

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1955-010

Fouten ontdekkende coderingen

J. Verhoeff



1955

Fouten ontdekkende coderingen.

§ 0. Inleiding

Bij telefoonnummers en bij gironummers e.d. kan het nuttig zijn om bepaalde nummers niet uit te reiken en verkeerde aansluitingen, 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 III door IX 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. Gesocht wordt dus naar een verzameling getallen met een vast aantal welke geen twee verwante getallen bevat. Men zou dit bereiken door men elk getal $[a_1, \dots, a_k]$ van k cijfers een $k+1$ ste (sluutel) toe te voegen, dusdanig dat noch twee getallen die slechts in één cijfer verschillen dezelfde sluitel 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 sluitel met het laatste cijfer verwisseld zou kunnen worden, zodat het vereist is dat als $[a_1, \dots, a_{k-1}, a_k]$ de sluitel a_{k+1} heeft, het getal $[a_1, \dots, a_{k-1}, a_{k-1}, a_k]$ $\neq$ niet de sluitel a_{k+1} krijgt. Een codering die hieraan voldoet zullen we foutenontdekkend noemen. Alleen voor het grondtal 2 bestaat een dergelijke codering maar 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 sluitel. Men zou bv. de sluitel rechtstreeks uit alle a_i 's kunnen trachten te bepalen, $a_{k+1} = f(a_1, \dots, a_k)$, 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: $a_1 = f_1(a_{k-1}, a_k)$ ($i=1, \dots, k$) waarbij a_1 willekeurig vast gekozen wordt. Het getal a_k is dan de gesochte sluitel a_{k+1} . Men kan eerst proberen alle f_1 '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 $n \neq 10$ zo'n functie kon 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 $f_1 = f$ als i even en $f_1 = g$ als i oneven is. (§ 4). Tot slot wordt in § 6 een methode gegeven om uit fouten ontdekkende coderingen voor grondtal n, n' er een voor het grondtal $n.n'$ 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 sluitel nemen: $a_{k+1} = \sum_{i=1}^k (-1)^{k-i} a_i$ ($0 < a_{k+1} < n$). De sluitel verandert kennelijk als één cijfer wordt veranderd. Als men a_{i+1} verandert neemt de sluitel toe met $\pm(2a_i - 2a_{i+1}) \neq 0$ (want n is oneven is. Het is echter eenen- (zie pag. 2)

tiel dat de a_k de factor 1 krijgt. Voor $k=2$ dus $a_2=a_1$, en niet $a_1=a_2$, daar in het tweede geval a_1a_2 de sleutel a_2 krijgt en dus verwisseling van de sleutel met het laatste cijfer niet wordt bereikt. Deze methode is echter voor even n bruikbaar. Definieren we de functie $a \times b$ als $a \times b = b - a \pmod{n}$ en $0 < a \times b < n$ dan geldt blijkbaar $a_{k+1} = (((a_1 \times a_2) \dots) \times a_{k-1}) \times a_k$.

§ 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. $a \times b \neq a \times c$. II. $b \times a \neq c \times a$, en III. $(a \times b) \times c \neq (a \times c) \times b$. (en ev. IV. $b \times c \neq c \times b$), mits $c \neq b \pmod{n}$.

Dit is gemakkelijk te verifiëren. IV is niet noodzakelijk, daar we aan elk getal eerst eenzelfde willekeurige a_0 kunnen laten voorafgaan, dus $a_{k+1} = (((a_0 \times a_1) \times a_2) \dots \times a_{k-1}) \times a_k$.

Beveiliging tegen verwisseling van de sleutel met het laatste cijfer geeft nog als eis: V. als $a \times b = c$ dan $a \times c \neq b$.

Voor $n=4$ geeft de functie gedefinieerd door de volgende tabel een voorbeeld. (Voldoet aan I-V).

$\times$	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 $n=8$

$\times$	1	2	3	4	5	6	7	0
1	1	5	4	3	7	2	6	0
2	0	1	5	4	2	7	3	6
3	7	2	6	3	1	0	4	5
4	2	7	3	6	0	1	5	4
5	4	5	1	0	6	3	7	2
6	5	4	0	1	3	6	2	7
7	0	3	7	2	4	5	1	0
0	3	6	2	7	5	4	0	1

zij voldoet aan I, II, III, V.

§ 3. Grondtal $n \equiv 2 \pmod{4}$

Voor $n=2$ is de foutenontdekkende codering onmogelijk door 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 $x \times y$.

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

$R_z(R_y x) \neq R_y(R_z x)$ 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-cycle (x) voorkomen.

Een enkele R_y mag twee 6n-cycles bevatten. Stel nl. $R_y = (x)(y)R_z$.

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_x .

Als een permutatie voorkomt met de structuur $(...)(...)(...)$ dan

mogen we aannemen dat dit $R_y(1\ 2)(3\ 4\ 5)(0)$ is.

Voor R_5 komt dan volgens I en III de 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_6
(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)

Volgens I en $R_5^{-1} R_6 R_5 \neq R_6$ zijn alle combinaties onmogelijk.

Derhalve moeten alle permutaties de structuur (.....)(.) hebben. Stel $R_0 = (1 2 3 4 5)(0)$. Volgens I hebben we voor R_5 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).

Volgens $R_0^{-1} R_5 R_0 \neq R_5$ 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_5). 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 $n \equiv 2 \pmod{4}$ een dergelijke functie niet bestaat.

Heeft men een functietabel gevonden met permutaties $R_0 \dots R_{n-1}$, dan vormt de tabel met permutaties $R_0^{-1} \dots R_{n-1}^{-1}$ 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. $n = 2n$ en n oneven.

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

$a_{k+1} = (((a_1^* \dots) *_0 a_{k-2}^* *_1 a_{k-1}^*) *_0 a_k$ een geschikte sleutel is.

Dit lukt inderdaad voor $n = 2n$, met $n \equiv 1 \pmod{2}$. Het H_1 (ruim) voldoende dat geldt:

I. $a *_e b \neq a *_e c$. II. $b *_e a \neq c *_e a$.

III. $(a *_e b) *_e c \neq (a *_e c) *_e b$. IV. $b *_e c \neq c *_e b$.

V. als $a *_e b = c$ dan $a *_e c \neq b$ voor $b \neq c$ en $e = 0$ of 1 .

$$\text{Indefinite: } a_n * \frac{1}{n} b_n = (-a(-1)^{n+2/3}) + b(-1)^{n+2/3} = (-1)^{n+2/3} - (-1)^{n+2/3} = 0$$
$$\text{III geest } (a *_{\epsilon} b) *_{\epsilon} c = (-(-a(-1)^{\alpha+\epsilon\beta} + b(-1)^{(1-\epsilon)\alpha} + (-1)^{\alpha}(-1)^{\beta})(-1)^{\alpha+\beta+(1-\epsilon)\gamma} + c(-1)^{\epsilon(\alpha+\beta)} + (-1)^{\alpha+\beta} - (-1)^{\gamma})_{\alpha, \beta, \gamma}$$

$$\text{en } (a *_{\epsilon} c) *_{\epsilon} b = (-(-a(-1)^{\alpha+\epsilon\gamma} + c(-1)^{(1-\epsilon)\alpha} + (-1)^{\alpha}(-1)^{\gamma})(-1)^{\alpha+\gamma}$$
$$(-1)^{\alpha+\beta} + (-1)^{\alpha+\gamma} = (-1)^{\alpha}(-1)^{\beta+\gamma}$$

$\Rightarrow$ dan dus b/c. De van b en c onafhankelijke termen zijn nu gelijk (ontstaan door verwisseling van de gelijken β en γ dus er blijft

$$\rightarrow (-)^{u-2\alpha} (-)^{2\beta+1+1-\gamma} + (-)^{2+1+3} \neq -(-)^{2+1+2} (-)^{2\beta+1+1-\beta} \rightarrow (-)^{2+1+2} \text{ of}$$

$2b(-)^{c(\alpha, \gamma)} \neq 2c(-)^{c(\alpha, \beta)}$ dit is zo door 2 en even $\#$ is en b.e.

$$\beta \neq \text{dan } (-)^{\beta\gamma} = -1 \text{ en de a, b, en e vallen weg, de rest is}$$

$$-(-1)^{\beta+1+\epsilon}\gamma - (-1)^{\gamma+1+\epsilon}\gamma + (-1)^{\alpha+\beta} - (-1)^{\gamma} \neq -(-1)^{\gamma+1+\epsilon}\beta - (-1)^{\alpha+\gamma+\beta+1+\epsilon}\beta$$

$$+ (-1)^{\alpha+\gamma} - (-1)^{\beta} \text{ of}$$
$$(-1)^{\alpha\gamma} + (-1)^{\alpha+1+\beta\gamma} + (-1)^{\alpha\gamma} - (-1)^{\alpha\gamma} + (-1)^{\alpha/\beta} + (-1)^{\alpha+1+\beta/\beta} + (-1)^{\alpha+\gamma} + (-1)^{\beta}$$

$$\text{also } \epsilon=0 \quad 1 + (-1)^{\alpha\gamma} - (-1)^{\alpha+\gamma} - (-1)^{\gamma} \neq 1 + (-1)^{\alpha+\beta} + (-1)^{\alpha+\gamma} + (-1)^{\gamma}$$

an als $\subset \mathbb{N}$ $(-1)^x + (-1)^y = -(-1)^{x+y} = (-1)^{x+y} \neq (-1)^x + (-1)^y$

Obk IV last sich direct verhalten

$$b^*_{\gamma} \epsilon_{\gamma} = (-1)^{\beta+\epsilon_{\gamma}} + (-1)^{1-\epsilon_{\gamma}/3} + (-1)^{\beta} - (-1)^{\gamma} \neq (-1)^{\gamma+\epsilon_{\gamma}} + (-1)^{1-\epsilon_{\gamma}} + (-1)^{\gamma} - (-1)^{\beta} = \epsilon_{\gamma}^* b_{\beta} \quad \text{dann}$$

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

$\forall$ als verallgemeinert als mit $a_{\alpha} \cdot b_{\beta} = b_{\beta}$ folgt dass $a_{\alpha} \cdot b_{\beta} = b_{\beta}$

$$-a(-)^{\alpha+2(\alpha,\beta)} + (-a)(-1)^{-\alpha+\beta} + b(-1)^{-(\beta-\alpha)} + (-1)^{\alpha} - (-1)^{\beta} (-1)^{\alpha/(1-\beta)} + (-1)^{\alpha} - (-1)^{\alpha/\beta})_0 = b_0$$

附錄 2

$$-a(-1)^{e/(n-1)}(1 + (-1)^a) + (-1)^{ea} - (-1)^{B(a+1-c)} + (-1)^a - (-1)^{a^2} \equiv 0 \pmod{n}.$$

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

$$-2a(-1)^{\epsilon\beta} = 2((-1)^{\beta} - 1) \quad \text{as } a = (-1)^{\epsilon} - (-1)^{1+\epsilon/\beta} \text{ also.}$$

-3-

Maar $((-1)^{\epsilon/\beta} - (-1)^{(\epsilon/\beta)_{\beta}}) \cdot b_{\beta} = (-1)^{\epsilon/\beta} - (-1)^{(\epsilon/\beta)_{\beta}} (-1)^{\epsilon/\beta} +$
 $+ b + (-1)^0 \sum (-1)^{\beta} = (-1 + (-1)^{\beta} + b + 1 - (-1)^{\beta})_{\beta} = b_{\beta}$

Men kan voor de restterm $(-1)^{\alpha} - (-1)^{\beta}$ in $a_{\alpha} \cdot b_{\beta}$ ook andere functies van α/β en ϵ kiezen.

Voor $n = 3$ krijgen we bv. als $A_0 = \{1, 2, 3\}$ en $A_1 = \{4, 5, 0\}$

*	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

*	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	5	4	1	3	2
5	4	0	5	2	1	3
0	5	4	0	3	2	1

Voor $n = 10$ kiezen we A_0 en A_1 s6 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 naar 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. (2^e methode)

We kunnen echter ook rechtstreeks uit $a_1 \dots a_k$ geschikte sleutel a_{k+1} bepalen. Deel als boven de cijfers a_i/ϵ in twee klassen in, A_0 en A_1 , beide een volledig reststelsel (mod m) en a_i/ϵ is de representant van a (mod m) uit de klasse A .

Stel de cijfers van een gegeven getal $a_1(\epsilon_1)$ dan is als sleutel bruikbaar $a_{k+1}(\epsilon_{k+1})$ met $a_{k+1} = (a_k - a_{k-1})(-1)^{\epsilon_{k-1}} + (a_{k-2} - a_{k-3})(-1)^{\epsilon_{k-2}} + \dots + (a_2 - a_1)(-1)^{\epsilon_1} + \sum_{i=1}^k (-1)^{\sigma_i}$

als k even is, anders gaat men door tot $(a_1 - a_0)(-1)^{\sigma_0}$ met $a_0 = \sigma_0 = 0$ waarbij $\sigma_i = \sum_{j=1}^i \epsilon_j$. De klasse ϵ_{k+1} wordt bepaald uit $\epsilon_{k+1} \equiv \sigma_k \pmod{2}$.

In formule $a_{k+1} = \sum_{i=1}^k (a_{k-2i} - a_{k-2i-1})(-1)^{\sigma_{k-2i-1}} + \sum_{i=1}^k (-1)^{\sigma_i}$ 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 $\epsilon_i = \epsilon_{i+1}$ en ± 2 als $\epsilon_i \neq \epsilon_{i+1}$. 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 $a_1 \dots a_k$ de sleutel a_{k+1} heeft en $a_1 \dots a_{k-1}, a_{k+1}$ 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 $a_{k+1} = a + a_k(-1)^{\epsilon_{k-1}} + (-1)^{\sigma_k}$.

$$-6-$$
 Was nu $a_k \equiv a_k' = s + a_{k+1}(-1)^{\tau_{k-1}} + (-1)^{\tau_{k-1}} s + s(-1)^{\tau_{k-1}} a_k + (-1)^{\tau_{k-1}}$
 $+ (-1)^{\tau_{k-1}} s$ dan zou $s(1 + (-1)^{\tau_{k-1}}) + 2(-1)^{\tau_{k-1}} \equiv 0 \pmod{n}$ zijn, dus
 $\tau_{k-1} = 0$ en $s \equiv -(-1)^{\tau_k} \pmod{n}$, maar dan is $a_{k+1} \equiv -(-1)^{\tau_k} + a_k(-1)^{\tau_{k-1}}$
 $+ (-1)^{\tau_k} a_k$ en daar wegens $\tau_{k-1} = 0$ a_k en a_{k+1} in dezelfde klasse
 liggen, waren ze gelijk.

§ 6. Samengesteld grondtal $n = m \cdot m'$ met $m, m' > 2$.

We delen nu de cijfers van $1 \dots n$ in m' klassen $A_\varepsilon (\varepsilon = 1, \dots, m')$ van m
 cijfers die alle mod n een volledig reststelsel vormen. Laat voor
 de grondtallen m en m' beide een geschikte/ordering gegeven zijn,
 welke aan $a_1 \dots a_k$ toegevoegd (m tallig) a_{k+1} en aan $\varepsilon_1 \dots \varepsilon_k$ (m' tal-
 lig) ε_{k+1} . Dan kunnen we als sleutel voor het getal $a_1/\varepsilon_1, \dots, a_k/\varepsilon_k$
 nemen $a_{k+1}/\varepsilon_{k+1}$.

Deze is geschikt, verandert nl. een cijfer dan verandert of de klas-
 se of de representant al naar gelang van dat cijfer de klasse of de
 representant verandert. Bij verwisseling zijn er ook twee mogelijk-
 heden.

1°. De verwisselde getallen behoren tot dezelfde klasse, dan zijn
 zij echter mod m verschillend en a_{k+1} verandert (en ε_{k+1} niet) dus
 de sleutel verandert.

2°. Zij behoren tot verschillende klassen, dan worden er twee on-
 gelijke ε 's verwisseld dus ε_{k+1} verandert en de sleutel a ferticert.
 Dit combinerend met de resultaten van § § 1 en 2 en 4(5) vinden wij
 een constructie methode voor de ordeling voor elke waarde van $n > 2$.

1. punten inloekende

11. punten en trekkingen