

Een paar gelijkmatig verdeelde codes

Andries Brouwer

2011-05-21

In 1976 promoveerde Henk van Tilborg (geboren te Tilburg) op een proefschrift getiteld „Uniformly packed codes”.

Stellingen

Eerst de bijgevoegde stellingen lezen.

Er zijn sterke redenen om aan te nemen dat alle k keer ingekorte binaire Hamming codes met lengte $2^m - 1 - k$, $1 \leq k < 2^{m-2}$, optimaal zijn. Voor $k = 1, 2$ en 3 is dit vermoeden bewezen.

Ja, dat laatste is nog van Marc Best en mij. Een mooi vermoeden. Ik zou nieuwsgierig zijn naar die sterke redenen. Misschien zijn er sinds 1976 geen vorderingen gemaakt. Dit vermoeden ligt ver buiten het bereik van de huidige methoden.

Het bestaan van een lineaire, gelijkmatig verdeelde code met parameters $n = 70$, $q = 2$, $e = 2$, $\lambda = 16$ en $\mu = 20$ zou het bestaan van een symmetrisch block design met parameters $(70, 24; 70, 24; 8)$ tot gevolg hebben.

Een nuttige stelling. We leren hoe *uniformly packed* vertaald dient te worden. (Helaas blijven we in het ongewisse aangaande *block design*.) De wiskundige inhoud heeft een jaar of tien geleefd. Robert Calderbank liet zien dat er geen binaire, lineaire, gelijkmatig verdeelde $[70, 58, 5]$ code is. (Deze parameters horen bij $\lambda = 16$ en $\mu = 10$ —die 20 was een drukfout, denk ik.) Aan de andere kant hebben Zvonimir Janko en Tran van Trung, en later ook anderen, zulke symmetrische block designs geconstrueerd.

Sectievorming bevordert sectarisch denken en dient derhalve niet gestimuleerd te worden.

Tot zover de bijgevoegde stellingen.

Perfekte codes

Het proefschrift zelf gaat over gelijkmatig verdeelde codes. Een code is gewoon een deelverzameling van de ruimte waar we naar kijken. Zeg, een niet-lege deelverzameling van een metrische ruimte. Nu is de minimum afstand van de code de kortste afstand tussen twee verschillende elementen van de code (codeworden), en de overdekkingsstraal de grootste afstand van een punt in de ruimte tot

de code. De code heet *perfect* als er een r is met de eigenschap dat de bollen met straal r rond de codewoorden een partitie van de ruimte vormen. Het is handig om aan te nemen dat alle afstanden geheel zijn, en een natuurlijke context is dan die van deelverzamelingen van grafen (met de grafenafstand: de afstand tussen twee punten van de graaf is het aantal kanten in een kortste pad van het ene punt naar het andere). De code heet *e-foutenverbeterend* als e het grootste getal is, zo dat bollen met straal e om de codewoorden onderling disjunct zijn.

Drie perfecte 1-foutenverbeterende codes:



Het tweede voorbeeld kan generaliseerd worden: Neem een willekeurige graaf (hier een vierkant), en neem alle punten als codewoorden. Nu hebben we een 0-foutenverbeterende perfecte code. Vervang elke kant door een pad met $2e + 1$ kanten (en $2e$ nieuwe punten). Nu hebben we een e -foutenverbeterende perfecte code. Het eerste voorbeeld laat zien dat je aan elk codewoord nog een willekeurige graaf kunt hangen waarvan alle punten binnen een e -bol blijven.

De omgekeerde vraag is veel moeilijker: Heeft een gegeven graaf een 1-foutenverbeterende perfecte code? Paul Cull en Ingrid Nelson laten zien dat dit beslissen NP-volledig is. Ze geven ook het volgende voorbeeld: In het 1-persoonsspel „Torens van Hanoi” heb je m schijven van oplopende groottes die op drie stapels liggen, nooit een grotere op een kleinere. Een zet bestaat uit het verplaatsen van een schijf naar een andere stapel. Kennelijk is het aantal mogelijke standen 3^m : van elke schijf moet je zeggen op welke stapel hij ligt. De spelgraaf verbindt twee standen als je met een zet van de ene naar de andere kunt komen. De code bestaande uit de standen met een even aantal schijven op de eerste en de tweede stapel is perfect 1-foutenverbeterend.

Perfecte codes in reguliere grafen

Die spelgraaf was niet regulier (wel bijna, trouwens). Als een k -reguliere graaf Γ met buurmatrix A een 1-foutenverbeterende perfecte code C heeft, dan heeft A een eigenwaarde -1 . (Bewijs: de vector u met $u_x = 1$ als $x \notin C$, en $u_x = -k$ als $x \in C$, is eigenvector.)

Perfecte codes in afstandsreguliere grafen

Norman Biggs hield de wereld voor dat de natuurlijke setting voor de studie van perfecte codes in grafen die van de afstandsreguliere grafen is. Hij geeft een „Stelling van Lloyd”: Laat Γ een afstandsreguliere graaf zijn. Als A en M de 0-1 matrices zijn met $A_{xy} = 1$ precies als x en y verbonden zijn, en $M_{xy} = 1$ precies als x en y afstand hooguit e hebben, dan is $M = f(A)$, waarbij f een polynoom van graad e is. Als Γ een e -foutenverbeterende code bevat, dan geldt voor e verschillende eigenwaarden λ van A dat $f(\lambda) = 0$. (Voor $e = 1$ geeft dit weer de voorwaarde uit de vorige paragraaf.)

Laura Chihara gebruikte deze voorwaarde om te laten zien dat er geen niet-triviale perfecte codes met $e \geq 1$ zijn in de afstandsreguliere grafen voor Grassmann ruimten, duaal polaire ruimten (anders dan van type B_N of C_N), bilineaire vormen, alternerende vormen, of Hermitese vormen. En geen niet-triviale perfecte codes met $e \geq 2$ in de duaal polaire ruimten van type B_N of C_N . Omdat alleen de parameters een rol spelen geldt dit bewijs ook voor de gedraaide Grassmann grafen van Edwin van Dam en Jack Koolen.

James Shearer merkte op dat voor $e = 1$ en type B_N of C_N , een perfecte code alleen kan bestaan als $N = 2^m - 1$ voor zekere m . In type C_3 vonden Dennis Stanton en Jef Thas voorbeelden.

Wat de exceptionele grafen betreft, alleen $e = 1$ komt in aanmerking, en dan overleven alleen $G_{2,1}(q)$ en ${}^2F_{4,2}(2)$ de eis dat -1 een eigenwaarde is. Jef Thas merkt op dat de eerste ovoiden heeft (dat is hier hetzelfde als perfecte codes). Misschien was de vraag nog open of die veralgemeende achthoek van orde $(4, 2)$ een perfecte code heeft. Maar hij heeft er geen: zijn duale heeft universele inbeddingsdimensie 80, en een perfecte code zou een „klein” hypervlak in die 80-ruimte geven, en een klein zoekprogrammaatje laat zien dat de code niet bestaat.

Blijft tenslotte het „dunne” geval, Hamming en Johnson grafen en familie.

Perfekte codes in Johnson grafen

De (Selmer) Johnson graaf $J(n, k)$ is de graaf op de k -tallen uit n symbolen, waarbij twee k -tallen verbonden zijn als ze $k - 1$ symbolen gemeen hebben. Triviale perfecte codes bestaan uit één k -tal, of uit alle k -tallen, of uit twee complementaire k -tallen (als $n = 2k$, $k = 2e + 1$). Zijn er ook niet-triviale perfecte codes in $J(n, k)$? Philippe Delsarte schrijft: *It is tempting to risk the conjecture that such codes do not exist.* Omdat $J(n, k)$ en $J(n, n - k)$ isomorf zijn mag aangenomen worden dat $n \geq 2k$. Nu is het beste resultaat van Cees Roos: als er een perfecte e -foutenverbeterende code in $J(n, k)$ is, dan $2k \leq n \leq (k - 1)(2e + 1)/e$, kortom, ligt n heel dicht bij $2k$. Eiichi Bannai en Peter Hammond laten zien dat $n \neq 2k + 1, 2k + 2$. Tuvi Etzion en Moshe Schwartz leiden nog vele extra voorwaarden af. Het probleem is open, maar op een heel klein kiertje.

Terwijl er hier geen voorbeelden lijken te zijn, zijn die er wel bij aanverwante grafen. De graaf $O(m)$ heeft als punten de $(m - 1)$ -tallen uit $2m - 1$ symbolen, verbonden als ze disjunct zijn. (Dus $O(m)$ is regulier van valentie m .) In het bijzonder heeft $O(4)$ als punten de 35 drietallen uit 7, met afstand 0, 1, 2, 3 als het aantal gemeenschappelijke symbolen respectievelijk 3, 0, 2, 1 is. We zien dat het Fano vlak een perfecte 1-foutenverbeterende code is. Gooien we deze 7 drietallen weg, dan resteert de Coxeter graaf. Maar er zijn twee disjuncte Fano vlakken op 7 punten, dus ook de Coxeter graaf heeft een perfecte 1-code.

In feite bestaat een perfecte code met $e = 1$ in $O(k + 1)$ dan en slechts dan als er een Steiner systeem $S(k - 1, k, 2k + 1)$ is. Het Witt design $S(4, 5, 11)$ levert dus een perfecte code in $O(6)$.

Perfecte codes in Hamming grafen

De (Richard) Hamming graaf $H(n, q)$ is de graaf op de rijtjes ter lengte n met letters uit een alfabet ter grootte q , waarbij twee rijtjes verbonden zijn als ze maar op één plaats verschillen. Marcel Golay beschreef in een artikel van een halve pagina de twee codes die zijn naam dragen, met $(n, q, e) = (23, 2, 3)$ en $(11, 3, 2)$ (deze laatste was al eerder gepubliceerd door de voetballoto spelende Juhani Virtakallio), en de codes die nu Hamming codes heten, met $n = (q^m - 1)/(q - 1)$ en q priem, later gegeneraliseerd tot alle priem machten q , en de repetitiecodes, met $n = 2e + 1$, $|C| = q$. Heel interessant, in de tijd dat men begonnen was de sporadische enkelvoudige groepen te ontdekken. De Golay codes hebben Mathieu groepen als automorfismengroep. Kun je zo ook andere sporadische groepen krijgen? Helaas blijkt dat niet het geval. Jack van Lint en Aimo Tietäväinen bewijzen voor priem machten q , en Hennie Reuvers en Marc Best en Yiming Hong voor algemene q dat er behalve de binaire Golay code geen e -foutenverbeterende codes in $H(n, q)$ zijn met $e \geq 3$.

Voor $e = 2$ is nog niet alles bekend (maar de ternaire Golay code is het enige niet-triviale voorbeeld waarbij q een priem macht is).

Voor $e = 1$ zijn er zeer veel verschillende perfecte codes met dezelfde parameters als de Hamming codes, zowel lineair als niet-lineair. Er zijn geen voorbeelden bekend waarbij het aantal codewoorden geen priem macht is. Olof Heden schrijft: *Finally, the author's very personal opinion is that no one ever will be able to find a perfect code over a non prime power alphabet. Simply, the amount of information needed to describe it, even in the smallest cases, will be too large.*

Perfecte codes in productgrafen

De Hamming graaf $H(n, q)$ is het product van n kopieën van de volledige graaf K_q . Veel andere productgrafen zijn onderzocht op het voorkomen van perfecte codes. Karel Post gaf voorwaarden op het product van een aantal circuits („Lee codes”).

Gelijkmatig verdeelde codes

Als samenvatting van de studie van perfecte codes in grafen: als de graaf mooi is, en vooraf gegeven, dan zijn er maar heel weinig gevallen waarin de graaf een perfecte code heeft. Misschien is die eis te sterk.

Vandaag lijkt het meest natuurlijke begrip dat van de volledig reguliere code te zijn. De *uitwendige distributie* van een code C is de matrix B waarbij B_{xi} het aantal codewoorden op afstand i van het punt x is. De code C heet *volledig regulier* als B_{xi} niet afhangt van x , maar alleen van $d(x, C)$, de afstand van het punt x tot de code.

Een aantal begrippen ligt qua sterkte in tussen volledig regulier en perfect. Een daarvan is *gelijkmatig verdeeld*, het onderwerp van Henk's proefschrift. Een e -foutenverbeterende code C heet gelijkmatig verdeeld als er constanten λ, μ zijn zo dat $B_{x,e+1} = \lambda$ als $d(x, C) = e$, en $B_{x,e+1} = \mu$ als $d(x, C) > e$.

Een voorbeeld. Kijk in de Johnson graaf $J(13, 4)$ naar de code C die bestaat uit de 13 lijnen van een projectief vlak $PG(2, 3)$. De gecondenseerde matrix B

wordt nu

$d(x, C)$	0	1	2	3	4
0	1	0	0	12	0
1	0	1	3	7	2
2	0	0	6	4	3

zodat deze code volledig regulier is, en in feite gelijkmatig verdeeld met $e = 1$, $\lambda = 3$, $\mu = 6$.

Algemener: elk Steiner systeem $S(2, 4, n)$ geeft zo'n code in $J(n, 4)$. (En Steiner tripelsystemen geven een gelijkmatig verdeelde code met $e = 0$ in $J(n, 3)$.) Kijk in de Johnson graaf $J(17, 5)$ naar de code $S(3, 5, 17)$ (een Möbiusmeetkunde). De gecondenseerde matrix B is

$d(x, C)$	0	1	2	3	4	5
0	1	0	0	40	15	12
1	0	1	6	26	26	9
2	0	0	10	20	30	8

zodat deze code volledig regulier is, en in feite gelijkmatig verdeeld met $e = 1$, $\lambda = 6$, $\mu = 10$. Op dezelfde manier is $S(5, 7, 28)$ gelijkmatig verdeeld in $J(28, 7)$. Er zijn hier ook oneindige families, bijvoorbeeld via $S(3, 5, 4^t + 1)$.

Olof Heden laat zien dat een perfecte code in een antipodale afstandsreguliere graaf een vereniging van antipodale klassen is, en dus een perfecte code in het quotient oplevert. Voor $H(n, 2)$ volgt dat $\mathbf{1} \in C$ als $\mathbf{0} \in C$.

Eiichi Bannai laat zien dat perfecte e -foutenverbeterende codes in de gehalveerde van een bipartiete afstandsreguliere graaf Γ equivalent zijn met gelijkmatig verdeelde $2e$ -foutenverbeterende codes in Γ . Er volgt dat de gehalveerde Hamming graaf geen perfecte e -foutenverbeterende codes met $e \geq 1$ heeft.

Henk keek naar gelijkmatig verdeelde codes in $H(n, q)$, liet zien dat $e \geq 4$ niet voorkomt, en gaf voorbeelden voor $e = 1, 2$.

Referenties

- [1] Eiichi Bannai, *Codes in bipartite distance-regular graphs*, J. London Math. Soc. **16** (1977) 197–202.
- [2] M. R. Best, *A contribution to the nonexistence of perfect codes*, proefschrift, Universiteit van Amsterdam, 1982.
- [3] M. R. Best & A. E. Brouwer, *The triply shortened Hamming code is optimal*, Discrete Math. **17** (1977) 235–245.
- [4] Norman Biggs, *Perfect codes in graphs*, J. Combin. Th. (B) **15** (1973) 289–296.
- [5] A. E. Brouwer, A. M. Cohen & A. Neumaier, *Distance-regular graphs*, Springer Verlag, 1989.
- [6] A. R. Calderbank, *Nonexistence of a uniformly packed $[70, 58, 5]$ code*, IEEE Trans. Inform. Theory **32** (1986) 828–833.
- [7] P. J. Cameron, J. A. Thas & S. E. Payne, *Polarities of generalized hexagons and perfect codes*, Geom. Dedicata **5** (1976) 525–528.
- [8] Laura Chihara, *On the zeros of the Askey-Wilson polynomials, with applications to coding theory*, SIAM J. Math. Anal. **18** (1987) 191–207.
- [9] H. S. M. Coxeter, *My graph*, Proc. London Math. Soc. **46** (1983) 117–136.

- [10] Dean Crnković, *Symmetric (70, 24, 8) designs having $\text{Frob}_{21} \times Z_2$ as an automorphism group*, Glasnik Matematički Vol. 34(54) (1999) 109–121.
- [11] P. Cull & I. Nelson, *Perfect Codes, NP-Completeness, and Towers of Hanoi Graphs*, Bull. Inst. Combin. Appl. **26** (1999) 13–38.
- [12] E. R. van Dam & J. H. Koolen, *A new family of distance-regular graphs with unbounded diameter*, Inventiones Math. **162** (2005) 189–193.
- [13] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10** (1973). (Citaat op blz. 55.)
- [14] T. Etzion & M. Schwartz, *Perfect constant-weight codes*, IEEE Trans. Inf. Th. **50** (2004) 2156–2165.
- [15] J.-M. Goethals & H. C. A. van Tilborg, *Uniformly packed codes*, Philips Research Reports **30** (1975) 9–36.
- [16] Marcel J. E. Golay, *Notes on Digital Coding*, Proc. IRE **37** (1949) 657.
- [17] Anka Golemac, *Construction of new symmetric designs with parameters (70, 24, 8)*, Discr. Math. **120** (1993) 51–58.
- [18] Peter Hammond, *On the non-existence of perfect and nearly perfect codes*, Discr. Math. **39** (1982) 105–109.
- [19] P. Hammond & D. H. Smith, *Perfect codes in the graphs O_k* , J. Combin. Th. (B) **19** (1975) 239–255.
- [20] Olof Heden, *Perfect codes in antipodal distance-transitive graphs*, Math. Scand. **35** (1974) 29–37.
- [21] Olof Heden, *On perfect codes over non prime power alphabets*, pp. 173–184 in: AMS Contemp. Math. 523, 2010. (Citaat op blz. 183.)
- [22] Yiming Hong, *On the nonexistence of unknown perfect 6- and 8-codes in Hamming schemes $H(n, q)$ with q arbitrary*, Osaka Math. J. **21** (1984) 687–700.
- [23] Z. Janko & Tran van Trung, *The existence of a symmetric block design for (70, 24, 8)*, Mitt. Math. Sem. Gießen **165** (1984) 17–18.
- [24] Jacobus H. van Lint, *Coding Theory*, Springer Lecture Notes in Math. 201, 1971.
- [25] K. A. Post, *Nonexistence theorems on perfect Lee codes over large alphabets*, Inf. Control **29** (1975) 369–380.
- [26] H. F. H. Reuvers, *Some non-existence theorems for perfect codes over arbitrary alphabets*, proefschrift, Technische Hogeschool Eindhoven, 18 januari 1977.
- [27] C. Roos, *A note on the existence of perfect constant weight codes*, Discr. Math. **47** (1983) 121–123.
- [28] D. H. Smith, *Perfect codes in the graphs O_k and $L(O_k)$* , Glasgow Math. J. **21** (1980) 169–172.
- [29] D. Stanton, *Some q -Krawtchouk polynomials on Chevalley groups*, Amer. J. Math. **102** (1980) 625–662.
- [30] J. A. Thas, *Two infinite classes of perfect codes in metrically regular graphs*, J. Combin. Th. (B) **23** (1977) 236–238.
- [31] J. A. Thas, *Polar spaces, generalized hexagons and perfect codes*, J. Combin. Th. (A) **29** (1980) 87–93.
- [32] A. Tietäväinen, *On the non-existence of perfect codes over finite fields*, SIAM J. Appl. Math. **24** (1973) 88–96.
- [33] H. C. A. van Tilborg, *Uniformly packed codes*, proefschrift, Technische Hogeschool Eindhoven, 1 juni 1976.