HOOFDSTUK II VERMENIGVULDIGERS

Het mooie van differentieverzamelingen is dat het blokdiagram volledig bekend is als één blok gegeven wordt. We gaan nu een stap verder en differentieverzamelingen besturderen die volledig gegeven zijn als één getal (de vermenigvuldiger) gegeven is. Natuurlijk zijn er veel differentieverzamelingen waarvoor zo'n getal niet bestaat.

Definitie Een getal t heet vermenigvuldiger van een (v,k,λ)-differentieverzameling $\{a_1, a_2, \ldots, a_k\}_v$ als er een getal s bestaat zó dat

$$\{ta_1, ta_2, \ldots, ta_k\}_v = \{a_1+s, a_2+s, \ldots, a_k+s\}.$$

Voorbeeld 1. 2 is een vermenigvuldiger van $\{1,2,4\}_7$ met $s=0$.
2 is een vermenigvuldiger van $\{3,4,6\}_7$ met $s=2$
3 is een vermenigvuldiger van $\{1,3,4,5,9\}_{11}$ met $s=0$.

De volgende stelling garandeert het bestaan van een vermenigvuldiger onder bepaalde omstandigheden.

Stelling II.1. (Hall & Ryser, 1951)
Zij D een $\{v,k,\lambda\}$-differentieverzameling. Zij d een deler van $k-\lambda$ en veronderstel dat $(d,v)=1$, $d>\lambda$. Zij t een getal zó dat voor elke priemdeler p van d er een getal j bestaat met $p^j \equiv t \pmod v$. Dan is t een vermenigvuldiger van D.

Gevolg Zij D een $\{v,k,\lambda\}$-differentieverzameling.
Zij p een priemdeler van $k-\lambda$ en stel $p \nmid v$, $p>\lambda$.
Dan is p een vermenigvuldiger van D.

Voor het bewijs van de stelling verwijzen we naar M. Hall jr. Proc. Amer. Math. Soc. 7 (1956), 975-986 en voor een speciaal geval naar het boek van Hall. Het Gevolg krijgen we door $t=p, j=1$ te nemen. Vermoed wordt dat de restrictie $p>\lambda$ niet nodig is.

Voordat we voorbeelden van de stelling geven, laten we eerst zien dat we onder bepaalde omstandigheden aan mogen nemen dat $s=0$ en $a_1=1$.

Stelling 11.2. Zij $D=\{a_1,\dots,a_k\}_v$ een (v,k,λ)-differentieverzameling met vermenigvuldiger t. Stel $(t-1,v)=1$. Dan bestaat een u zó dat $D_u := \{a_1+u, a_2+u, \dots, a_k+u\} = \{t(a_1+u), \dots, t(a_k+u)\}_v$.

Bewijs. Stel $\{ta_1,\dots,ta_k\}_v = \{a_1+s,\dots,a_k+s\}_v$. Wegens $(t-1,v)=1$ kunnen we $(t-1)u \equiv -s \pmod v$ oplossen. Voor deze u geldt $u \equiv ut+s \pmod v$. Dus

$$D_u = \{a_1+u,\dots,a_k+u\}_v = \{a_1+s+tu,\dots,a_k+s+tu\}_v$$

$$= \{ta_1+tu,\dots,ta_k+tu\}_v = \{t(a_1+u),\dots,t(a_k+u)\}_v. \qquad \square$$

De stelling zegt dus dat als t een vermenigvuldiger is van D en $(t-1,v)=1$, dan is er een t-invariante differentieverzameling in D. De volgende stelling zegt dat we soms mogen aannemen dat $1 \in D$.

Stelling 11.3. Zij $D=\{a_1,\dots,a_k\}_v$ een (v,k,λ)-differentieverzameling die t-invariant is. Dan heeft elk van $a_1,\dots,a_k$ een deler >1 met v gemeen of is er een t-invariante (v,k,λ)-differentieverzameling die 1 bevat.

Bewijs. Stel $(a_j,v)=1$. Zonder beperking mogen we aannemen dat $(a_1,v)=1$. Zij $ba_1 \equiv 1 \pmod v$. Dan geldt

$$\{t(ba_1),\dots,t(ba_k)\}_v = \{b(ta_1),\dots,b(ta_k)\}_v = \{ba_1,\dots,ba_k\}_v.$$

Dus de verzameling $\{ba_1=1, ba_2, \dots, ba_k\}_v$ is ook t-invariant. Omdat $(b,v)=1$, is het bovendien een (v,k,λ)-differentieverzameling, immers elk verschil wordt met b vermenigvuldigd mod. v en

$$\{1,2,\dots,v-1\} \equiv \{b,2b,\dots,(v-1)b\} \pmod v. \qquad \square$$

(met vermenigvuldiger t)

Stel dat v priem is en D een (v,k,λ)-differentieverzameling. Volgens Stelling 11.2 is er dan een t-invariante (v,k,λ)-differentieverzameling. Volgens Stelling 11.3 mogen we bovendien aannemen dat 1 er toe behoort.

Voorbeeld 2. We construeren projectieve vlakken van orde 2, 3, 4 en 8. Volgens de Stelling van Singer is er een $(q^2+q+1, q+1, 1)$-differentieverzameling als q een priemmacht p is. Volgens het Gevolg van Stelling 11.1 is p een vermenigvuldiger. Volgens Stelling 11.2 is er zelfs een p-invariante differentieverzameling. We starten steeds met de aanname dat 1 die verzameling zit.

$q=2$, $p=2$, $v=7$ $\quad D=\{1,2,4\}_7$.

$q=3$, $p=3$, $v=13$ $\quad D=\{1,3,9,0\}_{13}$ (alleen 0 kan toegevoegd worden)

$q=4$, $p=2$, $v=21$ $\quad D=\{1,2,4,8,16,11$ dit gaat mis!

Dus elk element heeft een deler met 21 gemeen.

$$D=\{3,6,12,7,14\}_{21}$$

$q=8$, $p=2$, $v=73$ $\quad D=\{1,2,4,8,16,32,64,55,37\}_{73}$.

Uit het voorgaande volgt dat dit inderdaad differentieverzamelingen zijn. Als men Stelling 11.1 niet gelooft, is het ook direct te controleren. Zie ook Beth, Jungnickel & Lenz 4.3.e) p. 477: Geen proj. vlak van orde 6k, 10, 14, 15, 21.

Voorbeeld 3. Zij $v=37$, $k=9$, $\lambda=2$. Stel er is een (v,k,λ) differentieverz. Volgens het Gevolg is 7 een vermenigvuldiger. Omdat 37 priem is, is er een 7-invariante verzameling die 1 bevat. Dus

$$D=\{1,7,12,10,33,9,26,34,16\}_{37}$$

Dit blijkt inderdaad een $(37,9,2)$-differentieverzameling te zijn. Dus is het op isomorfie na de enige.

Voorbeeld 4. Zij $v=23$, $k=11$, $\lambda=5$. Stel er is een (v,k,λ)-differentieverzameling. Volgens Stelling 11.1 met $d=6$ is $t=9$ een vermenigvuldiger, want $2^5 \equiv 9$, $3^2 \equiv 9$. Wegens (23,8) is er een 9-invariante verzameling die 1 bevat. Dit geeft

$$\{1,2,3,4,6,8,9,12,13,16,18\}_{23}.$$

Dus is deze reeds bekende differentieverzameling uniek (op isomorfie na). Ook 2 en 3 zijn vermenigvuldigers!

Voorbeeld 5. Zij $v=111$, $k=11$, $\lambda=1$. Stel er is een (v,k,λ)-differentieverzameling. Volgens het Gevolg is 2 een vermenigvuldiger. Wegens Stelling 2 is er een 2-invariante differentieverzameling. Stel a behoort hiertoe en $37 \nmid a$. (Zo'n element is er.) Dan zitten ook $a, 2a, 4a, 8a, 16a, 32a, 64a, 17a, 34a, 68a, 25a, 50a$ in die verzameling. Maar al deze elementen zijn verschillend mod. 111. Dus bestaat er geen $(111,11,1)$-differentieverzameling.

want mod 37 krijgen we 12 verschillende waarden: 1, 2, 4, 8, 16, 32, 27, 17, 34, 31, 25, 13

Baumert heeft in zijn artikel Difference Sets in SIAM J. Appl. Math. 17(1969), 826-833 laten zien voor welke v, k, λ met $k \leq 100$ er differentieverzamelingen bestaan. Er zijn 74 zulke tripletten (v,k,λ). Daarvan zijn er 23 via kwadraatresten, 5 via vierdemachtresten $(37,9,2), (101,25,6),$ $(197,49,12)$ en via vierdemachtsresten met 0 (nl $(13,4,1)$ en $(109,28,7)$), 47 Singerverzamelingen (waarbij enkele reeds eerder voorkomen) en nog een paar andere uitvoerige constructies kan men vinden in het boek van Hall. Bij sommige tripletten bestaan meerdere, inequivalente differentieverzamelingen.

Er zijn totaal 748 tripletten (v,k,λ) die voldoen aan $(v-1)\lambda = k(k-1)$ en $v > k > \lambda$, $k < v/2$ en $3 \leq k \leq 100$. Ongeveer 80% van de tripletten viel af op grond van de volgende testen:

A) Als v even is en $n = k - \lambda$ is geen kwadraat, dan is er geen (v,k,λ)-differentieverzameling. (Stelling 9.1)

B) Zij p een priemdeler van n en w een deler van v met $(p,w)=1, w>1$. Als $p^f \equiv -1 \pmod{w}$ voor zekere $f>0$ en $\text{mult}_p(n)$ is oneven, dan is er geen (v,k,λ)-differentieverzameling. (Als aan de voorwaarden van Stelling 9.2 voldaan is, is B) toepasbaar.) ($\text{mult}_p(n) = e$ als $p^e \mid n, p^{e+1} \nmid n$)

C) Zij p een priemdeler van n en w een deler van v met $(p,w)=1, w>1$. Stel $p^f \equiv -1 \pmod{w}$ voor zekere $f>0$. Zij $e = \text{mult}_p(n)$ en $\ell = \text{mult}_p(v)$. Als $p^{[e/2]} \geq (v/w)\, p^{-\ell}$, dan is er geen (v,k,λ)-differentieverz.

D) Zij $q \equiv 3 \pmod 4$ een priemdeler van v. Zij $\ell = \text{mult}_q(v)$. Stel elke priemdeler p van n voldoet aan (i) $\text{ord}_p(q)$ is even of (ii) $\text{ord}_p(q^\ell) = q^{\ell-1}(q-1)/2$ of (iii) $p = q$. Als een (v,k,λ)-differentieverzameling bestaat, dan heeft de vergelijking $4n = x^2 + q y^2$ een oplossing in gehele getallen x en y die voldoen aan $x \geq 0$, $0 \leq y \leq v q^{-\ell}$, $x + y \leq 2 v q^{-\ell}$. ($\text{ord}_p(n)$ is het kleinste getal $a \in \mathbb{N}$ met $p^a \equiv 1 \pmod n$)

Stellingen B), C) en D) zijn in wezen bewezen door K. Yamamoto, Decomposition fields of difference sets, Pacific J. Math. 13 (1963), 337-352, voortbouwend op het werk van Bruck-Ryser-Chowla. Soortgelijke stellingen werden bewezen door Mann, Rankin en Turyn.

Van de overblijvende tripletten valt ongeveer de helft af door de techniek beschreven in dit hoofdstuk toe te passen. Op de resterende tripletten worden soortgelijke, maar ingewikkelder technieken losgelaten om te laten zien dat daarvoor geen differentieverzamelingen bestaan.