ՀԱՅԿԱԿԱՆ ՍՍՌ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ՏԵՂԵԿԱԳԻՐ
ИЗВЕСТИЯ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР
Ֆիզիկա-մաթեմատ. գիտություններ XVII, № 5, 1964 Физико-математические науки

ВЫЧИСЛИТЕЛЬНАЯ МАТЕМАТИКА

Г. А. ГАРАКОВ

АЛГОРИТМ ОПРЕДЕЛЕНИЯ НЕПРИВОДИМЫХ ДВОИЧНЫХ ПОЛИНОМОВ И ИХ ПОКАЗАТЕЛЕЙ

В статье описывается алгоритм определения двоичных неприводимых полиномов и их показателей, приводится таблица этих полиномов для степеней $m \leqslant 11$, а для последующих степеней до $m = 20$ — таблица количественной характеристики указанных полиномов и их показателей.

Неприводимые двоичные полиномы являются основой образования бинарных циклических кодов для обнаружения и корректировки как независимых ошибок, так и пакетов ошибок [1, 2]. Поэтому, естественно, иметь удобный алгоритм определения неприводимых полиномов и их показателей.

§ 1. О двоичных неприводимых полиномах

Полиномы

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m, \tag{1.1}$$

коэффициенты которых могут принимать лишь значения 0 или 1 рассматриваются в соответствии с законами обычной алгебры за одним исключением, а именно: сложение здесь осуществляется по mod 2, например:

сложение

$$\begin{array}{r} 1 + x^2 + x^3 + x^4 \\ x + x^2 + x^4 \\ \hline 1 + x + x^3 \end{array}$$

умножение

$$\begin{array}{r} 1 + x^2 + x^3 + x^4 \\ 1 + x \\ \hline 1 + x^2 + x^3 + x^4 \\ x + x^3 + x^4 + x^5 \\ \hline 1 + x + x^2 + x^5. \end{array}$$

Полиномы вида (1.1) с операцией сложения по mod 2 будем называть двоичными. Двоичные полиномы обладают объединительными, распределительными и вычислительными свойствами обычных полиномов. Также, как и в обычной алгебре, каждый двоичный полином может быть разложен на простые множители (то есть на простые двоичные полиномы) единственным способом.

В этой статье рассматриваются только двоичные полиномы.

Определение 1. Двоичный полином степени m называется неприводимым, если он не имеет двоичных полиномов-делителей со степенью больше нуля и меньше m. Полиномы первой степени x, $1+x$, очевидно, являются неприводимыми. Полиномы высших степеней не могут быть неприводимыми, если содержат множитель x. Поэтому неприводимые полиномы высших степеней должны обязательно содержать свободный член 1.

Легко понять, что если полином содержит четное число членов, то он не может быть неприводимым, так как будет иметь делитель $1+x$. Следовательно, неприводимые полиномы степени m надо искать во множестве полиномов вида

$$p(x) = 1 + \alpha_1 x + \cdots + \alpha_{m-1} x^{m-1} + x^m \tag{1.2}$$

с нечетным числом членов (с нечетным весом).

В дальнейшем для полинома (1.2) мы часто будем пользоваться также обозначением $(1, \alpha_1, \cdots, \alpha_{m-1}, 1)$.

Определение 2. Для полинома $p(x)$ обратным (сопряженным) называется полином

$$\bar{p}(x) = x^m p\left(\frac{1}{x}\right). \tag{1.3}$$

Полином $\bar{p}(x)$ также степени m и характеризуется набором коэффициентов $(1, \alpha_{m-1}, \cdots, \alpha_1, 1)$.

Определение 3. Показателем полинома $p(x)$ называется наименьшее положительное целое число e, при котором $x^e - 1$ $(= x^e + 1 \bmod 2)$ делится на $p(x)$ без остатка.

Можно показать, что для любого целого положительного числа m существует, по крайней мере, один полином степени m, который имеет показатель $e = 2^m - 1$. Это значение является максимально возможным значением e.

Теорема 1. *Если полином $p(x)$ неприводимый, то и обратный полином $\bar{p}(x)$ неприводимый.*

Доказательство: Допустим противное, пусть

$$\bar{p}(x) = p_1(x)\, p_2(x).$$

В этом тождестве заменим x на $\frac{1}{x}$ и умножим обе его части на x^m:

$$x^m \bar{p}\left(\frac{1}{x}\right) = x^m p_1\left(\frac{1}{x}\right) p_2\left(\frac{1}{x}\right) = x^{m_1} p_1\left(\frac{1}{x}\right) x^{m_2} p_2\left(\frac{1}{x}\right) = \bar{p}_1(x)\, \bar{p}_2(x),$$

где m_1 и m_2 — соответственно степени полиномов $p_1(x)$, $p_2(x)$. В последнем равенстве слева имеем полином $p(x)$, а справа — произведение двух полиномов, степени которых больше нуля и меньше m, что противоречит условию неприводимости полинома $p(x)$.

Теорема 2. *Полиномы $p(x)$ и $\bar{p}(x)$ имеют один и тот же показатель.*

Пусть $p(x)$ имеет показатель e, а $\bar{p}(x)$ — $\bar{e}$.

Покажем, что $\bar{e} = e$.

Полином $x^e + 1$ делится на $p(x)$. Пусть

$$x^e + 1 = p(x)\, q(x).$$

В этом тождестве заменим x на $\frac{1}{x}$ и обе его части умножим на x^e, при этом получим:

$$x^e + 1 = x^e p\left(\frac{1}{x}\right) q\left(\frac{1}{x}\right) = x^m p\left(\frac{1}{x}\right) x^q q\left(\frac{1}{x}\right) = \bar{p}(x)\,\bar{q}(x),$$

где m и q — соответственно степени полиномов $p(x)$ и $q(x)$. Из последнего равенства вытекает, что $\bar{e} \leqslant e$. Аналогично можно показать, что $e \leqslant \bar{e}$, откуда и получим $\bar{e} = e$.

Теорема 3. *Если полином $p(x)$ принадлежит максимальному показателю $e = 2^m - 1$, то он неприводимый.*

Доказательство. Допустим противное, пусть

$$p(x) = p_1(x)\, p_2(x),$$

где полиномы $p_1(x)$ и $p_2(x)$ сперва предположим взаимно простыми. Далее, пусть эти полиномы имеют соответственно степени m_1, m_2 и показатели e_1, e_2.

Тогда, очевидно, полином

$$x^{e_1 e_2} - 1 = (x^{e_1})^{e_2} - 1 = (x^{e_2})^{e_1} - 1$$

делится как на $p_1(x)$, так и на $p_2(x)$, а следовательно, и на их произведение $p(x)$.

С другой стороны,

$$e_1 e_2 < (2^{m_1} - 1)(2^{m_2} - 1) = 2^m + 1 - 2^{m_1} - 2^{m_2} < 2^m - 1 = e,$$

что противоречит условию принадлежности $p(x)$ максимальному показателю e.

Общий случай

$$p(x) = p_1^{m_1}(x)\, p_2^{m_2}(x) \cdots p_k^{m_k}(x),$$

где $p_i(x)$, $i = 1, 2, \cdots k$ и $k \geqslant 2$ — неприводимые полиномы, легко привести к рассмотренному случаю.

Наконец, остается рассмотреть случай

$$p(x) = [p_1(x)]^{m_1},$$

где $p_1(x)$ — неприводимый полином и $m_1 \geqslant 2$. Пусть степень полинома $p_1(x)$ — γ, показатель — e_1.

Кроме того, пусть $2^{r-1} < m_1 \leqslant 2^r$. Тогда

$$[p_1(x)]^{m_1} / (x^{e_1} - 1)^{m_1} / (x^{e_1} - 1)^{2^r} = x^{e_1 \cdot 2^r} - 1.$$

Поэтому

$$e \leqslant e_2 \cdot 2^r \leqslant (2^\gamma - 1) \cdot 2^r = 2^{\gamma+r} - 2^r < 2^{\gamma+r} - 1 \leqslant 2^{m_1\gamma} - 1 = 2^m - 1 = e, \quad (1.4)$$

что следует из очевидных неравенств

$$r \leqslant m_1 - 1 \ (m_1 \leqslant 2^{m_1 - 1}), \quad \gamma + r \leqslant \gamma + m_1 - 1 < m_1\gamma, \quad m_1 \geqslant 2, \quad \gamma \geqslant 1.$$

Противоречие (1.4) показывает, что последний случай также невозможен. Этим завершается доказательство теоремы. К максимальным показателям могут принадлежать только неприводимые полиномы, а к немаксимальным показателям как неприводимые, так и приводимые полиномы. Например, неприводимый полином

$$p(x) = 1 + x + x^2 + x^4 + x^6$$

принадлежит показателю 21, этому же показателю также принадлежит полином

$$f(x) = 1 + x^2 + x^3 + x^6 = (1 + x)(1 + x + x^2)(1 + x^2 + x^3).$$

Теперь рассмотрим вопрос о количестве неприводимых полиномов степени m. Пусть $n = 2^m - 1$ имеет делители $n_1, n_2, \cdots n_k$, причем $n_1 = 1$ и $n_k = 2^m - 1$. Для каждого из этих делителей n_i имеет место сравнение

$$2^m \equiv 1 \pmod{n_i}, \quad i = 1, 2, \cdots k. \quad (1.5)$$

Однако, для некоторых из делителей n_i сравнение вида (1.5) может иметь место и при меньших, чем m степенях:

$$2^\gamma \equiv 1 \pmod{n_i}, \quad 1 \leqslant \gamma < m. \quad (1.6)$$

Для других же делителей n_i возможно только сравнение (1.5) и невозможно сравнение вида (1.6). Именно эти последние делители n_i и только они, являются теми показателями, к которым могут принадлежать неприводимые полиномы степени m. Такие делители числа $n = 2^m - 1$ обозначим через $\bar{n}_i$. Очевидно, $n_k = 2^m - 1$ является делителем этого последнего вида.

Число неприводимых полиномов степени m, имеющих показатель $\bar{n}_i$, будет $\frac{\varphi(\bar{n}_i)}{m}$, где $\varphi(\bar{n}_i)$ — функция Эйлера, показывающая число натуральных чисел, непревосходящих $\bar{n}_i$ и взаимнопростых с $\bar{n}_i$ [4].

Число неприводимых полиномов степени m, принадлежащих максимальному показателю $e = 2^m - 1$, равно $\frac{\varphi(2^m - 1)}{m}$.

Число же всех неприводимых полиномов степени m равно

$$N(m) = \sum_{\bar{n}_i / 2^m - 1} \frac{\varphi(\bar{n}_i)}{m}.$$

Например, для

$$m = 9, \quad n = 2^9 - 1 = 511 = 7 \cdot 73$$

$$n_1 = 1, \quad n_2 = 7, \quad \bar{n}_3 = 73, \quad \bar{n}_4 = 511,$$

имеем:

$$2^1 \equiv 1 \pmod 1$$
$$2^3 \equiv 1 \pmod 7$$
$$2^9 \equiv 1 \pmod{73}$$
$$2^9 \equiv 1 \pmod{511},$$

и делителями вида $\bar{n}_i$ будут 73 и 511.

Число же всех неприводимых полиномов 9-ой степени будет:

$$\frac{\varphi(73)}{9} + \frac{\varphi(511)}{9} = 56.$$

§ 2. Описание алгоритма определения неприводимых полиномов данной степени и их показателей

Этот алгоритм может быть описан блок-схемой (фиг. 1).

Блок № 1. Для получения всех полиномов $(1.2) - (1, \alpha_1, \cdots, \alpha_{m-1}, 1)$ с нечетными весами, достаточно последовательно брать все наборы вида

$$\gamma_1, \gamma_2, \cdots, \gamma_{m-2}, 0, \tag{2.1}$$

начиная с нулевого, и каждый из них поразрядно складывать по mod 2 с набором, который получается из (2.1) путем сдвига его разрядов на одну позицию вправо:

$$\frac{\begin{matrix}\gamma_1, \gamma_2, \cdots, \gamma_{m-2}, 0\\ 0, \gamma_1, \cdots, \gamma_{m-3}, \gamma_{m-2}\end{matrix}}{(0+\gamma_1), (\gamma_1+\gamma_2), \cdots, (\gamma_{m-3}+\gamma_{m-2}), (\gamma_{m-2}+0)}. \tag{2.2}$$

Полученный набор-сумма (2.2) будет иметь четный вес, так как независимо от вида набора (2.1) общее количество единиц в наборах-слагаемых четно, а в результате их модульного сложения число единиц может уменьшиться только на четное число.

Теперь, если инвертировать в наборах (2.2) последний (вообще любой фиксированный) разряд, то получим все наборы

$$(\alpha_1, \alpha_2, \cdots, \alpha_{m-1}) \tag{2.3}$$

с нечетными весами.

В самом деле, достаточно показать, что в результате применения описанных выше операций к двум различным наборам γ и β вида (2.1) полученные преобразованные наборы $\bar{\gamma}$ и $\bar{\beta}$ будут также различными. Действительно, допустим, что $\bar{\gamma}$ и $\bar{\beta}$ совпадают:

$$[(0+\gamma_1),\ (\gamma_1+\gamma_2),\cdots(\gamma_{m-3}+\gamma_{m-2}),\ \overline{(\gamma_{m-2}+0)}=$$
$$=[(0+\beta_1),\ (\beta_1+\beta_2),\cdots,(\beta_{m-3}+\beta_{m-2}),\ \overline{(\beta_{m-2}+0)}],$$

откуда имели бы

$$\gamma_i=\beta_i\quad(i=1,\ 2,\cdots,\ m-2),$$

что противоречит условию нетождественности γ и β.

Наконец, сложив полученные наборы (2.3) с постоянным набором $1\underbrace{00\cdots0}_{m-1}1$, получим точно 2^{m-2} наборов (полиномов) $(1, \alpha_1,\cdots$ $\cdots\alpha_{m-1}\ 1)$ с нечетными весами.

Блок № 2. Здесь осуществляется проверка — является ли поступивший в блок очередной полином (набор) $p(x)$ с нечетным весом неприводимым или нет. Для этого полином $p(x)$ последовательно делится на все неприводимые полиномы степени $\frac{m}{2}$, либо $\frac{m-1}{2}$ в зависимости от четности или нечетности числа m, начиная с неприводимого полинома второй степени.

Фиг. 1. Блок—схема определения неприводимых двоичных полиномов данной степени и их показателей.

Так, для $m=10$ (также $m=11$) полином $p(x)$ должен делиться на все неприводимые полиномы (наборы)

111*, 1101, 11001, 11111*,
100101, 101111, 110111,

а также на их обратные полиномы, то есть всего на 12 неприводимых полиномов, которые могут быть получены непосредственно.

Символом * отмечены самосопряженные полиномы, то есть полиномы, которые совпадают со своими обратными.

При этом делении нас не интересует частное, а важно знать имеет ли место деление с остатком или без остатка.

Алгоритм самого процесса деления прост: делитель пишется под делимым так, чтобы коэффициент его члена в наивысшей степени находился под коэффициентом аналогичного члена делимого. Написанные наборы поразрядно складываются по mod 2; полученный набор-сумма сдвигается на одну позицию влево, анализируется его левый крайний разряд; если он—единица, то делитель складывается по mod 2 со сдвинутым набором, если же он—нуль, то сдвинутый набор снова сдвигается влево на один разряд и т. д. Процесс сдвигов и модульного сложения продолжается до тех пор, пока в последнем полученном наборе-сумме число разрядов станет меньше числа разрядов де-

лителя. Последний набор-сумма будет остатком от деления. Если набор-сумма состоит только из одних нулей, то деление имеет место без остатка, в противном случае с остатком.

Если полином $p(x)$ делится на один из неприводимых полиномов степени $\frac{m}{2}$ $\left(\text{либо } \frac{m-1}{2}\right)$, то этот полином—приводимый и поэтому управление передается блоку № 1 для посылки очередного полинома (1.2) с нечетным весом.

Полином $p(x)$ будет неприводимым, если он не делится (без остатка) ни на один из неприводимых полиномов степени $\frac{m}{2}$ $\left(\text{либо } \frac{m-1}{2}\right)$.

Из числа 2^{m-2} кандидатов в неприводимые полиномы степени m через блок № 2 пройдут лишь $\sum_{\bar{n}_i/2^m-1} \frac{\varphi(\bar{n}_i)}{m}$ неприводимых полиномов.

Блок № 3. Здесь определяется показатель неприводимого полинома степени m. Работа блока определяется в зависимости от количества делителей числа $n=2^m-1$ вида $\bar{n}_i$.

Так, для $m=11$, $n=2^{11}-1=2047=23\cdot 89$ делителями будут

$$\bar{n}_1=1,\ \bar{n}_2=23,\ \bar{n}_3=89 \text{ и } \bar{n}_4=2047.$$

Число неприводимых полиномов 11-ой степени, принадлежащих последним трем делителям, соответственно будет 2, 8 и 176.

Для определения показателя неприводимого полинома $p(x)$ сначала делим $x^{23}+1$ на этот полином по вышеописанному алгоритму. Если деление имеет место без остатка, то показатель полинома $p(x)-23$, если же $x^{23}+1$ не делится на полином $p(x)$, то на него делим $x^{89}+1$ (ввиду особенной простоты полинома (набора) вида x^k+1 его деление на другие полиномы в ЭВЦМ легко осуществляется). В случае, если это последнее деление будет безостаточное, то показатель полинома $p(x)$—89, в противном случае полином $p(x)$ будет принадлежать максимальному показателю 2047.

Блок функционирует так, что если выбраны все $\frac{\varphi(\bar{n}_i)}{m}$ неприводимых полиномов степени m, принадлежащих показателю $\bar{n}_i$, то работа соответствующего подблока по выявлению именно этих неприводимых полиномов прекращается, но работа других аналогичных подблоков, по которым еще соответствующие количества неприводимых полиномов степени m не выбраны, продолжается.

Надобность в блоке отпадает в том случае, когда число $n=2^m-1$ является простым, ибо тогда все неприводимые полиномы

степени m будут принадлежать максимальному показателю $e = 2^m - 1$ [4].

Для простоты числа $n = 2^m - 1$ необходимо, чтобы число m было простым. Но это условие недостаточно, так как уже при $m = 11$, n — составное.

До сих пор неизвестно, существует ли конечное или бесконечное число простых чисел вида $n = 2^m - 1$. Известно 20 простых чисел этого вида (для $m = 2, 3, 5, 7, 13, 17, 19$ и др.), из которых наибольшее — $n = 2^{4423} - 1$, которое вместе с тем является наибольшим

Таблица №1

Неприводимых двоичных полиномов и их показателей (для степеней $m \leq 11$)

m	P(x)	e	m	P(x)	e	m	P(x)	e
1	2	–		1207	511		2257	341
	3*)	1		1225	511		2355	341
				1243	511		2437	341
2	7*)	3		1257	511		2547	341
				1267	511		2633	341
3	13	7		1275	511		2653	341
				1317	511		3277	341
4	23	15		1333	511		3367	341
	37	5		1423	511		3417	341
				1437	511			
5	45	31		1473	511		2055	93
	57	31		1517	511		2413	93
	67	31		1533	511		3247	93
				1577	511			
6	103	63		1617	511		2251*)	33
	133	63					3043*)	33
	147	63		1003	73			
	127	21		1027	73		3777*)	11
	111*)	9		1113	73			
				1145	73	11	4005	2047
7	203	127					4027	2047
	211	127	10	2011	1023		4053	2047
	217	127		2033	1023		4055	2047
	235	127		2047	1023		4107	2047
	247	127		2055	1023		4143	2047
	253	127		2145	1023		4145	2047
	277	127		2157	1023		4161	2047
	313	127		2213	1023		4173	2047
	357	127		2305	1023		4215	2047
				2327	1023		4225	2047
8	435	255		2347	1023		4237	2047
	453	255		2363	1023		4251	2047
	455	255		2377	1023		4261	2047
	515	255		2415	1023		4317	2047
	537	255		2443	1023		4347	2047
	543	255		2475	1023		4353	2047
	607	255		2583	1023		4365	2047
	717	255		2527	1023		4415	2047
				2533	1023		4423	2047
	477	85		2617	1023		4445	2047
	567	85		2627	1023		4451	2047
	573	85		2707	1023		4473	2047
	613	85		2767	1023		4475	2047
	433	51		2773	1023		4505	2047
	637	51		3023	1023		4533	2047
	471*)	17		3067	1023		4563	2047
	727*)	17		3117	1023		4565	2047
				3133	1023		4577	2047
9	1021	511		3177	1023		4603	2047
	1033	511		3337	1023		4617	2047
	1055	511		3427	1023		4653	2047
	1063	511		2017	341		4655	2047
	1131	511		2035	341		4671	2047
	1137	511		2107	341		4707	2047
	1157	511		2123	341		4745	2047
	1167	511		2143	341		4767	2047
	1175	511		2231	341		5007	2047

m	P(x)	e	m	P(x)	e	m	P(x)	e
	5023	2047		5607	2047		6417	2047
	5025	2047		5613	2047		6447	2047
	5135	2047		5623	2047		6507	2047
	5177	2047		5657	2047		6557	2047
	5235	2047		5667	2047		6637	2047
	5247	2047		5675	2047		6673	2047
	5253	2047		5733	2047		6727	2047
	5263	2047		5747	2047		6747	2047
	5285	2047		5813	2047		7043	2047
	5337	2047		5837	2047		7137	2047
	5357	2047		6127	2047		7237	2047
	5373	2047		6153	2047		7317	2047
	5403	2047		6163	2047			
	5453	2047		6277	2047		4303	89
	5477	2047		6233	2047		4463	89
	5513	2047		6263	2047		4757	89
	5537	2047		6277	2047		5779	89
	5557	2047		6307	2047			
	5575	2047		6367	2047		5343	23

Таблица № 2

Количественной характеристики неприводимых двоичных полиномов и их показателей для степеней $12 \leq m \leq 20$

Степень полинома	Число полиномов с нечетными весами	Число всех неприводимых полиномов	
		Всего	В том числе по показателям
12	1024	335	4095 (144); 1365 (48); 819 (36); 585 (24); 455 (24); 315 (12); 273 (8); 195 (8); 117 (5); 105 (4); 91 (6); 65 (4); 45 (2); 39 (2); 35 (2); 13 (1)
13	2048	630	8191 (630)
14	4096	1161	16383 (756); 5461 (378); 381 (18); 129 (6); 43 (3)
15	8192	2182	32767 (1800), 4581 (300); 1057 (60); 217 (12), 151 (10)
16	16384	4080	65535 (2048); 13845 (1024); 13107 (512); 4369 (256); 3855 (128); 1285 (64); 771 (32); 257 (16)
17	32768	7710	131071 (7710)
18	65536	14532	262143 (7776), 87381 (2592), 37449 (1296); 28127 (864), 13797 (432); 12483 (432); 9709 (432), 4599 (144), 4161 (144); 2991 (108); 1971 (72); 1533 (48); 1387 (72), 1197 (36); 657 (24); 513 (18); 399 (12); 219 (8); 189 (6), 171 (6); 133 (6); 57 (2); 27 (1), 19 (1)
19	131072	27594	524287 (27594)
20	262144	52377	1048575 (24000); 349525 (12000); 209715 (4800); 95325 (2400); 69905 (2400); 41334 (1200); 33825 (800); 31775 (1200); 25575 (600), 19065 (480); 13981 (600); 11275 (400); 8525 (300); 6766 (160); 6355 (240); 5115 (120); 3813 (120); 3075 (80); 2325 (80); 2255 (80); 1705 (60); 1353 (40); 1271 (60), 1025 (40); 825 (20), 775 (30); 615 (18); 465 (12), 451 (20); 275 (10), 205 (8), 165 (4); 155 (6); 123 (4), 75 (2); 55 (2); 41 (2); 25 (1)

известным в настоящее время простым числом, имеющим 1332 цифры [3].

По описанному выше алгоритму на электронно-вычислительной машине были определены неприводимые полиномы и их показатели. Для степеней $m \leqslant 11$ неприводимые полиномы и их показатели при-

ведены в табл. 1. В ней m—степень, а e—показатель полинома $p(x)$. Полиномы записаны в восьмерично-двоичной системе. Так, например, записи 1267, 2065 и 5623 или (001) (010) (110) (111), (010) (000) (110)(101) и (101) (110) (010) (011) соответственно означают полиномы $x^9+x^7+x^5+x^4+x^2+x+1$, $x^{10}+x^5+x^4+x^2+1$ и $x^{11}+x^9+x^8+x^7+x^4+x+1$.

Знаком * отмечены самосопряженные полиномы; из двух сопряженных (обратных) неприводимых полиномов в таблицу включен тот, который в восьмерично-двоичной системе изображается меньшим числом. Для полиномов степеней от $m=12$ до $m=20$ в табл. 2 приведены количественные характеристики числа неприводимых полиномов и их показателей. В скобках указано количество неприводимых полиномов, принадлежащих данному показателю.

Из этой таблицы видно, что число неприводимых полиномов при увеличении степени полинома на единицу почти удваивается. С ростом m увеличивается также объем вычислений, необходимых для определения неприводимых полиномов данной степени и их показателей. Однако, с практической точки зрения нас всегда интересуют небольшие значения m, для которых применение описанного алгоритма не требует значительного объема вычислений.

Поступила 16 III 1964

Գ. Հ. ԳԱՐԱԿՈՎ

ԵՐԿՈՒԱԿԱՆ ԱԻՍՏԵՄԻ ՉՎԵՐԱԾՎՈՂ ԲԱԶՄԱՆԴԱՄՆԵՐՆ ՈՒ ՆՐԱՆՑ ՑՈՒՑԻՉՆԵՐԸ ԳՏՆԵԼՈՒ ԱԼԳՈՐԻԹՄ

Ա մ փ ո փ ո ւ մ

Հոդվածում բերված են երկուական սիստեմի չվերածվող բազմանդամների հատկությունները, որոնց հիման վրա նկարագրված է այդ բազմանդամները և նրանց ցուցիչները գտնելու ալգորիթմը։

Բերված են (աղյուսակի ձևով) մինչև 11 աստիճանի նշված բազմանդամները և նրանց ցուցիչները, որոնք ստացված են էլեկտրոնային հաշվիչ մեքենայի օգնությամբ՝ բուն առաջարկված ալգորիթմի։

ЛИТЕРАТУРА

1. *Гараков Г. А.* Об использовании циклических кодов для контроля записи и считывания с магнитной ленты ЭЦВМ. Вопросы радиоэлектроники, серия VII, № 5, 1963.
2. *Гараков Г. А.* Коды Р. К. Боуза—Д. К. Рой-Чоудхури и вопросы их схемной реализации. Известия АН АрмССР, серия физ.-мат. наук, 16, № 6, 1963.
3. *Серпинский В.* Что мы знаем и чего не знаем о простых числах. Физматгиз, М.—Л., 1963.
4. *Bernard Elspas.* The theory of autonomous linear sequential networks. IRE, Transactions of circuit theory, CT—6, № 1, March (1959), 45—60.