STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1958 - 014

Voordracht in de serie "Actualiteiten"

J. Verhoeff

27 september 1958

Niet-binaire fouten-ontdekkende codes

1958

ZW 1958-014

Voordracht in de serie

"Actualiteiten"

door

J. Verhoeff

27 september 1958

Niet-binaire fouten-ontdekkende codes

Fouten-ontdekkende codes vinden evenals fouten-corrigerende codes hun oorsprong bij de informatietheorie bij het overbrengen van informatie door een kanaal met ruis. De informatie wordt overgebracht in groepjes van k nullen en enen, waarbij elk groepje zijn betekenis heeft. Door de ruis bestaat er de mogelijkheid dat een nul als een één wordt ontvangen en omgekeerd. Het bericht komt dan soms verminkt over. Door nu bijvoorbeeld alleen groepjes met een even aantal enen betekenis te geven wordt een groepje zinloos wanneer er één bit fout wordt ontvangen. Hierdoor wordt de fout ontdekt. Men spreekt hier van een fouten-ontdekkende code. Een code is een verzameling van groepjes die men uitgezocht heeft uit alle mogelijke groepjes.

De Heer Scholten (10) is in een vorige actualiteiten-voordracht ingegaan op codes met de eigenschap dat elk tweetal groepjes op minstens drie plaatsen verschillend zijn. Wordt dan per groepje één bit verkeerd ontvangen, dan kan men altijd de fout herstellen. Zo'n code noemt men fouten-corrigerend.

In die gevallen, waarin fouten in de groepjes elkaar niet beïnvloeden, is een fouten-ontdekkende code voldoende, daar men dan meestal achteraf de (ontdekte) foute groepjes kan herstellen zonder dat de rest daarop moet wachten (telefooncentrales). In rekenautomaten zal men in het algemeen een fouten-corrigerende code moeten prefereren.

Over binaire codes zijn diverse artikelen geschreven (zie bijv. (1), (2), (3), (6)).

Gebruikt men bij het overbrengen van informatie een hoger talstelsel dan het tweetallige, dan kan men verschillende kanten uit.
Men kan, denkend aan tel-en drukwielen,als fout definiëren de verandering van een cijfer in een ander cijfer dat een eenheid hoger of lager ligt (zie(8)en(9)). Verschillende resultaten over binaire codes kunnen dan gegeneraliseerd worden tot hogere talstelsels. Ook kan men onbeperkte fouten per cijfer toelaten (schrijffouten). Men krijgt nu direct een fouten-ontdekkende code door bijvoorbeeld alleen die groepjes van cijfers (in het n-tallig stelsel) toe te laten, waarvan de som van de cijfers door n deelbaar is. Een geheel ander soort doch eveneens veel voorkomende schrijf- en collationneer-fout is het verwisselen van twee naast elkaar staande cijfers. Het is vooral bij codenummers van artikelen e.d. dikwijls gewenst daartegen beveiligd te zijn. Dit is het eigenlijke onderwerp van deze lezing.
In het geval dat het grondtal van het talstelsel oneven is gaat dat zonder extra moeite door alleen die getallen toe te laten waarvan de alternerende som der cijfers door n deelbaar is. Immers we hebben $x-y \not\equiv y-x \mod n$, als $x \not\equiv y \mod n$. Voor even n gaat dit kennelijk niet op. Helaas heeft een veel gebruikt talstelsel een dergelijk grondtal. Verschillende voor de hand liggende generalisaties van bovengenoemde methode , mislukken voor $n \equiv 2 \mod 4$ (zie(5)). Een ervan wordt toegepast in (7) voor het 10-tallige stelsel. Daar laat men alleen die getallen $[a_1 \ldots a_x]$ toe, waarvoor $a_1+f(a_2)+a_3+f(a_4)+\ldots \equiv 0 \mod 10$, waarbij f(x) de permutatie $\begin{pmatrix} 0&1&2&3&4&5&6&7&8&9 \\ 0&2&4&6&8&1&3&5&7&9 \end{pmatrix}$ is.
Voor het voldoen van deze code is nodig (en voldoende) dat $x+f(y) \not\equiv y+f(x) \mod 10$ als $x \neq y$. M.a.w. $x-f(x) \not\equiv y-f(y)$ als $x \neq y$, dus $x-f(x)=g(x)$ moet ook een permutatie van (0- -9) zijn. Dit is hier niet het geval daar $0-f(0) = 9-f(9)=0$. Men kan echter gemakkelijk zien dat een dergelijke f(x) niet kan bestaan.
Stel n.l. van wel.
Beschouw nu de even cijfers 0,2,4,6,8 en laten er onder de cijfers f(0), f(2), f(4), f(6) en f(8) er k even zijn $0 \leq k \leq 5$, dan zijn er dus van f(1), f(3), f(5), f(7) en f(9) precies (5-k) even en dus k oneven. Maar dan zijn er van g(x) in het

totaal 2k even wat niet kan als g(x) een permutatie is. Deze redenering blijft voor elke $n \equiv 2 \bmod 4$ steekhoudend. Er blijft dus de hoop dat er voor $n \equiv 0 \bmod 4$ wel een geschikte f(x) te vinden zal zijn. Dit blijkt (door eenvoudig alle 2^4 candidaten te examineren) niet het geval.
Aangezien bij deze beschouwingen de cijfers de rol spelen van onderscheidbare symbolen, behoeven we ons niet te beperken tot optelling mod n, maar kunnen nu evengoed optellen volgens een willekeurige abelse groep. Voor $n \equiv 2 \bmod 4$ kan men weer laten zien dat er geen f(x) kan bestaan die voldoet aan de eisen, hoe men de groep ook kiest. Voor n=4 echter gaat een en ander mits men optelt in de groep van Klein (zie (12)).
Dit geeft voor $n \equiv 2 \bmod 4$ een somber beeld dat culmineert in (11) waar wordt beweerd, dat voor n=10 dergelijke codes niet kunnen bestaan, één en ander in tegenspraak met (5) waar verschillende codes expliciet worden aangegeven.
In (7) wordt het betreurd dat fouten van de vorm cba in plaats van abc niet worden ontdekt (10-tallig). In het 5-tallig stelsel is dit weer eenvoudig wanneer we alleen die getallen $[a_1 \ldots a_x]$ vormen met $a_1+2a_2+3a_3+4a_4+a_5+2a_6 \ldots \equiv 0 \pmod 5$.
Men bemerkt dan zelfs fouten zoals abcd en dbca, dus willekeurige verwisselingen binnen groepjes van 4 cijfers. Evenzo in het p-tallige stelsel, met p priem, binnen groepjes van (p-1) cijfers.
In (12) worden voor het 4-en 8-tallige stelsel codes aangegeven, beveiligd tegen verwisselingen binnen groepjes van resp. 3 en 7 cijfers. Gezien deze resultaten zou men dus kunnen hopen codes te vinden die in het 10-tallige stelsel beveiliging geven tegen willekeurige verwisselingen binnen groepjes van negen cijfers.

Literatuur:

(1) Hamming, R.W., Error Detecting and Error Correcting Codes, Bell S.T.J.26, 1950, p.147-160.

(2) Gilbert, E.N., A Comparison of Signalling Alphabets, Bell S.T.J.31, 1952, p.504-522.

(3) Laemmel, A.E., Efficiency of noise-reducing codes, Communication theory edited by Jackson 1953, p.111-118.

(4) Yngve, V.H., Language as an error-correcting code, Quarterly Progress Report, Research Lab.of Electronics, M.I.T., 1954, April 15, p.73-74.

(5) Verhoeff, J.,Fouten-ontdekkende coderingen, Rapport Mathem. Centrum, ZW 1955-010 (Intern).

(6) Slepian, D., A class of Binary Signalling Alphabets, Bell S.T.J.35, 1956, p.-203-234.

(7) I.B.M., Self checking number device for 24-26 card punches, Manual of Operation, 2nd ed., 1956.

(8) Ulrich, W., Non-binary error correcting codes, Bell S.T.J.36, 1957, p.1341-1388.

(9) Lee, C.Y., Some properties of Nonbinary Error-correcting codes, I.R.E. Trans.on Inf.Th., I.T.June 4,no 2,1958 p.77-82.

(10) Scholten, C.S., Zelf controlerende codes, Rapport Mathem. Centrum, ZW 1958-011.

(11) Sisson, R.L., An improved decimal redundancy check, Comm.of the Ass.of Comp.Machinery, Vol.1 no 5, May 1958, p.10-12.

(12) .....