HOOFDSTUK 10 DIFFERENTIEVERZAMELINGEN

Een verzameling van k resten modulo v, $D = \{a_1, \dots, a_k\}_v$ heet een <u>(v,k,λ) – differentieverzameling</u> als er voor elke $d \not\equiv 0 \pmod v$ precies λ geordende paren $(a_i, a_j) \in D^2$ zijn zó dat $a_i - a_j \equiv d \pmod v$. Verder eisen we dat $0 < \lambda < k < v-1$.

<u>Voorbeelden</u>: 1. $\{1,2,4\}_7$ is een $(7,3,1)$-differentieverzameling. Immers de verschillen zijn $\pm 1, \pm 2, \pm 3 \pmod 7$.

2. $\{1,5,6,8\}_{13}$ is een $(13,4,1)$-differentieverzameling, want de verschillen zijn $\pm 4, \pm 5, \pm 1, \pm 6, \pm 3, \pm 2$.

<u>Stelling 10.1</u> Een verzameling resten mod. v, $D = \{a_1, \dots, a_k\}_v$ is een (v,k,λ)-differentieverzameling dan en slechts dan als de blokken

$$X_i = [\, a_1+i,\ a_2+i,\ \dots,\ a_k+i \,] \qquad (i = 0, 1, \dots, v-1)$$

waarbij de elementen mod. v gereduceerd worden, een (v,k,λ)-blokdiagram vormen.

Bewijs. $\Rightarrow$ We hebben v elementen en v blokken. Elk blok bevat k elementen en elk element zit in k blokken. Neem een vast paar elementen. Beschouw het verschil. Er zijn λ paren in de differentieverzameling die dit verschil hebben. Met elk zo'n paar correspondeert een blok, dat de twee betreffende elementen bevat, en omgekeerd, met elk blok dat beide elementen bevat correspondeert een paar in de differentieverzameling met hetzelfde verschil.

$\Leftarrow$ Vanwege de bovenomgeschreven correspondentie (bijectie) is het aantal blokken dat een vast paar elementen bevat gelijk aan het aantal paren in D^2 dat hetzelfde verschil mod. v heeft. Het eerste aantal is λ, het tweede dus ook. $D = X_0$ bestaat uit k elementen en we weten dat $0 < \lambda < k < v-1$. $\square$

Niet elk symmetrisch blokdiagram correspondeert met een differentieverz. Dit is alleen het geval als de incidentiematrix van het blokdiagram een circulant is.

Als de resten $\{a_1, \ldots, a_k\}_v$ een (v, k, λ) - differentieverzameling vormen, dan vormen de overige $v-k$ resten mod v ook een differentieverzameling. Dit leidt tot het complementaire blokdiagram met parameters $(v, v-k, v-2k+\lambda)$. Door zonodig het complement te nemen kunnen we dus $k \leq v/2$ maken.

1, 2 en 4 zijn juist de kwadraatresten van 7. In de getaltheorie spelen de kwadraatresten een belangrijke rol en in hoofdstuk 3 zijn enkele eigenschappen genoemd en sommige ook bewezen. Omdat elk priemgetal een primitieve wortel w heeft en voor $p > 2$ de kwadraatresten juist de even machten van w zijn, is duidelijk dat het product van twee kwadraatresten een kwadraatrest is, evenals het product van twee niet-kwadraatresten. Het product van een kwadraatrest en een niet-kwadraatrest is een niet-kwadraatrest. Verder is bewezen dat -1 een niet-kwadraatrest is als $p \equiv 3 \pmod 4$. Hieruit volgt:

Geldt ook voor priemmachten zie Beth et al p.264

<u>Stelling 10.2.</u> Zij p een priemgetal, $p \equiv 3 \pmod 4$, $p \geq 7$. Zij $p = 4t-1$. Dan vormen de $(p-1)/2$ kwadraatresten $D = \{a_1, \ldots, a_k\}_p$ een $(4t-1, 2t-1, t-1)$ - differentieverzameling.

Bewijs. Zij λ het aantal kwadraatresten a_i, a_j met $a_i - a_j \overset{v}{=} 1$. Zij c een kwadraatrest. Dan zijn ca_i en ca_j kwadraatresten met $ca_i - ca_j \overset{v}{=} c$. Door met c^{-1} te vermenigvuldigen (c^{-1} is ook een kwadraatrest) vinden we de oorspronkelijke oplossing weer terug. Er zijn dus precies λ oplossingen van $x - y \overset{v}{=} c$ in kwadraatresten x, y. Zij nu c een niet-kwadraatrest. Dan is $-c = c \cdot -1$ een kwadraatrest. Omdat er λ oplossingen van $x - y \overset{v}{=} -c$ in kwadraatresten zijn, zijn er ook λ oplossingen van $x - y \overset{v}{=} c$ in kwadraatresten, want met $a_i - a_j \overset{v}{=} -c$ correspondeert $a_j - a_i \overset{v}{=} c$. Dus $\lambda = \frac{(2t-1)(2t-2)}{4t-2}$

<u>Voorbeelden</u>. 3. $\{1, 3, 4, 5, 9\}_{11}$ vormt een $(11, 5, 2)$ - differentieverzameling.

4. $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}_{19}$ vormt een $(19, 9, 4)$ - differentieverzameling.

Gevolg. Als $p \equiv 3 \pmod 4$ priem is, bestaat er een Hadamardmatrix van orde $p+1$. Dus bestaan Hadamardmatrices van orde

$2, 4, 8, 12\ (=11+1),\ 16\ (=4^2),\ 20\ (=19+1),\ 24\ (=23+1),\ 32\ (=31+1),\ 40\ (=2\times 20),$
$44\ (=43+1),\ 48\ (=47+1),\ 60\ (=59+1),\ 64\ (=8\times 8),\ 68\ (=67+1),\ 72\ (=71+1),$
$80\ (=79+1),\ 84\ (=83+1),\ 88\ (=2\times 44),\ 96\ (=4\times 24).$

Elk symmetrisch blokdiagram met $\lambda = 1$ correspondeert met een projectief vlak. Men kan ook projectieve ruimten van hogere dimensie beschouwen. Zo krijgt men een uitgebreide klasse van differentieverzamelingen en daarmee van blokdiagrammen.

Stelling 10.3 (Singer, 1938). Voor elke priemmacht $q = p^s$ en elk natuurlijk getal $n \geq 2$ bestaat er een differentieverzameling met parameters

$$\left(\frac{q^{n+1}-1}{q-1},\ \frac{q^n-1}{q-1},\ \frac{q^{n-1}-1}{q-1} \right).$$

Voordat we het bewijs geven, tonen we aan de hand van voorbeelden aan hoe de differentieverzamelingen geconstrueerd kunnen worden.

Voorbeeld 8. We construeren een $(15,7,3)$- differentieverzameling. Daartoe kiezen we $q = (k-1)/\lambda = 2$ en n zó dat $\frac{q^n-1}{q-1} = 7$, dus $n=3$. Het lichaam met $q^{n+1} = 16$ elementen wordt voortgebracht door het primitieve polynoom $x^4 + x + 1$ over $\mathbb{F}_2$. We vinden de differentie-verzameling door de recurrentieformule $u_{n+4} \stackrel{2}{=} u_{n+1} + u_n$ te gebruiken, startend met $u_0 = u_1 = u_2 = 0, u_3 = 1$ (of met enige andere niet-triviale startwaarden.) We vinden $u_4 = u_5 = 0$, $u_6 = 1$, $u_7 = 1$, $u_8 = 0$, $u_9 = 1$, $u_{10} = 0$, $u_{11} = u_{12} = u_{13} = u_{14} = 1$. De differentieverzameling vinden we door de indices van de nullen te nemen:

$$\{0, 1, 2, 4, 5, 8, 10\}_{15}.$$

(Het is niet moeilijk na te gaan dat dit een differentieverzameling is. De getallen i uit de differentieverzameling corresponderen met de machten α^i op p. 19 voor welke de coëfficiënt van α^3 gelijk aan nul is.)

Voorbeeld 6. We construeren een $(13,4,1)$ - differentieverzameling. Nu is $q=3$ en $n=2$. Het lichaam van $q^{n+1}=27$ elementen wordt voortgebracht door het primitieve polynoom x^3-x+1 over F_3. Pas de recurrentie $u_{n+3} \overset{3}{=} u_{n+1} - u_n$ toe met $u_0=u_1=0, u_2=1$. Dat geeft $u_3=0, u_4=1, u_5=2, u_6=1, u_7=1, u_8=2, u_9=0, u_{10}=1=u_{11}=u_{12}\cdots$ Dit levert de differentieverzameling (projectief vlak van orde 3)

$$\{0,1,3,9\}_{13}.$$

(Door hier 5 (mod 13) bij op te tellen krijgen we voorbeeld 2.)

Voorbeeld 7. We construeren een $(21,5,1)$ - differentieverzameling. Nu is $q=4$ en $n=2$. Het grondlichaam is $F_4=\{0,1,w,w+1\}$ met $w^2=w+1$. Het polynoom x^3+wx^2+wx+w blijkt primitief te zijn over F_4. De recurrentieformule $u_{n+3}=wu_{n+2}+wu_{n+1}+wu_n$ met startwaarden $u_0=u_1=0$, $u_2=1$ levert $u_3=w, u_4=1, u_5=w+1$, $u_6=0, u_7=w+1, u_8=0, u_9=1, u_{10}=w+1, u_{11}=w+1, u_{12}=w$, $u_{13}=w+1, u_{14}=w+1, u_{15}=w+1, u_{16}=1, u_{17}=w, u_{18}=0, u_{19}=1$, $u_{20}=1$. Dit geeft de $(21,5,1)$ - differentieverzameling

$$\{0,1,6,8,18\}_{21}$$

die correspondeert met een projectief vlak van orde 4.

Het bewijs van Stelling 10.3 maakt gebruik van eindige projectieve ruimten, een generalisatie van de eindige projectieve vlakken die we krijgen door $n=2$ te nemen. Zij F_q het eindige lichaam met $q=p^s$ elementen. Beschouw de vectorruimte

$$F_q^{n+1}=\{(a_0,a_1,\ldots,a_n) \mid a_i\in F_q \text{ voor } i=0,1,\ldots,n\}.$$

Een punt in onze projectieve ruimte is de verzameling vectoren

$$\{(bx_0,\ldots,bx_n) \mid b\in F_q \text{ variabel}, (x_0,\ldots,x_n)\in F_q^{n+1}, \text{ niet nul, vast}\}$$

In het algemeen is een $(k+1)$ - dimensionale deelruimte van F_q^{n+1} een k - dimensionale deelruimte van onze projectieve ruimte. Onze projectieve ruimte is dus n - dimensionaal en heeft $v=\dfrac{q^{n+1}-1}{q-1}$ punten. Een $(n-1)$ - dimensionale deelruimte heet een hypervlak. Een hypervlak omvat $k=\dfrac{q^n-1}{q-1}$ punten. Als je twee verschillende hypervlakken snijdt, krijg je een $(n-2)$ - dimensionale deelruimte en dus een ruimte met $\lambda=\dfrac{q^{n-1}-1}{q-1}$ punten. We noteren onze projectieve ruimte met $PG(n,p^s)$

Bewijs van Stelling 10.3. De projectieve ruimte $PG(n,q)$ heeft v punten (elementen) en v hypervlakken (blokken). Immers elk hypervlak in $PG(n,q)$ is een hypervlak in $\mathbb{F}_q^{n+1}$, staat dus loodrecht op een lijn in $\mathbb{F}_q^{n+1}$, d.w.z. een punt in $PG(n,q)$. Elk hypervlak bevat k punten en twee hypervlakken snijden elkaar in λ punten. Een hypervlak dat een gegeven punt bevat staat loodrecht op een punt in het loodhypervlak op dat gegeven punt. Zo volgt dat elk punt in k hypervlakken ligt. We hebben dus dat ~~het duale een blokdiagram is, en dus dat de~~ hypervlakken een blokdiagram vormen, omdat $v > k$ en $\lambda > 0$. We moeten alleen nog bewijzen dat de incidentiematrix cyclisch is.

Zij x een primitieve wortel van $\mathbb{F}_{q^{n+1}}$ met als primitief polynoom

(10.1) $$F(X) = X^{n+1} + c_n X^n + \ldots + c_1 X + c_0, \qquad c_i \in \mathbb{F}_q.$$

Dus $F(x) = 0$, d.w.z. $x^{n+1} = -c_n x^n \ldots - c_1 x - c_0$. Door steeds hiermee te reduceren kunnen we elke macht x^i schrijven als

(10.2) $$x^i = a_0 + a_1 x + \ldots + a_n x^n, \qquad a_j \in \mathbb{F}_q.$$

De $q^{n+1}-1$ verschillende machten van x corresponderen met de $q^{n+1}-1$ verschillende vectoren $(a_0, \ldots, a_n) \in \mathbb{F}_q^{n+1}$ ongelijk aan $(0,0,\ldots,0)$. Merk op dat de q vectoren $0, 1, x^v, x^{2v}, \ldots, x^{(q-2)v}$ alle voldoen aan de vergelijking $z^q = z$. (Bijv. $(x^v)^q = (x^{\frac{q^{n+1}-1}{q-1}})^q = (x^{q^{n+1}-1})(x^{\frac{q^{n+1}-1}{q-1}}) = 1 . x^v = x^v$.) Omdat er hoogstens q oplossingen zijn, zijn dit alle oplossingen. De vectoren $0, 1, x^v, x^{2v}, \ldots, x^{(q-2)v}$ vormen dus het deellichaam $\mathbb{F}_q$ van $\mathbb{F}_{q^{n+1}}$. Dus als $(x^v)^s = t$, dan is $t \in \mathbb{F}_q$, en dan volgt uit (10.2)

$$x^{i+sv} = t . x^i = t(a_0 + a_1 x + \ldots + a_n x^n).$$

Dus x^i en x^j corresponderen met hetzelfde punt in $PG(n,q)$ als $i-j$ door v deelbaar is. Het omgekeerde is ook waar, want als $x^j / x^i \in \mathbb{F}_q$, dan volgt $x^{j-i} \in \{0, 1, x^v, x^{2v}, \ldots, x^{(q-2)v}\}$.

De machten $1, x, x^2, \ldots, x^{v-1}$ representeren dus precies de v punten van $PG(n,q)$, en corresponderen dus precies met de v hypervlakken van $PG(n,q)$ waar ze loodrecht op staan.

Beschouw nu de afbeelding $f: PG(n,q) \to PG(n,q)$, gegeven door $f(0) = 0$, $f(x^i) = x^{i+1}$ voor $i \in \mathbb{Z}$. Merk op dat f^ℓ een punt $\neq 0$ van $PG(n,q)$ op zichzelf afbeeldt dan en slechts dan als $v \mid \ell$.

<u>Bewijs van Stelling 10.3.</u> De projectieve ruimte $PG(n,q)$ heeft v punten (elementen) en v hypervlakken (blokken). Immers elk hypervlak in $PG(n,q)$ is een hypervlak in $\mathbb{F}_q^{n+1}$, staat dus loodrecht op een lijn in $\mathbb{F}_q^{n+1}$, d.w.z. een punt in $PG(n,q)$. Elk hypervlak bevat k punten en twee hypervlakken snijden elkaar in λ punten. Een hypervlak dat een gegeven punt bevat staat loodrecht op een punt in het loodhypervlak op dat gegeven punt. Zo volgt dat elk punt in k hypervlakken ligt. We hebben dus dat ~~het duale een blokdiagram is, en dus dat de~~ hypervlakken een blokdiagram vormen, omdat $v-1 > k$ en $\lambda > 0$.
We moeten alleen nog bewijzen dat de incidentiematrix cyclisch is.

Zij x een primitieve wortel van $\mathbb{F}_{q^{n+1}}$ met als primitief polynoom

(10.1) $$F(X) = X^{n+1} + c_n X^n + \dots + c_1 X + c_0, \qquad c_i \in \mathbb{F}_q.$$

Dus $F(x) = 0$, d.w.z. $x^{n+1} = -c_n x^n \dots - c_1 x - c_0$. Door steeds hiermee te reduceren kunnen we elke macht x^i schrijven als

(10.2) $$x^i = a_0 + a_1 x + \dots + a_n x^n, \qquad a_j \in \mathbb{F}_q.$$

De $q^{n+1}-1$ verschillende machten van x corresponderen met de $q^{n+1}-1$ verschillende vectoren $(a_0, \dots, a_n) \in \mathbb{F}_q^{n+1}$ ongelijk aan $(0,0,\dots,0)$. Merk op dat de q vectoren $0, 1, x^v, x^{2v}, \dots, x^{(q-2)v}$ alle voldoen aan de vergelijking $z^q = z$. (Bijv. $(x^v)^q = (x^{\frac{q^{n+1}-1}{q-1}})^q = (x^{q^{n+1}-1})(x^{\frac{q^{n+1}-1}{q-1}}) = 1 \cdot x^v = x^v$.) Omdat er hoogstens q oplossingen zijn, zijn dit alle oplossingen. De vectoren $0, 1, x^v, x^{2v}, \dots, x^{(q-2)v}$ vormen dus het deellichaam $\mathbb{F}_q$ van $\mathbb{F}_{q^{n+1}}$. Dus als $(x^v)^s = t$, dan is $t \in \mathbb{F}_q$, en dan volgt uit (10.2)

$$x^{i+sv} = t \cdot x^i = t(a_0 + a_1 x + \dots + a_n x^n).$$

Dus x^i en x^j corresponderen met hetzelfde punt in $PG(n,q)$ als $i-j$ door v deelbaar is. Het omgekeerde is ook waar, want als $x^j / x^i \in \mathbb{F}_q$, dan volgt $x^{j-i} \in \{0, 1, x^v, x^{2v}, \dots, x^{(q-2)v}\}$.

De machten $1, x, x^2, \dots, x^{v-1}$ representeren dus precies de v punten van $PG(n,q)$, en corresponderen dus precies met de v hypervlakken van $PG(n,q)$ waar ze loodrecht op staan.

Beschouw nu de afbeelding $f: PG(n,q) \to PG(n,q)$, gegeven door $f(0) = 0$, $f(x^i) = x^{i+1}$ voor $i \in \mathbb{Z}$. Merk op dat f^ℓ een punt $\neq 0$ van $PG(n,q)$ op zichzelf afbeeldt dan en slechts dan als $v \mid \ell$.

Ofwel, in vectornotatie, wegens (10.1) en (10.2),

$$f: (a_0, a_1, \dots, a_n) \longmapsto (-a_n c_0, a_0 - a_n c_1, \dots, a_{n-1} - a_n c_{n-1})$$

Omdat het rechterlid lineair in de a_j's is, is f een homomorfisme (d.w.z. $f(\mu\vec{a} + \nu\vec{b}) = \mu f(\vec{a}) + \nu f(\vec{b})$; ga na). Het is zelfs een isomorfisme. Dus f beeldt elke deelruimte van dimensie ℓ af op een deelruimte van dimensie ℓ en in het bijzonder elk hypervlak van $PG(n,q)$ op een hypervlak van $PG(n,q)$. Het is duidelijk dat f de punten van $PG(n,q)$ cyclisch verwisselt. We zullen hetzelfde aantonen voor de hypervlakken. We weten dat f^v elk punt van $PG(n,q)$ op zichzelf afbeeldt (en dat f^μ voor $0<\mu<v$ geen enkel punt op zichzelf afbeeldt.) Stel dat f^j een hypervlak op zichzelf afbeeldt. Dan permuteert f^j de k punten van het hypervlak, en wel in cycles ter lengte $t := v/(v,j)$. Nu volgt dat de k punten van het hypervlak in groepjes van grootte t uiteenvallen en dus $t \mid k$. Uit $t \mid v$, $t \mid k$ en $v - qk = 1$ volgt $t = 1$. Dus $v = (v,j)$, d.w.z. $v \mid j$. Dus $f^0, f^1, \dots, f^{v-1}$ toegepast op een hypervlak levert v verschillende hypervlakken, d.w.z. allemaal. De hypervlakken van $PG(n,q)$ worden dus ook door f cyclisch verwisseld. Als we dus de elementen uit één hypervlak nemen, $x^{i_1}, x^{i_2}, \dots, x^{i_k}$ met $0 \le i_1 < i_2 < \dots < i_k \le v-1$, dan vormt $\{i_1, i_2, \dots, i_k\}_v$ een (v,k,λ)-differentieverzameling. $\square$

punt $\neq 0$

In de voorbeelden hebben we het hypervlak genomen dat loodrecht staat op x^n, d.w.z. alle machten x^i met $a_n = 0$. Voor voorbeeld 5 is dit af te leiden uit de tabel op p. 18. Voor voorbeeld 7 is dit uitgewerkt op p. 61. De recurrentie-relatie (corresponderend met het primitieve polynoom) is een eenvoudige manier om de coëfficienten van x^n te bepalen zonder de termen te hoeven uitrekenen. Immers, omdat $x^{i+n} = -c_n x^{i+n-1} - c_{n-1} x^{i+n-2} \dots - c_0 x^i$ geldt voor de coefficient u_i van x^n dat $u_{i+n} = -c_n u_{i+n-1} \dots - c_0 u_i$. Als we met andere beginwaarden starten, krijgen we een ander hypervlak, d.w.z. een cyclische verschuiving van het hypervlak loodrecht op x^n.

Voorbeeld 7 (vervolg)

Een primitief polynoom van F_{64} over F_4 wordt gegeven door x^3+wx^2+wx+w. De elementen zijn dus 0,

1	$=$	1		
x	$=$		x	
x^2	$=$			x^2
x^3	$=$	w	$+\ wx$	$+\ wx^2$
x^4	$=$	$w+1$	$+\ x$	$+\ x^2$
x^5	$=$	w	$+\ x$	$+\ (w+1)x^2$
x^6	$=$	1	$+\ (w+1)x$	
x^7	$=$		x	$+\ (w+1)x^2$
x^8	$=$	1	$+\ x$	
x^9	$=$		x	$+\ x^2$
x^{10}	$=$	w	$+\ wx$	$+\ (w+1)x^2$
x^{11}	$=$	1	$+\ (w+1)x$	$+\ (w+1)x^2$
x^{12}	$=$	1		$+\ wx^2$
x^{13}	$=$	$w+1$	$+\ wx$	$+\ (w+1)x^2$
x^{14}	$=$	1	$+\ wx$	$+\ (w+1)x^2$
x^{15}	$=$	1		$+\ (w+1)x^2$
x^{16}	$=$	1		$+\ x^2$
x^{17}	$=$	w	$+\ (w+1)x$	$+\ wx^2$
x^{18}	$=$	$w+1$	$+\ x$	
x^{19}	$=$		$(w+1)x$	$+\ x^2$
x^{20}	$=$	w	$+\ wx$	$+\ x^2$
x^{21}	$=$	w		
x^{22}	$=$		wx	
x^{23}	$=$			wx^2
x^{24}	$=$	$w+1$	$+\ (w+1)x$	$+\ (w+1)x^2$
$-$	$-$	$-$	$-$	$-$
x^{42}	$=$	$w+1$		
x^{43}	$=$		$(w+1)x$	
x^{44}	$=$			$(w+1)x^2$
x^{45}	$=$	1	$+\ x$	$+\ x^2$
$-$	$-$	$-$	$-$	$-$

Hypervlak $a_2=0$ geeft $\{0,1,6,8,18\}_{21}$

Hypervlak $a_0=0$ geeft $\{1,2,7,9,19\}_{21}$

Hypervlak $a_1=0$ geeft $\{0,2,12,15,16\}_{21}$

Hypervlak $(\perp x^8)$ $a_0+a_1=0$ geeft $\{2,3,8,10,20\}_{21}$

(Merk op dat $a_0=1$ geen hypervlak geeft.)

Hypervlak $(\perp x^3)$ $a_0+a_1+a_2=0$ geeft $\{5,8,9,14,16\}_{21}$