STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1955-010

Fouten ontdekkende coderingen

J. Verhoeff

1955

Foutem ontdekkende coderingen.

§ 0. Inleiding:

Bij telefoonnummers en bij girorummers e.d. kan het nuttig zijn om bepaalde nummers niet uit te reiken en verkeerde aanduidingen, die ontstaan door fouten in het reproduceren van de nummers, te voorkomen. Veel voorkomende fouten zijn: 1e. fout in één cijfer, 2e. verwisseling van twee opeenvolgende cijfers, 3e. in het 10-tallig stelsel vervangen van XY door YX door de fonetische verwantschap van dertig en dertien (thirty and thirteen e.d.).

De fouten onder 1e en 2e zullen we elementaire fouten noemen en twee getallen verwant als ze in elkaar overgaan door zo'n fout. Gemeenschappelijk wordt dus naar een verzameling getallen met een vast aantal valse gaan twee verwante getallen bevat. Men zou dit bereiken door aan elk getal $[a_1,\ldots,a_k]$ van k cijfers een $k+1^{\text{ste}}$ (sleutel) toe te voegen, dusdanig dat noch twee getallen die slechts in één cijfer verschillen dezelfde sleutel krijgen noch twee getallen die slechts daarin verschillen dat twee opeenvolgende cijfers verwisseld zijn. Er moet natuurlijk op gelet worden dat er ook gevaar bestaat dat de sleutel met het laatste cijfer verwisseld zou kunnen worden, zodat het bereist is dat als $[a_1\ldots a_{k-1}a_k]$ de sleutel a_{k+1} bezit, het getal $[a_1\ldots a_{k-1}\cdot a_{k-1}]$ ≠ niet de sleutel a_k krijgt. Een codering die hieraan voldoet zullen we foutenontdekkend noemen. Alleen voor het grondtal 2 bestaat een dergelijke codering naar zal blijken niet.

Het is duidelijk dat dit een maximale verzameling van de boven genoemde aard geeft. Verder bereikt men door de genoemde methode dat reeds bestaande nummers door verlenging tot een "beveiligd" systeem kan worden uitgebreid.

In principe zijn er verschillen methoden ter bepaling van de sleutel. Men zou bv. de sleutel rechtstreeks uit alle a_i's kunnen trachten te bepalen, $a_{k+1} = f(a_1,\ldots a_k)$, dit wordt gedaan in § 1 voor talstelsels met oneven grondtal n en in § 5 voor $n \equiv 2 \pmod 4$. Ook kan men a_{k+1} recurrent bepalen als volgt: $a_i = f_i(a_{i-1}, a_i)$ $(i=1,\ldots k)$ waarbij a_1 willekeurig vast gekozen wordt. Het getal a_k is dan de gezochte sleutel a_{k+1}. Men kan eerst proberen alle f_i's gelijk te nemen, dit wordt gedaan in § 1 voor oneven n en in § 2 voor n=4 en n=8. Voldoende voorwaarden voor de functie f worden aangegeven. In § 3 wordt bewezen dat men voor n=6 niet met één functie kan volstaan.

De aanleiding van dit rapport was de vraag of er voor n=10 zo'n functie kan worden aangegeven. Vermoedelijk bestaat deze echter niet in de gevallen dat $n \equiv 2 \pmod 4$. Wel lukt dit met twee verschillende functies g en f, waarbij $f_i = f$ als i even en $f_i = g$ als i oneven is.(§ 4). Tot slot wordt in § 6 een methode gegeven om uit fouten ontdekkende coderingen voor grondtal m en m' er een voor het grondtal m.m' af te leiden. Met deze productstelling en de methode voor $n \equiv 2 \pmod 4$ en die voor 4 en 8 is dus een constructie aangegeven voor elke n.

§ 1. Talstelsel met oneven grondtal n.

In het geval van het n-tallig stelsel met oneven n kan men voor de sleutel nemen: $a_{k+1} \equiv \sum_{i=1}^{k} (-1)^{k-i} a_i \pmod n$, $0 \leq a_{k+1} \leq n$. De sleutel verandert kennelijk als één cijfer wordt veranderd. Is nu a_{i+1} verder verwisseld neemt de sleutel toe met $\pm(2a_i - 2a_{i+1}) \neq 0$ (n oneven is. Nu is echter

(zie pag. 2)

tieel dat de a_k de factor 1 krijgt. Voor k= 2 dan $a_2=a_1$, en niet $a_1=a_2$, daar in het tweede geval a_1a_3 de sleutel a_2 krijgt en dan verwisseling van de sleutel met het laatste cijfer niet wordt bemerkt. Deze methode is echter voor even n onbruikbaar.
Definiëren we de functie a*b als $a*b \equiv b-a \pmod n$ en $0 \leq a*b < n$ dan gelidt blijkbaar $a_{k+1} = (((a_1 * a_2)\ldots) * a_{k-1}) * a_k$.

§ 2. Grondtal 4 of 8.

Het ligt voor de hand om te proberen voor even n ook zo'n functie te vinden. Deze is bruikbaar als zij voldoet aan:
I. $a*b \neq a*a$. II. $b*a \neq a*a$. en III. $(a*b)*a \neq (a*a)*b$. (en ev. IV. $b*a \neq a*b$), mits $a \not\equiv b \pmod n$.
Dit is gemakkelijk te verifiëren. IV is niet noodzakelijk, daar we aan elk getal eerst eenzelfde willekeurige a_0 kunnen laten voorafgaan, dus $a_{k+1} = ((((a_0 * a_1) * a_2) * \ldots a_{k-1}) * a_k$.
Beveiliging tegen verwisseling van de sleutel met het laatste cijfer geeft nog als eis: V. als $a*b=a$ dan $a*a \neq b$.
Voor n=4 geeft de functie gedefiniëerd door de volgende tabel een voorbeeld. (Voldoet aan I-V).

*	1	2	3	0
1	1	3	0	2
2	0	2	1	3
3	2	0	3	1
0	3	1	2	0

en voor n=8

*	1	2	3	4	5	6	7	8
1	1	8	4	5	7	2	6	3
2	8	1	3	4	2	7	3	6
3	7	2	6	3	1	8	4	5
4	2	7	3	6	8	1	5	4
5	4	3	1	8	6	3	7	2
6	5	4	8	1	3	6	2	7
7	6	1	7	2	4	5	1	8
8	3	6	2	7	5	4	8	1

Zij voldoet aan I,II,III,V.

§ 3. Grontal $n \equiv 2 \pmod 4$

Voor n= 2 is de foutenontdekkende codering onmogelijk daar 00,10 en 01 uit elkaar kunnen ontstaan door een 'elementaire' fout, terwijl voor de codering alleen 0 en 1 beschikbaar zijn.
Voor n= 6 bestaat er geen functie die aan I,II en III voldoet.
Bewijs: Laat R_y de permutatie zijn die x overvoert in x*y.
Dit is krachtens II inderdaad een permutatie van de cijfers 0,1,2,3,4,5. De eis I luidt: $R_y x \neq R_z x$ voor alle x, en III
$R_z(R_y x) \neq R_y(R_z x)$ voor alle x, of wel
$(R_y^{-1} R_z R_y)x \neq R_z x$ (alle x).
We zullen nu laten zien dat er geen 6 van zulke permutaties bestaan.
Wegens I moet in één of andere R_y de 1-cyclo (x) voorkomen.
Geen enkele R_y mag twee één-cyclen bevatten. Stel nl. $R_y = (x)(y)R_y'$.
Wegens I is er een R_u met $R_u x = y$ (uiteraard $u \neq x$) en
$R_z^{-1} R_u R_z\, x = y = R_u x$, wat in tegenspraak is met III.
Neem de permutatie die x invariant laat R_{xy}.
Als een permutatie voorkomt met de structuur (...)(..)(.) dan mogen we aannemen dat dit $R_{xy}(1\ 2)(3\ 4\ 5)(0)$ is.

Voor $R_{(3)}$ komt dan wegens I en III één slechts in aanmerking

(1 0) (2 4 3)(5)	(1 3 0 4 2)(5)	
(2 0) (1 4 3)(5) en	(1 4 3 2 0)(5)	en voor $R_{(4)}$
	(1 0 2 4 3)(5)	
(1 0)(2 3 5)(4)	(1 3 0 3 2)(4)	
(2 0)(1 3 5)(4)	(1 3 5 2 0)(4)	
	(1 0 2 3 5)(4)	

Wegens I en $R_{(3)}^{-1}R_{(4)}R_{(3)}x \neq R_{(4)}x$ zijn alle combinaties onmogelijk.

Derhalve moeten alle permutaties de structuur (.....)(.) hebben.
Stel $R_{(0)}$ = (1 2 3 4 5)(0). Wegens I hebben we voor $R_{(3)}$ dan de mogelijkheden (1 3 2 0 4)(5) (1 3 2 4 0)(5), (1 3 0 2 4)(5), (1 3 0 4 2)(5), (1 4 2 0 3)(5), (1 4 0 3 2)(5), (1 4 3 2 0)(5), (1 4 3 0 2)(5), (1 0 2 4 3)(5), (1 0 3 2 4)(5), (1 0 3 4 2)(5), (1 0 4 3 2)(5).

Wegens $R_{(0)}^{-1}R_{(5)}R_{(0)}x \neq R_{(3)}x$ vervallen de onderstreepten.

Voor $R_{(4)}$ komen in aanmerking (5 2 1 0 3)(4), (5 2 0 3 1)(4), (5 3 2 0 1)(4), (5 0 1 3 2)(4), (5 0 2 1 3)(4) en (5 0 3 2 1)(4).
(de permutatie (1 5 4 3 2) toepassen op de mogelijkheden voor $R_{(3)}$).
Mogelijk blijft (1 3 0 4 2)(5) en (5 0 2 3 1)(4) of
(1 0 3 2 4)(5), (5 0 2 3 1)(4), of (1 0 3 4 2)(5),
(5 3 2 0 1)(4), of (5)(1 0 3 4 2) en (5 0 1 3 2)(4).
In geen van deze gevallen is echter een $R_{(3)}$ die aan I en III voldoet te vinden. Het vermoeden ligt voor de hand dat, in analogie met de Grieks-Latijnse vierkanten, voor n ≡ 2 (mod 4) een dergelijke functie niet bestaat.
Heeft men een functietabel gevonden met permutaties $R_0 \ldots R_{n-1}$, dan vormt de tabel met permutaties $R_0^{-1} \ldots R_{n-1}^{-1}$ ook een dergelijke functie.

In al de gevonden gevallen vormen deze beide tabellen, als ze verschillend zijn, orthogonale Latijnse vierkanten, wat ook op een verband tussen beide problemen kan wijzen.

§ 4. n = 2m en m oneven.

Het volgende dat geprobeerd kan worden is het vinden van twee functies $*_0$ en $*_1$, zodat

$a_{k+1} = ((((a_1 *\ ) \ldots)*_0\ a_{k-2})*_1\ a_{k-1})*_0\ a_k$ een geschikte sleutel is.
Dit lukt inderdaad voor n = 2m, met m ≡ 1 mod 2. Het zij (ruim) voldoende dat geldt:

I. $a *_\varepsilon b \neq a *_\varepsilon c$. II. $b *_\varepsilon a \neq c *_\varepsilon a$.

III. $(a *_\varepsilon b) *_{1-\varepsilon} c \neq (a *_\varepsilon c) *_{1-\varepsilon} b$. IV. $b *_\varepsilon c \neq c *_\varepsilon b$.
V. als $a *_\varepsilon b = c$ dan $a *_\varepsilon c \neq b$ voor $b \neq c$ en $\varepsilon = 0$ of 1.

Remarks. Deel de cijfers $a = 1, \ldots, n$ in twee klassen A_0 en A_1 elk van n cijfers, die beide een volledig restsysteem mod n vormen. Met a_α ($\alpha = 0$ of 1) duiden we dat cijfer uit de klasse A_α aan dat mod n congruent a is. Met de Griekse letters rekenen we mod 2, dus $\alpha + \beta = 0$ als $\alpha = \beta$ en $\alpha + \beta = 1$ als $\alpha \neq \beta$.

Definitie. $a_\alpha *_\varepsilon b_\beta = (-a(-1)^{\alpha+\varepsilon\beta} + b(-1)^{(1-\varepsilon)\alpha} = (-1)^{\alpha\beta} - (-1)^{\alpha+\beta}$

I resp. II volgen hieruit dat bij vaste a_α (resp. b_β) de functie $\to a_\alpha *_\varepsilon b_\beta$ (resp. $a_\alpha *_\varepsilon b_\beta$) alle n cijfers doorloopt.

III geeft $(a_\alpha *_\varepsilon b_\beta) *_\varepsilon c_\gamma = (-(-a(-1)^{\alpha+\varepsilon\beta} + b(-1)^{(1-\varepsilon)\alpha} +$
$+ (-1)^{\alpha\beta} - (-1)^{\beta})(-1)^{\alpha\beta+\varepsilon\gamma} + c(-1)^{\varepsilon(\alpha+\beta)} + (-1)^{\alpha+\beta} - (-1)^{\gamma})_{\alpha+\beta+\gamma}$

en $(a_\alpha *_\varepsilon c_\gamma) *_{1-\varepsilon} b_\beta = (-(-a(-1)^{\alpha+\varepsilon\gamma} + c(-1)^{(1-\varepsilon)\alpha} + (-1)^{\alpha} - (-1)^{\gamma})(-1)^{\alpha+\gamma+\beta}$
$+ (-1)^{\alpha+\gamma} - (-1)^{\beta})_{\alpha+\beta+\gamma}$.

Nu er beide rechter leden tot $A_{\alpha+\beta+\gamma}$ behoren is het voldoende te laten zien dat ze mod n incongruent zijn.

1^0.

$b = \gamma$ dan dus $b \neq c$. De van b en c onafhankelijke termen zijn nu gelijk (ontstaan door verwisseling van de gelijken β en γ) dus er blijft
$-b(-)^{1-\varepsilon+\alpha+\beta+\gamma+1+\varepsilon+\gamma} + c(-)^{\varepsilon(\alpha+\beta)} \not\equiv -c(-)^{\alpha+\beta+1-\varepsilon} + b(-)^{\varepsilon+\alpha+\beta}$ of

$2b(-)^{\varepsilon+\alpha+\gamma} \not\equiv 2c(-)^{\varepsilon+\alpha+\beta}$ dit is zo daar n oneven én $b \neq c$.

2^0.

$\beta \neq \gamma$ dan $(-)^{\beta+\gamma} = -1$ en de a, b, en c vallen weg, de rest is
$-(-1)^{\beta+(1-\varepsilon)\gamma} - (-1)^{\alpha+\beta+\gamma+(1-\varepsilon)\gamma} + (-1)^{\alpha+\beta} - (-1)^{\gamma} \not\equiv -(-1)^{\beta+(1-\varepsilon)\beta} - (-1)^{\alpha+\gamma+\beta+(1-\varepsilon)\beta}$
$+ (-1)^{\alpha+\gamma} - (-1)^{\beta}$ of

$(-1)^{\varepsilon\gamma} + (-1)^{\alpha+(1-\varepsilon)\gamma} + (-1)^{\alpha+\gamma} - (-1)^{\gamma} \not\equiv (-1)^{\varepsilon\beta} + (-1)^{\alpha+(1-\varepsilon)\beta} + (-1)^{\alpha+\gamma} + (-1)^{\beta}$

als $\varepsilon = 0$ $\quad 1 + (-1)^{\alpha+\gamma} - (-1)^{\alpha+\gamma} - (-1)^{\gamma} \not\equiv 1 + (-1)^{\alpha+\beta} + (-1)^{\alpha+\gamma} + (-1)^{\beta}$

of $\quad -(-1)^{\gamma} \not\equiv -(-1)^{\gamma}$

en als $\varepsilon = 1$ $\quad (-1)^{\gamma} + (-1)^{\alpha} + (-1)^{\alpha+\gamma} - (-1)^{\gamma} \not\equiv (-1)^{\alpha} + (-1)^{\alpha}$
$+ (-1)^{\alpha+\gamma} + (-1)^{\gamma} - (-1)^{\alpha+\gamma} \not\equiv + (-1)^{\alpha+\gamma}$.

Ook IV laat zich direct verifiëren:

$b_\beta *_\varepsilon c_\gamma = (-b(-1)^{\beta+\varepsilon\gamma} + c(-1)^{(1-\varepsilon)\beta} + (-1)^{\beta} - (-1)^{\gamma})_{\beta+\gamma} \neq (-c(-)^{\gamma+\varepsilon\beta} +$
$+ b(-1)^{(1-\varepsilon)\gamma} + (-1)^{\gamma} - (-1)^{\beta})_{\beta+\gamma} = c_\gamma *_\varepsilon b_\beta$ dan

$2b \not\equiv 2c \pmod n$ als $\beta = \gamma$ en wegens $(-)^{\beta} - (-)^{\gamma} = \pm 2 \not\equiv \pm 2 =$
$= (-)^{\gamma} - (-)^{\beta}$ als

V dus vervuld als uit $a_\alpha *_\varepsilon (a_\alpha *_\varepsilon b_\beta) = b_\beta$ volgt dat $a_\alpha *_\varepsilon b_\beta = b_\beta$.
$-a(-)^{\alpha+2(\alpha+\beta)} + (-(a)(-1)^{\alpha+\varepsilon\beta} + b(-1)^{(1-\varepsilon)\alpha} + (-1)^{\alpha} - (-)^{\beta} \quad (-1)^{\alpha+(1-\varepsilon)}$
$+ (-)^{\alpha} - (-)^{\alpha+\beta} \quad)_\beta = b_\beta$

geeft

$-a(-)^{\varepsilon(\alpha+\beta)}(1 + (-)^{\alpha}) + (-)^{\varepsilon\alpha} - (-)^{\beta+\alpha+(1-\varepsilon)} + (-)^{\alpha} - (-)^{\alpha+\beta} \equiv 0 \pmod n$.

Dit kan niet als $\alpha = 1$ en dus $\alpha = 0$, dus moet

$-2a(-)^{\varepsilon\beta} \equiv 2((-)^{\beta} - 1)$ of $a \equiv (-)^{\varepsilon} - (-)^{(1-\varepsilon)\beta}$ zijn.

Maar $((-)^{\varepsilon/\beta} - (-)^{(\alpha-\varepsilon)/\beta}) *_\varepsilon b_\beta = (-((-)^{\varepsilon/\beta} - (-)^{(1-\varepsilon)/\beta})(-)^{\varepsilon/\beta} +$
$+ b + (-)^0 \Sigma (-)^\beta)_\beta = (-1 + (-)^\beta + b + 1 - (-)^\beta)_\beta = b_\beta$
Men kan voor de resttterm $(-)^\alpha - (-)^\beta$ in $a_\alpha *_\varepsilon b_\beta$ ook andere functies van α, β en ε kiezen.
Voor n = 3 krijgen we bv. als $A_0 = \{1,2,3\}$ en $A_1 = \{4,5,0\}$

$*_4$	1	2	3	4	5	0
1	3	1	2	5	0	4
2	2	3	1	4	5	0
3	1	2	3	0	4	5
4	0	5	4	1	3	2
5	4	0	5	2	1	3
0	5	4	0	3	2	1

$*_7$	1	2	3	4	5	0
1	3	1	2	5	0	4
2	2	3	1	0	4	5
3	1	2	3	4	5	0
4	0	4	5	3	1	2
5	4	5	0	2	3	1
0	5	0	4	1	2	3

Voor n = 10 kiezen we A_0 en A_1 zó dat 0 en 1 in een verschillende klasse komen. Daar de klasse index van de sleutel mod 2 gelijk is aan de som van de klasse indices van de cijfers, is het direct duidelijk dat, wanneer men a0 verandert in 1a (bv. 30 in 13), de sleutel verandert daar zelfs zijn klasse dat doet.
Kies bv. $A_0 = (0,2,4,6,8)$ en $A_1 = (1,3,5,7,9)$.

5. n = 2m en m oneven. (2e methode)

We kunnen echter ook rechtstreeks uit $a_1 \ldots a_k$ een geschikte sleutel a_{k+1} bepalen. Deel als boven de cijfers a(ε) in twee klassen in, A_0 en A_1, beide een volledig restsysteem (mod m) en a(ε) is de representant van a (mod m) uit de klasse A_ε.
Stel de cijfers van een gegeven getal $a_i (\varepsilon i)$ dan is als sleutel bruikbaar a_{k+1} (ε_{k+1}) met $a_{k+1} = (a_k - a_{k-1})(-1)^{\sigma_{k-1}} + (a_{k-2} - a_{k-3})(-1)^{\sigma_{k-3}} +$
$+ \ldots + (a_2 - a_1)(-1)^{\sigma_1} + \sum_{i=1}^{A} (-1)^{\sigma_i}$
als k even is, anders gaat men door tot $(a_1 - a_0)(-1)^{\sigma_0}$ met $a_0 = \sigma_0 =$
$= 0$ waarbij $\sigma_i = \sum_{\gamma=1}^{i} \varepsilon_\gamma$. De klasse ε_{k+1} wordt bepaald uit $\varepsilon_{k+1} \equiv \sigma_k \pmod 2$.
In formule $a_{k+1} = \sum_{i=0}^{k/2} (a_{2k-2i} - a_{2k-2i-1})(-1)^{\sigma_{k-2i-1}} + \sum_{i=1}^{A} (-1)^{\gamma_i}$ met $a_0 = 0 = \sigma_0$
Bij verandering van een cijfer verandert of de klasse of de representant. Verwisseling van a_i en a_{i+1} heeft geen invloed op de klasse, zij moet dus de bovenstaande uitdrukking (mod m) veranderen. Het verschil bedraagt $\pm 2(a_i - a_{i+1})$ als $\varepsilon_i = \varepsilon_{i+1}$ en ± 2 als $\varepsilon_i \neq \varepsilon_{i+1}$.
In het eerste geval is echter $(a_i - a_{i+1}) \not\equiv 0 \pmod m$, dus daar m oneven is is het verschil in beide gevallen $\not\equiv 0 \pmod m$.
Als $(a_1 \ldots a_k)$ de sleutel a_{k+1} heeft en $(a_1 \ldots a_{k-1} a_{k+1})$ de sleutel a'_k dan geldt $a'_k \neq a_k$. Daar a_k en a'_k in dezelfde klasse zitten moet dus gelden $a_k \not\equiv a'_k \pmod m$. Stel $a_{k+1} = s + a_k(-1)^{\sigma_{k-1}} + (-1)^{\sigma_k}$.

Was nu $a_k = a'_k = s + a_{k+1}(-1)^{\tau_{k-1}} + (-1)^{\tau_{k-1}+\tau_k} s + s(-1)^{\tau_{k-1}} a_k + (-1)^{\tau_{k-1}}$ $+ (-1)^{\tau_k+\tau_{k-1}}$dan zou $s(1 + (-1)^{\tau_{k-1}}) + 2(-1)^{\varepsilon} \equiv 0 \pmod m$ zijn, dus $\tau_{k-1} = 0$ en $s \equiv -(-1)^{\varepsilon_k} \pmod m$, maar dan is $a_{k+1} \equiv -(-1)^{\varepsilon} + a_k(-1)^{\tau_{k-1}} +$ $+ (-1)^{\varepsilon_k + \tau_{k-1}} a_k$ en daar wegens $\tau_{k-1} = 0$ a_k en a_{k+1} in dezelfde klasse liggen, waarom ze gelijk.

§ 6. Samengestelde grondtal $n = m.m'$ met $m.m' > 2$.

We delen nu de cijfers van $1 \ldots n$ in m' klassen $A_\varepsilon (\varepsilon = 1, \ldots, m')$ van m cijfers die alle mod n een volledig restsysteem vormen. Laat voor de grondtallen n en m' beide een geschikte codering gegeven zijn, welke aan $a_1 \ldots a_k$ toegevoegd (n tallig) a_{k+1} en aan $\varepsilon_1 \ldots \varepsilon_k$ (m' tallig) ε_{k+1}. Dan kunnen we als sleutel voor het getal $a_k/\varepsilon_1, \ldots, a_k/\varepsilon_k)$ nemen $a_{k+1}{}^{\varepsilon}{}_{k+1}$.
Deze is geschikt// verandert nl. een cijfer dan verandert of de klasse of de representant al naar gelang van dat cijfer de klasse of de representant verandert. Bij verwisseling zijn er ook twee mogelijkheden.
1°. De verwisselde getallen behoren tot dezelfde klasse, dan zijn zij echter mod n verschillend en a_{k+1} verandert (en ε_{k+1} niet) dus de sleutel verandert.
2°. Zij behoren tot verschillende klassen, dan verdwijnen twee ongelijke ε's verwisseld dus ε_{k+1} verandert en de sleutel a fortiori.
Dit combinerend met de resultaten van § § 1 en 2 en 4(5) vinden wij een constructie methode voor de codering voor elke waarde van $n > 2$.

1 fouten ontdekkende
// vinden en verbeteren