Im Debattierclub 19
Zyklische Codes, Teilbarkeitsrelation und mehr

Irreduzible Polynome $g_k(x)$ vom Grade **k** in x über GF(2)
(Generatorpolynome zyklischer (n, n-k)-Codes)
besitzen die Perioden $\mathbf{n_0}$ (kleinstes n für das gilt $g_k(x) | x^n \oplus 1)$:

k	1	2	3	4	5	6	7	8	9	10	11	12	...
$\mathbf{n_0}$	1	3	7	15	31	63	127	255	511	1023	2047	4095	
				5		21		85	73	341		1365	
						9		51		33		819	
								17				585	
												455	
												273	
												195	
												65	

Unter Benutzung der Abkürzung

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

und der kommutativen Gruppenoperation auf $\mathbb{N}$

$$x \circ y = \frac{x*y}{[ggT(x,y)]^2} \; ; e=1 \; ; x^{-1} = x \qquad (2)$$

(mehr in Unit 53)

kann man die vorstehende k-n_0 Wertetabelle wie folgt codieren:

k	$n_{0,cod.}$
2	$\underline{1} \circ \underline{2}$
3	$\underline{1} \circ \underline{3}$
4	$\underline{1} \circ \underline{4}$, $\underline{1} \circ \underline{2} \circ \underline{4}$
5	$\underline{1} \circ \underline{5}$
6	$\underline{1} \circ \underline{6}$, $\underline{1} \circ \underline{2} \circ \underline{6}$, $\underline{1} \circ \underline{3} \circ \underline{6}$
7	$\underline{1} \circ \underline{7}$
8	$\underline{1} \circ \underline{8}$, $\underline{1} \circ \underline{2} \circ \underline{8}$, $\underline{1} \circ \underline{2} \circ \underline{4} \circ \underline{8}$, $\underline{1} \circ \underline{4} \circ \underline{8}$
9	$\underline{1} \circ \underline{9}$, $\underline{1} \circ \underline{3} \circ \underline{9}$
10	$\underline{1} \circ \underline{10}$, $\underline{1} \circ \underline{2} \circ \underline{10}$, $\underline{1} \circ \underline{5} \circ \underline{10}$
11	$\underline{1} \circ \underline{11}$
12	$\underline{1} \circ \underline{12}$, $\underline{1} \circ \underline{2} \circ \underline{12}$, $\underline{1} \circ \underline{2} \circ \underline{4} \circ \underline{12}$, $\underline{1} \circ \underline{3} \circ \underline{12}$, $\underline{1} \circ \underline{3} \circ \underline{6} \circ \underline{12}$, $\underline{1} \circ \underline{4} \circ \underline{12}$, $\underline{1} \circ \underline{2} \circ \underline{6} \circ \underline{12}$, $\underline{1} \circ \underline{6} \circ \underline{12}$

Hierbei entsprechen sich z.B. bei k=8

$n_0 = 51$ und $n_{0,cod.} = \underline{1}\circ\underline{2}\circ\underline{4}\circ\underline{8}$

und die Menge der $n_{0,cod.}(k)$ Codewörter entspricht der Menge aller Wege vom Knoten $\underline{1}$ zum Knoten $\underline{k}$ im Graphen der Teilbarkeitsrelation „x ist echter Teiler von y; x,y∈ℕ“, dargestellt als Zeichenkette der Sequenz der durchlaufenen Knoten,

für $n_0 = 51$ und $n_{0,cod.} = \underline{1}\circ\underline{2}\circ\underline{4}\circ\underline{8}$ im Graphen rot markiert.

Bild Graph der Teilbarkeitsrelation
x ist echter Teiler von y

Die zugehörige Dekodierungsvorschrift

$n_{0,cod.} \rightarrow n_0$ ist durch die Gln (2) und (1) gegeben.

Problem 1

Konstruieren Sie einen Codierungsalgorithmus $n_0 \rightarrow n_{0,cod.}$ (Codierung = Zerlegung von n_0 in ein $\circ$ Produkt).

Problem 2

Sondieren Sie das „Umfeld“ der Teilbarkeitsrelation (vgl. Unit 47) bezüglich weiterer Ausbeute zu den irreduziblen Polynomen über GF(2).

Problem 3

**** Notieren Sie für andere asymmetrische Relationsgraphen (vgl. Unit 47) analog zur vorliegenden k-$n_{0,cod.}$-Tabelle die Knoten-Wege-Tabellen in $\circ$ Produkt-Darstellung.**

**** Dekodieren Sie nun die $\circ$ Produkte analog zu $n_{0,cod} \rightarrow n_0$ mittels der Gln (2) und (1).**

**** Interpretieren Sie die erhaltenen Tabellen analog zur vorliegenden k-n_0-Tabelle. Welche Semantik lässt sich jeweils für die durch die Dekodierung erhaltenen Zahlen angeben?**

Problem 4

Umgekehrt: suchen Sie für Tabellen, die analog zu der vorliegenden k-n_0-Tabelle aufgebaut sind, die zugehörigen $\circ$ Code-Relationen.