Unit 901
– Aus der „Schülerinformatik“ vor 20 Jahren -

11 Generatorpolynom eines zyklischen Kodes

Ein Polynom vom Grade k in x über GF(2)

$$g_k(x) = \sum_{i=0}^{k} \oplus a_i x^i \quad , \quad a_0=a_k=1 \tag{1}$$

heißt Generatorpolynom eines zyklischen (n,n-k)-Kodes [1,2,3,4], wenn gilt

$$g_k(x) \mid x^n \oplus 1 \quad . \tag{2}$$

Das kleinste n, für das bei gegebenem $g_k(x)$ Gl.(2) erfüllt ist, heißt Periode (Exponent) n_0 von $g_k(x)$; alle übrigen n sind dann Vielfache dieser Periode:

$$n_0 \mid n \quad . \tag{3}$$

Ein Generatorpolynom $g_k(x)$ heißt irreduzibel, wenn es sich über GF(2) nicht in Produkte von Polynomen niederen Grade zerlegen läßt, andernfalls reduzibel.
Ein Generatorpolynom $g_k(x)$ mit der (größtmöglichen) Periode $n_0 = 2^k-1$ heißt primitiv, es ist dann zugleich auch irreduzibel.

Aufgaben

1. Geben Sie
   - einen Algorithmus zur Bestimmung der
   - bzw. einen Formelausdruck für die

   Periode n_0 eines vorliegenden Generatorpolynoms $g_k(x)$ an.

   Anleitung:
   - Das Generatorpolynom werde (umkehrbar eindeutig) dargestellt durch k und

$$a = \sum_{i=1}^{k-1} a_i \cdot 2^{i-1} \quad . \tag{4}$$

     Gesucht ist dann $n_0 = \varphi(k,a)$.
   - Die gesuchte Funktion φ besitzt folgende Eigenschaften:

$$D_a(\varphi) = \mathbb{N}(0,2^{k-1}-1) \tag{5.1}$$

$$W(\varphi) \subset \mathbb{N}(k,2^k-1) \quad , \quad \mathrm{card}(W(\varphi)) = \mathrm{fib}(k+1) \tag{5.2}$$

fib(k) - k-tes Glied der Fibonacci-Folge mit dem Bildungsgesetz

$fib(0) = 0 \quad , \quad fib(1) = 1$

$fib(k) = fib(k-1) + fib(k-2) \quad ; \quad k=2,3,..$

(vgl. Abschn. 1)

- $\varphi(k,0) = k \quad , \quad \varphi(k,2^{k-1}-1) = k+1$ (5.3)

- $\varphi(k,a) = \varphi(k,inv(a)) \quad , \quad inv(a) = \sum_{i=1}^{k-1} a_{k-i} \cdot 2^{i-1}$ (5.4)

- Außerdem ist nachstehende Wertetabelle von φ für $k = 2,3,..,6$ gegeben.

card(Ψ(φ))		2	3	5	8	13
31						7
30						30
29						31
28						15
27						12
26						21
25						63
24						31
23						31
22						63
21						12
20						28
19						63
18						21
17						10
16						63
15					6	30
14					31	15
13					31	63
12					14	31
11					31	21
10					15	8
9					8	21
8					21	14
7				5	31	15
6				7	12	31
5				6	15	28
4				15	31	9
3			4	7	14	31
2			7	6	31	14
1		3	7	15	21	63
0		2	3	4	5	6
a \ k	1	2	3	4	5	6

__ : $g_k(x)$ ist irreduzibel

2. Schreiben Sie für die Lösung von 1. ein Programm und berechnen Sie damit die Wertetabelle von $\varphi(k,a)$ für

$$k = 7,8,9$$
$$a = 0,1,..,2^{k-1}-1 \quad .$$

3. Geben Sie
   - einen Algorithmus zur Bestimmung der
   - bzw. einen Formelausdruck für die

   Perioden n_0 an, die bei irreduziblen Generatorpolynomen vom Grade k überhaupt auftreten können.

   Anleitung:
   - Aus Literaturangaben liegt hierzu folgende Wertetabelle vor:

k	Perioden n_0, die bei den irreduziblen Generatorpolynomen vom Grad k überhaupt auftreten können	Anzahl der irreduziblen Generatorpolynome vom Grade k, die die Periode n_0 besitzen
1	1	
2	3	1
3	7	2
4	15,5	2,1
5	31	6
6	63,21,9	6,2,1
7	127	18
8	255,85,51,17	16,8,4,2
9	511,73	
10	1023,341,33	
11	2047	
12	4095,1365,819,585,455,273,195,65	

   - Unter Benutzung der Abkürzung

$$\underline{x} = 2^x - 1 \qquad (6)$$

   und der verallgemeinerten Multiplikation

$$x \circ y = \frac{x \cdot y}{(ggT(x,y))^2} \qquad (7)$$

(Abelsche Gruppe)

   kann man die gegebene Wertetabelle wie folgt notieren:

k	n_0
2	1 • 2
3	1 • 3
4	1 • 4 , 1 • 2 • 4
5	1 • 5
6	1 • 6 , 1 • 2 • 6 , 1 • 3 • 6
7	1 • 7
8	1 • 8 , 1 • 2 • 8 , 1 • 2 • 4 • 8 , 1 • 4 • 8
9	1 • 9 , 1 • 3 • 9
10	1 • 10 , 1 • 2 • 10 , 1 • 5 • 10
11	1 • 11
12	1 • 12 , 1 • 2 • 12 , 1 • 2 • 4 • 12 , 1 • 3 • 12 , 1 • 3 • 6 • 12 , 1 • 4 • 12 , 1 • 2 • 6 • 12 , 1 • 6 • 12

- Interpretieren Sie diese Tabelle anhand des Relationsgraphen der Teilbarkeitsrelation x|y.