятой степени $f_5^{(1)}=102112$. Воспользовавшись рекуррентной формулой (26), вычислим последовательность вычетов по модулю $f_5^{(1)}$ и сведём её в табл. 16.

Таблица 16

Последовательность вычетов, порождаемая полиномом $f_5^{(1)}$

$$\boldsymbol{S}_1=100;$$
$$\boldsymbol{S}_2=2022;$$
$$\boldsymbol{S}_3=22222;$$
$$\boldsymbol{S}_4=12021;$$
$$\boldsymbol{S}_5=1.$$

В качестве альтернативного рассмотрим полином $f_5^{(2)}$, не являющийся априори неприводимым. Предположим, что $f_5^{(2)}$ образован модульным произведением (т. е. без учета межразрядных переносов) двух НП над $GF(3)$. Пусть таковыми являются $f_3=1121$ и $f_2=112$, порождающие составной полином $f_5^{(2)}=1121\overset{3}{\otimes}112=122222$. Полиному $f_5^{(2)}$ соответствуют вычеты, сведенные в табл. 17.

Таблица 17

Последовательность вычетов, порождаемая полиномом $f_5^{(2)}$

$$\boldsymbol{S}_1=100;$$
$$\boldsymbol{S}_2=22101;$$
$$\boldsymbol{S}_3=22121;$$
$$\boldsymbol{S}_4=11010;$$
$$\boldsymbol{S}_5=11221.$$

Содержимое табл. 16 и 17 подтверждает априорную информацию относительно полиномов $f_5^{(1)}$ и $f_5^{(2)}$. И в заключении раздела отметим, что технология синтеза НП над $GF(p)$, $p\geq 3$, сохраняется такой же простой (и линейно сложной), как и для двоичных полиномов.

Выводы

Основным результатом статьи является разработка оригинального линейной сложности алгоритма синтеза неприводимых полиномов в широком диапазоне степеней, достигающих нескольких Кбит. Известные алгоритмы генерации НП обладают существенным недостатком, который состоит в том, что их вычислительная сложность является, как правило, не менее чем квадратической. А из этого следует, что для построения НП больших степеней необходимо привлекать вычислительные ресурсы весьма высокой производительности. Предлагаемый алгоритм синтеза базируется на так называемых реперных сетках (лестницах), число ступенек в которых совпадает со степенью синтезируемых полиномов. На каждой ступеньке лестницы осуществляются простейшие однотипные рекуррентные модулярные вычисления, по завершении которых тестируемый полином однозначно классифицируется или как неприводимый, или как составной. Разработанный алгоритм может быть не только продолженным на решение задачи синтеза НП с коэффициентами из поля Галуа произвольной характеристики, но и применен для факторизации степеней составных полиномов.

ЛИТЕРАТУРА

[1]. В. Прасолов, *Многочлены*, М.: МЦНМО, 2001, 336 с.

[2]. R. Lidl, H. Niederreiter, *Finite Fields,* Cambridge University Press, 1996.

[3]. О. Василенко, *Теоретико-числовые алгоритмы в криптографии*, М.: МЦНМО, 2003, 328 с.

[4]. В. Фомичёв, *Дискретная математика и криптография*, М.: Диалог-MIFI, 2013, 397 с.

[5]. С. Титов, А. Торгашов, "Генерация неприводимых многочленов, связанных степенной зависимостью корней", *Управление, вычислительная техника и информатика*, Томск: Труды Томского Гос. ун-та, № 2 (22), С. 310-317, 2010.

[6]. Б. Шнайер, *Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С+,* Триумф, 2002, 816 с.

[7]. R. Blahut, *Theory and Practice of Error Control Codes,* Addison-Wesley Publishing Company Reaging, 1984, 500 p.

[8]. W. Peterson, E. Weldon, *Error Correcting Codes*, MIT press, Cambridge, MA, 1972.

[9]. Ф. Мак- Вильямс, Н. Слоэн, *Теория кодов, исправляющих ошибки*, М: Связь, 1979, 744 с.

[10]. В. Жельников, *Криптография от папируса до компьютера*, М: ABF, 1996, 355 с.

[11]. М. Мазурков, В. Дмитренко, Е. Конопака, "Эффективный алгоритм нахождения первообразных неприводимых полиномов", *Праці УНДІРТ*, Одесса, № 1, С. 32-35, 2005.

[12]. E. Berlekamp, *Algebraic Coding Theory*, 1968.

[13]. А. Леухин, С. Бахтин, "Новый алгоритм синтеза всех неприводимых многочленов над заданным конечным полем". [Electronic resource]. Available at: http://bio.marstu.net/data/materials/conf/mmro13/mmro13pdf/LEUKHIN_SI_2.pdf.

[14]. А. Трахтман, В. Трахтман, *Основы теории дискретных сигналов на конечных интервалах*, М: Сов. радио, 1975, 208 с.

[15]. Wilfrid Keller. "Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$", *Math. of Comp.*, 41, pp. 661-673, 1983.

АЛГОРИТМ СИНТЕЗУ НЕЗВІДНИХ ПОЛІНОМІВ ЛІНІЙНОЇ СКЛАДНОСТІ

Незвідні поліноми знаходять широке застосування в різноманітних областях науки і техніки. Незважаючи на велику затребуваність синтез незвідних поліномів до теперішнього часу є досить складне завдання і, як зазначено В. Жельніковим, «знаходження незвідних поліномів досі покрито мороком. Криптографічні служби високорозвинених країн працювали і працюють над пошуком многочленів якомога більш високого ступеня, але свої результати вони майже не висвітлюють у відкритій пресі». Відомі алгоритми синтезу незвідних поліномів мають суттєвий недолік, який полягає в тому, що їх обчислювальна складність є, як правило, квадратичною. Отже, побудова поліномів великих ступенів може бути реалізовано лише на обчислювальних комплексах високої продуктивності. Запропонований алгоритм спирається на так звані реперні сітки (сходи), число сходинок в яких збігається зі ступенем синтезованих поліномів. На кожній сходинці здійснюються найпростіші рекурентні однотипні модулярні обчислення, по завершенні яких поліном, що тестується, однозначно класифікується або як незвідний, або як складовий. Розроблений алгоритм відноситься до підкласу алгоритмів лінійної складності. Суть рекурентних операцій на множені двійкових поліномів зводиться до обчислення залишків за модулем тестуємого на незвідність поліному, представленого в векторній формі (набором бінарних коефіцієнтів поліному), від квадрата залишку, утвореного на попередній сходинці перетворення і доповненого справа нулем. Якщо верхня (порогова) ступінь синтезованих незвідних поліномів не велика, наприклад, не перевищує двох десятків, то формування множені поліномів, що тестуються, може здійснюватися за методом повного перебору. У тому випадку, коли ступінь поліному перевищує порогове значення, то генерацію поліномів зручніше реалізовувати статистичним моделюванням. В роботі коротко позначений алгоритм синтезу незвідних поліномів над простим полем Галуа характеристики $p \geq 3$.

Ключові слова: незвідні та складові поліноми, сингулярні поліноми, реперні сітки, порівнянність за модулем.

ALGORITHM FOR THE SYNTHESIS OF IRREDUCIBLE POLYNOMIALS OF LINEAR COMPLEXITY

Irreducible polynomials are widely used in various fields of science and technology. Despite the great demand, the synthesis of irreducible polynomials is still a rather complicated task and, as V. Zhelnikov noted, "finding irreducible polynomials is still obscured. Cryptographic services of highly developed countries have worked and are working on the search for polynomials of the highest possible degree, but they hardly cover their results in the open press". Known algorithms for the synthesis of irreducible polynomials have a significant disadvantage, which is that their computational complexity is, as a rule, square. Consequently, the building of large polynomials can be implemented only at computational complexes of rather high performance. The proposed algorithm based on the so-called reference meshes (stairs) the number of steps in which coincides with the degree of the polynomials synthesized. On each rung of the ladder, the simplest recurrent single-type modular calculations carried out. The end of the polynomial tested is unambiguously classified either as non-accepted or compound. The developed algorithm belongs to the subclass of linear complexity algorithms. The

essence of recurrence operations on a set of binary polynomials reduced to calculating the residues by the module of the polynomial irreducibility test represented in vector form from the deduction square formed at the previous transformation step and added to the right by zero. If the upper (threshold) degree of the synthesized non-acceptance polynomials is not large, e.g., does not exceed two tens. The formation of the set of polynomials under test can be carried out by the method of total elimination. When the degree of polynomial exceeds the threshold value, it is more convenient to generate the polynomials under test by statistical modeling. The paper briefly describes the synthesis algorithm for irreducible polynomials over a simple Galois field of characteristics $p \geq 3$.

Keywords: irreducible and compound polynomials, singular polynomials, defining steps, modular comparability.

Белецкий Анатолий Яковлевич, доктор технических наук, профессор, заслуженный деятель науки и техники Украины, лауреат Гос. премии Украины в области науки и техники, профессор кафедры электроники, робототехники и технологий мониторингу и Интернета вещей Национального авиационного университета.
E-mail: abelnau@ukr.net.
Orcid ID: 0000-0002-3798-8150.

Білецький Анатолій Якович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, професор кафедри електроніки, робототехніки та технологій мониторингу и Інтернету речей Національного авіаційного університету.

Beletsky Anatoly, Doctor of Science, Professor, Honored Scientist of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, Department of Electronics, Robotics, Monitoring and IoT Technologies, Professor, National Aviation University.

Ковальчук Арсен Витальевич, студент кафедры электроники, робототехники и технологий мониторингу и Интернета вещей Национального авиационного университета.
E-mail: kovalchuk.arsen1@gmail.com.
Orcid ID: 0000-0001-5085-3173.

Ковальчук Арсен Віталійович, студент кафедри електроніки, робототехніки та технологій мониторингу и Інтернету речей Національного авіаційного університету.

Kovalchuk Arsen, Department of Electronics, Robotics, Monitoring and IoT Technologies, Student, National Aviation University.

Новиков Константин Андреевич, студент кафедры электроники, робототехники и технологий мониторингу и Интернета вещей Национального авиационного университета.
E-mail: kostia.novikov1703@ukr.net.
Orcid ID: 0000-0002-9418-030X.

Новиков Костянтин Андрійович, студент кафедри електроніки, робототехніки та технологій мониторингу и Інтернету речей Національного авіаційного університету.

Novikov Konstantin, Department of Electronics, Robotics, Monitoring and IoT Technologies, Student, National Aviation University.

Полторацкий Дмитрий Анатольевич, студент кафедры электроники, робототехники и технологий мониторингу и Интернета вещей Национального авиационного университета.
E-mail: dpoltoratskyi@ukr.net.
Orcid ID: 0000-0003-3802-9928.

Полторацький Дмитро Анатолійович, студент кафедри електроніки, робототехніки та технологій мониторингу и Інтернету речей Національного авіаційного університету.

Poltoratskyi Dmytro, Department of Electronics, Robotics, Monitoring and IoT Technologies, Student, National Aviation University.