HOOFDSTUK 9. DE STELLING VAN BRUCK-RYSER-CHOWLA

In dit hoofdstuk behandelen we twee stellingen die impliceren dat voor zekere waarden van v, k, λ er geen (v,k,λ)-blokdiagram is. Zij $n = k-\lambda$. De eerste stelling gaat over even v, de tweede over oneven v.

Stelling 9.1. Als in een (v,k,λ) blokdiagram v even is, dan is $n = k-\lambda$ een kwadraat.

Bewijs. Wegens $\det A = \det A^T$ geldt (vgl. bewijs Stelling 7.2 met $r=k$)

$$(\det A)^2 = (k+(v-1)\lambda)(k-\lambda)^{v-1} \overset{(8.1)}{=\!=} k^2(k-\lambda)^{v-1}.$$

Omdat v even is, is $k-\lambda = \left(\dfrac{\det A}{k(k-\lambda)^{(v-2)/2}}\right)^2$ een kwadraat. □

Stelling 9.2. (Bruck-Ryser-Chowla). Als in een (v,k,λ)-blokdiagram v oneven is, dan heeft de vergelijking

$$z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2 \qquad (n = k-\lambda)$$

een oplossing in gehele getallen x, y, z met $(x,y,z) \neq (0,0,0)$.

Gevolg Er is geen projectief vlak van orde 6 en dus geen volledig stel O.L.V. van orde 6. Stel nl. dat het wel bestaat. Dan zou een $(43,7,1)$-blokdiagram bestaan, en dus $z^2 = 6x^2 - y^2$ een niet-triviale oplossing hebben. Door gemeenschappelijke delers weg te delen, zorgen we er voor dat $(x,y,z)=1$. Uit $3 \mid 6x^2$ volgt $3 \mid y^2+z^2$. Maar $y^2 \overset{3}{=} 0$ of 1 en $z^2 \overset{3}{=} 0$ of 1, dus $y^2 \overset{3}{=} 0$ en $z^2 \overset{3}{=} 0$, ofwel $3 \mid y$ en $3 \mid z$. Dus $9 \mid y^2+z^2 = 6x^2$ ofwel $3 \mid 2x^2$. Hieruit volgt $3 \mid x$. Dus $3 \mid (x,y,z)$, een tegenspraak.

Het bewijs van Stelling 2 eist wat voorbereidingen. Lemma 1 wordt bewezen in het college Getaltheorie.

LEMMA 1. Elk natuurlijk getal n is te schrijven als som van vier kwadraten, $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$ met $b_1, b_2, b_3, b_4 \in \mathbb{Z}$.

LEMMA 2. Zij A de incidentiematrix van een (v,k,λ)-blokdiagram. Zij

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_v \end{pmatrix} \quad \text{en} \quad \vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_v \end{pmatrix} = A\vec{x}$$

Dan geldt

$$y_1^2 + \ldots + y_v^2 = (k-\lambda)(x_1^2 + \ldots + x_v^2) + \lambda (x_1 + \ldots + x_v)^2.$$

Bewijs. $y_1^2 + \ldots + y_v^2 = \vec{y}^T\vec{y} = (A\vec{x})^T A\vec{x} = \vec{x}^T A^T A \vec{x} =$

$$\overset{(8.1)}{=\!=} \vec{x}^T \left((k-\lambda) I_v + \lambda J_{v,v} \right) \vec{x} = (k-\lambda)\, \vec{x}^T\vec{x} + \lambda\, \vec{x}^T J_{v,v} \vec{x}$$

$$= (k-\lambda)(x_1^2 + x_2^2 + \ldots + x_v^2) + \lambda (x_1 + x_2 + \ldots + x_v)^2.$$

LEMMA 3. Stel $b_1, b_2, b_3, b_4 \in \mathbb{Z}$, $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$.
Beschouw

$$S = \begin{pmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & -b_4 & b_3 \\ b_3 & b_4 & b_1 & -b_2 \\ b_4 & -b_3 & b_2 & b_1 \end{pmatrix}$$

Dan geldt a) $SS^T = S^TS = n I_4$

b) $|\det S| = n^2$.

Bewijs. a) Ga na.

b) $(\det S)^2 = (\det S^T)(\det S) = \det(S^TS) = \det(nI_4) = n^4$.

Bewijs van Stelling 8.2. Stel er bestaat een (v,k,λ)-blokdiagram. Zij $n = k - \lambda$. Volgens Lemma 1 zijn er gehele getallen b_1, b_2, b_3, b_4 zó dat

(1) $$n = b_1^2 + b_2^2 + b_3^2 + b_4^2.$$

Zij $\vec{z} = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_v \end{pmatrix}$ een willekeurige vector. We onderscheiden twee gevallen:

a) $v \equiv 1 \pmod 4$.

Voor $\vec{z}_i := (z_{4i+1}, z_{4i+2}, z_{4i+3}, z_{4i+4})$ schrijven we

$$(2) \quad \vec{x}_i = \begin{pmatrix} x_{4i+1} \\ x_{4i+2} \\ x_{4i+3} \\ x_{4i+4} \end{pmatrix} := S^{-1} \begin{pmatrix} z_{4i+1} \\ z_{4i+2} \\ z_{4i+3} \\ z_{4i+4} \end{pmatrix} = S^{-1} \vec{z}_i \qquad (i = 0, 1, \ldots, \left[\tfrac{v}{4}\right] - 1).$$

Hieruit volgt $x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 + x_{4i+4}^2 = \vec{x}_i^{\,T} \vec{x}_i = (S^{-1}\vec{z}_i)^T (S^{-1}\vec{z}_i)$

$= \vec{z}_i^{\,T} S^{-1\,T} S^{-1} \vec{z}_i = \vec{z}_i^{\,T} (SS^T)^{-1} \vec{z}_i = \frac{1}{n} \vec{z}_i^{\,T} \vec{z}_i = \frac{1}{n}(z_{4i+1}^2 + z_{4i+2}^2 + \ldots + z_{4i+4}^2)$ *

Verder definieren we $x_v = z_v$. Nu volgt

$$(3) \quad n(x_1^2 + x_2^2 + \ldots + x_{v-1}^2 + x_v^2) = z_1^2 + z_2^2 + \ldots + z_{v-1}^2 + n z_v^2.$$

Volgens Lemma 2 geldt voor $\vec{y} := A\vec{x}$ dat

$$(4) \quad y_1^2 + y_2^2 + \ldots + y_v^2 = n(x_1^2 + x_2^2 + \ldots + x_v^2) + \lambda (x_1 + x_2 + \ldots + x_v)^2$$
$$= z_1^2 + z_2^2 + \ldots z_{v-1}^2 + n z_v^2 + \lambda (x_1 + x_2 + \ldots + x_v)^2.$$

In feite staat hier een identiteit in $z_1, \ldots, z_v$ met rationale coëfficiënten. Immers $x_1, \ldots, x_v$ is met rationale coëfficiënten lineair in $z_1, \ldots, z_v$ uit te drukken en daarmee ook $y_1, \ldots, y_v$. Door in (4) links en rechts zo uit te schrijven, krijgen we een kwadratische identiteit in $z_1, \ldots, z_v$ met rationale coëfficiënten. Zij $w = x_1 + \ldots + x_v$. Dan is ook w lineair in $z_1, \ldots, z_v$ uit te drukken met rationale coëfficiënten en geldt

$$(5) \quad y_1^2 + y_2^2 + \ldots + y_v^2 = z_1^2 + z_2^2 + \ldots + z_{v-1}^2 + n z_v^2 + \lambda w^2.$$

We ~~kiezen~~ gaan straks $z_1, \ldots, z_{v-1}$ ~~nu zo~~ zo kiezen dat $y_1^2 = z_1^2$, $y_2^2 = z_2^2, \ldots, y_{v-1}^2 = z_{v-1}^2$. Dan krijgen we een simpele identiteit in z_v van het gewenste type, nl.

$$y_v^2 = n z_v^2 + \lambda w^2.$$

Omdat we z_v vrij kunnen kiezen, kunnen we aantonen dat er een niet-triviale oplossing is.

Stel $y_j = c_{j1} z_1 + c_{j2} z_2 + \ldots + c_{jv} z_v \qquad (j = 1, \ldots, v)$.

Als $c_{11} \neq 1$, dan eisen we $y_1 = z_1$, dus $(c_{11}-1) z_1 + c_{12} z_2 + \ldots + c_{1v} z_v = 0$.
Als $c_{11} = 1$, dan eisen we $y_1 = -z_1$, dus $(c_{11}+1) z_1 + c_{12} z_2 + \ldots + c_{1v} z_v = 0$.
In beide gevallen is $y_1^2 = z_1^2$ en is z_1 lineair uit te drukken in $z_2, \ldots, z_v$ met rationale coëfficiënten. Dus houden we over

$$y_2^2 + y_3^2 + \ldots + y_v^2 = z_2^2 + \ldots + z_{v-1}^2 + n z_v^2 + \lambda w^2$$

waarbij $y_2, y_3, \ldots, y_v, w$ lineaire uitdrukkingen in $z_2, \ldots, z_v$ zijn met rationale coëfficiënten. Door dit proces achtereen volgens op $y_2, y_3, \ldots, y_{v-1}$ toe te passen, vinden we uiteindelijk

$$y_v^2 = n z_v^2 + \lambda w^2$$

waarbij y_v en w lineaire uitdrukkingen in z_v zijn met rationale coëfficiënten. Zij $y_v = \frac{a_1}{d_1} z_v$ en $w = \frac{a_2}{d_2} z_v$ met $a_1, a_2, d_1, d_2 \in \mathbb{Z}$

en $d_1 \geq 1, d_2 \geq 1$. Omdat z_v nog vrij is, geldt $\frac{a_1^2}{d_1^2} = n + \lambda \frac{a_2^2}{d_2^2}$,

ofwel $(a_1 d_2)^2 = n (d_1 d_2)^2 + \lambda (a_2 d_1)^2$. Omdat $d_1 d_2 \neq 0$, heeft $z^2 = n x^2 + \lambda y^2$ dus een niet-triviale oplossing $x, y, z \in \mathbb{Z}$. Dit bewijst de stelling voor $v \equiv 1 \pmod 4$.

b) $v \equiv 3 \pmod 4$.
We voegen een variabele z_{v+1} toe en definiëren (2) voor $i = 0, 1, \ldots, \left[\frac{v}{4}\right]$
Nu volgt in plaats van (3)

(3′) $\quad n(x_1^2 + x_2^2 + \ldots + x_v^2 + x_{v+1}^2) = z_1^2 + z_2^2 + \ldots + z_v^2 + z_{v+1}^2$

en door $\vec{y} = A\vec{x} = A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_v \end{pmatrix}$ te definiëren in plaats van (4)

(4′) $\quad y_1^2 + y_2^2 + \ldots + y_v^2 + n x_{v+1}^2 = z_1^2 + z_2^2 + \ldots + z_v^2 + z_{v+1}^2 + \lambda (x_1 + \ldots + x_v)^2$,

dus met $w := x_1 + \ldots + x_v$ in plaats van (5)

(5′) $\quad y_1^2 + y_2^2 + \ldots + y_v^2 + n x_{v+1}^2 = z_1^2 + z_2^2 + \ldots + z_v^2 + z_{v+1}^2 + \lambda w^2$

Hierbij zijn $y_1, y_2, \ldots, y_v, x_{v+1}$ en w lineaire vormen in $z_1, \ldots, z_v$

met rationale coëfficiënten. Vervolgens kiezen we als onder a) $z_1, \ldots, z_v$ zó dat $y_i^2 = z_i^2$ voor $i = 1, \ldots, v$. Dan volgt

$$n x_{v+1}^2 = z_{v+1}^2 + \lambda w^2$$

waarbij x_{v+1} en w rationale veelvouden zijn van z_{v+1}. Doorredenerend als onder a) vinden we dat $nx^2 = z^2 + \lambda y^2$ een niet-triviale oplossing heeft. □

Als toepassing bewijzen we Stelling 4.3, daarbij gebruik makend van een andere stelling uit het Getaltheorie college.

Stelling 9.3 = Stelling 4.3. (Bruck-Ryser, 1949)
Zij $n \equiv 1 \pmod 4$ of $n \equiv 2 \pmod 4$. Stel er is een priemgetal p met $p \equiv 3 \pmod 4$ zó dat n een oneven aantal factoren p bevat. Dan is er geen volledig stel O.L.V. van orde n en ook geen projectief vlak van orde n.

Bewijs. Volgens Stelling 6.5 zijn beide beweringen equivalent. Stel er is wel een projectief vlak van orde n. Dan bestaat er dus een $(n^2+n+1, n+1, 1)$-blokdiagram. Omdat $n^2+n+1 = n(n+1)+1$ oneven is, heeft volgens Stelling 9.2 de vergelijking

$$z^2 = nx^2 + (-1)^{\frac{v-1}{2}} y^2$$

een niet-triviale oplossing. Omdat $n \equiv 1 \pmod 4$ of $n \equiv 2 \pmod 4$, volgt dat $(v-1)/2 = n(n+1)/2$ oneven is. Dus $z^2 = nx^2 - y^2$ heeft een niet-triviale oplossing, ofwel nx^2 is te schrijven als som van twee kwadraten, $y^2 + z^2$. Volgens een stelling uit de Getaltheorie deelt dan elk priemgetal $p \equiv 3 \pmod 4$ het getal nx^2 tot een even macht. Maar dan deelt p het getal n ook tot een even macht. □

Als $n \equiv 0 \pmod 4$ of $n \equiv 3 \pmod 4$, dan is $(v-1)/2$ even. We krijgen dan dat $z^2 = nx^2 + y^2$ een niet-triviale oplossing heeft. Omdat dit een ware bewering is (neem $z = y = 1, x = 0$) levert de stelling van Bruck-Ryser-Chowla nu geen nieuwe informatie op.