Diophantische vergelijkingen
Partieelbreuksplitsing
BCH codes
Lanczos algoritme
Ijle stelsels
GGD
Padé benadering
Gram-Schmidt orthogonalisatie
CD
Hankel matrices
Partiële realisatie
Orthogonale veeltermen
Eigenwaarden
Krylov rijen
Kettingbreuken
Lineaire systemen
Getaltheorie
Toeplitz matrices
Het eindeloze verhaal

Het Euclidisch Algoritme:

Een rode draad

door de wiskunde en toepassingen

Adhemar Bultheel

Departement Computerwetenschappen,

K.U.Leuven

Euclides en Gehele Getallen

$r_{-1} = 8$ $\qquad$ $r_0 = 6$ $\qquad$ $GGD(8,6)$?

$$
\begin{aligned}
8 - 6 = 2 \quad &\Longrightarrow \quad \frac{8}{6} = 1 + \frac{2}{6} \\
6 - 2 = 4 \\
4 - 2 = 2 \quad &\Longrightarrow \quad \frac{6}{2} = 3 + \frac{0}{2} \\
2 - 2 = 0
\end{aligned}
$$

Dus $GGD(8,6) = 2$

$$
\begin{aligned}
2 &= 8 \,\mathbf{mod}\, 6 \\
0 &= 6 \,\mathbf{mod}\, 2
\end{aligned}
$$

$GGD(a,b)$
$r_{-1} = a,\ r_0 = b$
$k = 1$
while $r_{k-1} \neq 0$
    stel $r_k = r_{k-2} \,\mathbf{mod}\, r_{k-1}$
    $k = k + 1$
endwhile

Euclides en veeltermen

$$
\begin{aligned}
r_{-1} &= x^4 - x^3 - x^2 + 3x + 2 \\
r_0 &= x^3 - 3x^2 - x - 1
\end{aligned}
$$

$$GGD(r_{-1}, r_0) = (x - 1) \text{ want}$$

$$
\begin{aligned}
r_1 &= (r_{-1} \,\mathbf{mod}\, r_0) = 2x^2 + 2x - 4 \\
r_2 &= (r_0 \,\mathbf{mod}\, r_1) = r_2 = x - 1 \\
r_3 &= (r_1 \,\mathbf{mod}\, r_2) = 0
\end{aligned}
$$

Kettingbreuken

gehele getallen

$$\frac{8}{6} = 1+\frac{2}{6} = 1+\frac{1}{\frac{6}{2}} = 1+\frac{1}{3+\frac{0}{2}}$$

veeltermen

$$\begin{aligned} r_{-1} &= x^4 - x^3 - x^2 + 3x + 2 \\ r_0 &= x^3 - 3x^2 - x - 1 \end{aligned}$$

$$\begin{aligned} \frac{r_{-1}}{r_0} &= (x-2) + \frac{r_1}{r_0} = (x-2) + \frac{1}{\frac{r_0}{r_1}} \\ &= (x-2) + \frac{1}{\frac{1}{2}x + \frac{r_2}{r_1}} = (x-2) + \frac{1}{\frac{1}{2}x + \frac{1}{\frac{r_1}{r_2}}} \\ &= (x-2) + \frac{1}{\frac{1}{2}x + \frac{1}{(2x+4) + \frac{0}{x-1}}} \end{aligned}$$

EA en KB eindigen!

- absolute waarde $|r_k| \searrow$ en ≥ 0
- graad veeltermen $\deg r_k \searrow$ en ≥ 0

Euclidisch domein

integriteitsdomein met valuatie ∂

$$\partial : D \to \mathbb{N}$$

$$\begin{aligned}
&\partial(a) = 0 \ \text{ asa } \ a = 0 \\
&\partial(ab) \geq \partial(a), \quad \forall a, b \neq 0 \\
&a = bq + r, \quad \partial(r) < \partial(b), \quad b \neq 0
\end{aligned}$$

In een Euclidisch domein is een GGD uniek
op een eenheid (inverteerbaar element) na

Voor $\mathbb{Z}$: eenheden zijn $\{1, -1\}$

Voor $\mathbb{C}[x]$: eenheden zijn $\mathbb{C}_0$

EA eindigt want $\partial(r_k) \searrow$ en ≥ 0

Onze interesse gaat naar het geval
waarbij het EA niet eindigt

Differentievergelijkingen

$$\frac{r_{k-2}}{r_{k-1}} = q_k + \frac{r_k}{r_{k-1}}$$

$$\Downarrow$$

$$r_k = r_{k-2} - r_{k-1}q_k$$

$$\Downarrow$$

$$[r_{k-1} \quad r_k] = [r_{k-2} \quad r_{k-1}]V_k; \quad V_k = \begin{bmatrix} 0 & 1 \\ 1 & -q_k \end{bmatrix}$$

2de orde differentievergelijking

2 fundamentele oplossingen

$$\begin{bmatrix} u_{-1} & u_0 \\ v_{-1} & v_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} u_{k-1} & u_k \\ v_{k-1} & v_k \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_k \end{bmatrix}$$

$$u_{k-1}v_k - v_{k-1}u_k = (-1)^k$$

$$\Downarrow$$

$$GGD(u_k, v_k) = GGD(u_{k-1}, u_k) = GGD(v_{k-1}, v_k) = 1$$

elke oplossing is een l.c. van $\{u_k\}$ en $\{v_k\}$

$$r_k = r_{-1}u_k + r_0v_k$$

Diophantische vergelijkingen

$$r_k = r_{-1}u_k + r_0 v_k = au_k + bv_k$$

$$\begin{array}{lllllll} (1) & k = n-1 & : & g & = & au_{n-1} + bv_{n-1}; & g = GGD(a,b) \\ (2) & k = n & : & 0 & = & au_n + bv_n & \end{array}$$

(1) $GGD(a,b)$ = l.c. van a en b
(2) EA lost diophantische vergelijking op

$$ax + by = 0, \qquad GGD(x,y) = 1$$

algemeen

$$ax + by = c$$

heeft oplossing asa $c = sg$ en die is

$$x = su_{n-1} + tu_n$$

$$y = sv_{n-1} + tv_n$$

met t willekeurig want

$$ax + by = s(au_{n-1} + bv_{n-1}) + t(au_n + bv_n) = sg + 0$$

Partieelbreuksplitsing

$$ax + by = c$$

$$\Downarrow$$

$$\frac{x}{b} + \frac{y}{a} = \frac{c}{ab}$$

Om al deze redenen

bereken ook x en y

$\therefore$ $\boxed{\text{bereken ook } \{u_k\} \text{ en } \{v_k\}}$

Dit is het Uitgebreide Euclidisch Algoritme (UEA)

UEA

In elke stap

$$\frac{r_{k-2}}{r_{k-1}} = q_k + \frac{r_k}{r_{k-1}}$$

$$\Downarrow$$

$$[r_{k-1} \;\; r_k] = [r_{k-2} \;\; r_{k-1}]V_k; \quad V_k = \begin{bmatrix} 0 & 1 \\ 1 & -q_k \end{bmatrix}$$

kunnen eenheden introduceren

$$\Downarrow$$

$$[s_k \;\; r_k] = [s_{k-1} \;\; r_{k-1}]V_k; \quad V_k = \begin{bmatrix} y_k & c_k \\ x_k & a_k \end{bmatrix}$$

$$a_k = -q_k c_k; \quad c_k, x_k \text{ eenheden}; \quad y_k = 0$$

$$\boxed{\text{UEA}} = \text{bewaar ook } V_0 V_1 \ldots V_k$$

$$G_{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ s & r \end{bmatrix}; \quad G_k = G_{-1} V_1 \ldots V_k = \begin{bmatrix} y_{0k} & c_{0k} \\ x_{0k} & a_{0k} \\ s_k & r_k \end{bmatrix}$$

LFT en Kettingbreuken

$$T_k(z) = \frac{c_k + y_k z}{a_k + x_k z}$$

$$z = x/y$$

$$T_k(x/y) = \frac{c_k y + y_k x}{a_k y + x_k x}$$

$$\begin{bmatrix} c_k y + y_k x \\ a_k y + x_k x \end{bmatrix} = \begin{bmatrix} y_k & c_k \\ x_k & a_k \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$$T_1 \circ T_2(z) = \frac{c_1 + y_1 \dfrac{c_2 + y_2 z}{a_2 + x_2 z}}{a_1 + x_1 \dfrac{c_2 + y_2 z}{a_2 + x_2 z}}$$

$$y_k = 0$$

$$T_1 \circ T_2(z) = \frac{c_1}{a_1 + x_1 \dfrac{c_2}{a_2 + x_2 z}} = \cfrac{c_1}{a_1} + \cfrac{x_1 c_2}{a_2} + \cfrac{x_2 z}{1}$$

LFT en Kettingbreuken (2)

Konvergenten

$$T_1 \circ \cdots \circ T_k(0) = \frac{c_1}{\lfloor a_1} + \frac{x_1 c_2}{\lfloor a_2} + \cdots + \frac{x_{k-1} c_k}{\lfloor a_k} = \frac{c_{0k}}{a_{0k}}$$

staart

$$z_0 = T_1 \circ \cdots \circ T_k(z_k) = \frac{c_1}{\lfloor a_1} + \frac{x_1 c_2}{\lfloor a_2} + \cdots + \frac{x_{k-1} c_k}{\lfloor a_k} + \frac{x_k z_k}{\lfloor 1}$$

$$z_k = -r_k / s_k$$

$$G_{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ s & r \end{bmatrix}; \quad G_k = G_{-1} \underbrace{V_1 \ldots V_k}_{V_{0k}} = \begin{bmatrix} x_{0k} & c_{0k} \\ y_{0k} & a_{0k} \\ s_k & r_k \end{bmatrix}$$

$[x_{0k} \quad c_{0k}]$ = op eenheden na $[u_{k-1} \quad u_k]$
$[y_{0k} \quad a_{0k}]$ = op eenheden na $[v_{k-1} \quad v_k]$

Het eindeloze verhaal

reële getallen

$$
\begin{aligned}
3.1415926\ldots &= 3 + \cfrac{1}{\cfrac{1}{0.1415926\ldots}} \\
&= 3 + \cfrac{1}{7.0625133\ldots} \\
&= 3 + \cfrac{1}{7 + \cfrac{1}{\cfrac{1}{0.0625133\ldots}}} \\
&= 3 + \cfrac{1}{7 + \cfrac{1}{15.9965\ldots}} \\
&= 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292.63459\ldots}}}}
\end{aligned}
$$

Bijvoorbeeld

$$
\begin{aligned}
e &= 2 + \cfrac{1}{1} + \cfrac{1}{2} + \cfrac{1}{1} + \cfrac{1}{4} + \\
&\quad \cfrac{1}{1} + \cfrac{1}{1} + \cfrac{1}{6} + \cfrac{1}{1} + \cfrac{1}{1} + \\
&\quad \cfrac{1}{8} + \cfrac{1}{1} + \cfrac{1}{1} + \cfrac{1}{10} + \cfrac{1}{1} + \cdots
\end{aligned}
$$

$$
\begin{aligned}
\pi &= 3 + \cfrac{1}{7} + \cfrac{1}{15} + \cfrac{1}{1} + \cfrac{1}{292} + \\
&\quad \cfrac{1}{1} + \cfrac{1}{1} + \cfrac{1}{1} + \cfrac{1}{2} + \cfrac{1}{1} + \\
&\quad \cfrac{1}{3} + \cfrac{1}{1} + \cfrac{1}{14} + \cfrac{1}{2} + \cfrac{1}{1} + \cfrac{1}{1} \cdots
\end{aligned}
$$

Het eindeloze verhaal (deel II)

Laurentreeksen $\mathbb{F}\langle z^{-1}\rangle$

$$f(z) \;=\; 3\cdot z^0 + 1\cdot z^{-1} + 4\cdot z^{-2} + 1\cdot z^{-3} + \cdots \in \mathbb{F}\langle z^{-1}\rangle$$

het vorige werkt ook met Laurentreeksen

$$f(z) \;=\; 3 + \cfrac{1}{z - 4 + \cfrac{1}{\cfrac{z^{-1} + 4z^{-2} + z^{-3} + 5z^{-4} + \cdots}{15z^{-2} - z^{-3} + 11z^{-4} + 9z^{-5} + \cdots}}}$$

"quotient" = polynoom deel

Laurentreeks $\mathbb{F}\langle z\rangle$

"quotient" = kritisch deel + cst term
(Arne Magnus P-fraction)

Benadering

Laurentreeks $\mathbb{F}\langle z^{-1}\rangle$

Afgebroken KB na k stappen geeft

$$-\frac{r_0}{s_0} = \underbrace{\frac{c_{0k}}{a_{0k}}}_{benadering} + \underbrace{\frac{r_k}{a_{0k}}}_{fout}$$

Als $f = -r_0/s_0$ geen veelterm-stuk heeft dan

$$\deg(f - \frac{c_{0k}}{a_{0k}}) = -2\alpha_{0k} - \alpha_{k+1}$$

$\deg a_k = \alpha_k$; $\quad \deg a_{0k} = \alpha_{0k} = \alpha_1 + \cdots + \alpha_k$

Minimale partiële realisatie (MPR) probleem
(Berlekamp-Massey) – (Gragg-Lindquist)

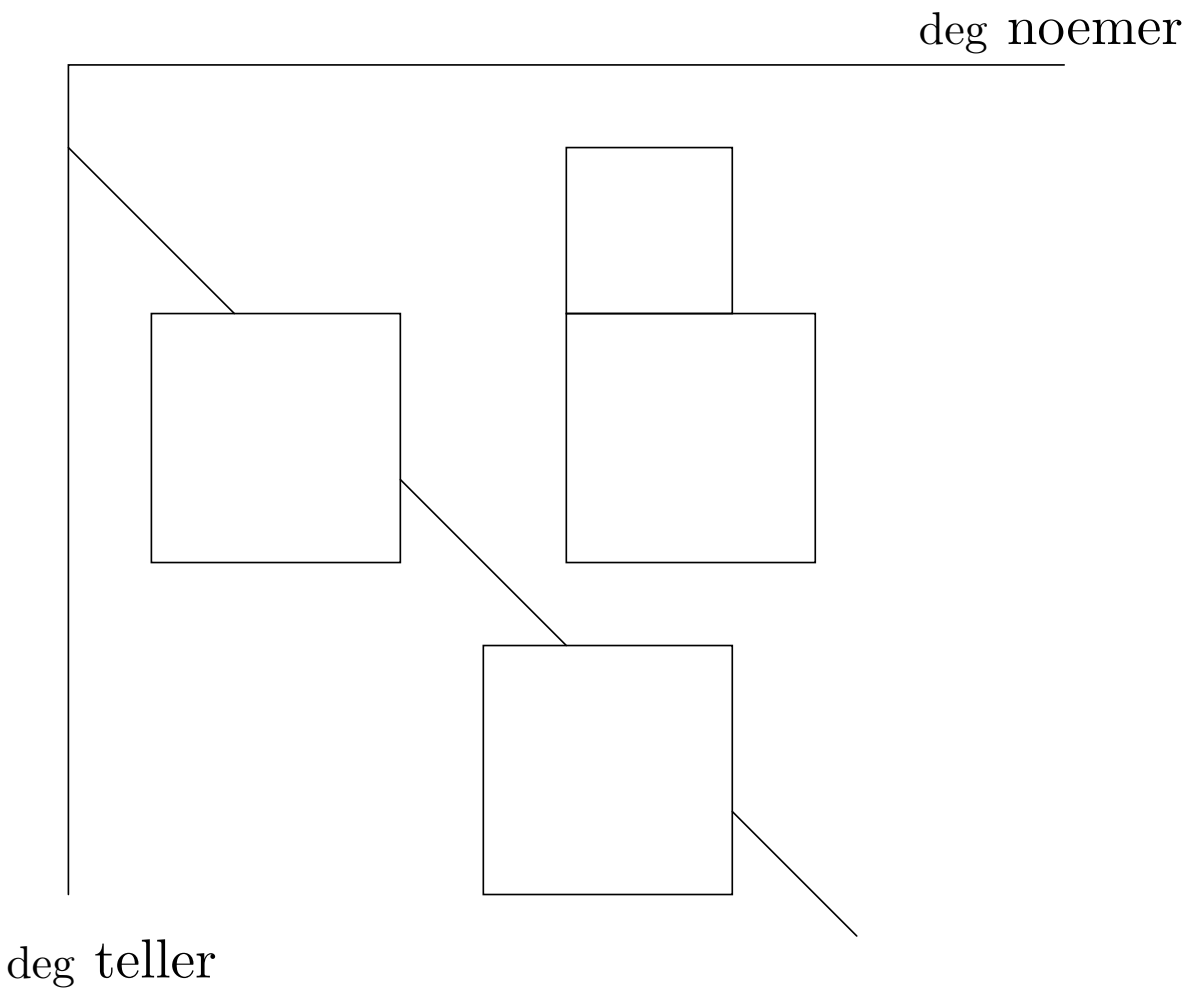
Voor formele machtreeksen $\mathbb{F}[[z]]$

Padé benadering
graad $\rightarrow$ orde
(MPR $\approx$ Padé op ∞)

EA "springt" over de blokken in de Padé tabel
en loopt langs de hoofd(sub)diagonaal

$\Rightarrow$ notie van minimale Padé benadering. (MPB)

Padé tabel



$$f(z)q(z) - p(z) = \mathcal{O}(z^{m+n+1})$$

$$\deg p(z) \leq m; \qquad \deg q(z) \leq n$$

Lineaire algebra

$$f(z) = \sum_{k=1}^{\infty} f_k z^{-k} \in \mathbb{F}\langle z^{-1} \rangle$$

Benadering

$$f(z)a_{0,k}(z) - c_{0,k}(z) = r_k(z) = \mathcal{O}(z^{-\alpha_{0,k+1}})$$

$$\alpha_{0,k+1} = \sum_{i=0}^{k+1} \alpha_i \ ; \quad \alpha_i = \deg a_i \quad \text{(quotiënten)}$$

Herformulering met Hankels

$$\begin{bmatrix} f_1 & f_2 & f_3 & \cdots \\ f_2 & f_3 & \cdots & \\ f_3 & \cdots & & \\ \vdots & & & \\ \vdots & & & \end{bmatrix} \begin{bmatrix} a_{0,k}^{(0)} \\ \vdots \\ a_{0,k}^{(\alpha_{0,k})} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \breve{r}_k \\ \vdots \end{bmatrix} \leftarrow \alpha_{0,k+1}$$

$$H\mathbf{a}_{0,k} = \mathbf{r}_k$$

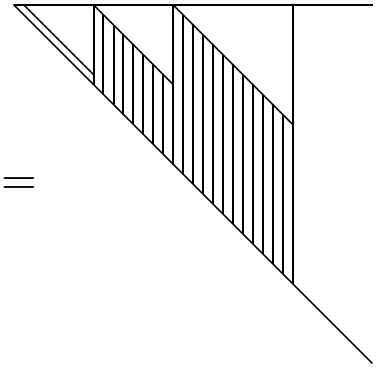
Kern struktuur van Hankel matrices

Blok triangulaire factorisatie

Z = neerschuif operator

$$Z^T H \mathbf{a}_{0k} = H[Z\mathbf{a}_{0,k}] = Z^T \mathbf{r}_k$$

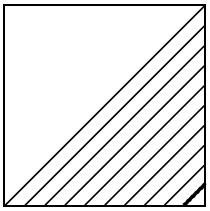
Organiseer in blokken

$A =$  $= [A_{\cdot,1}|A_{\cdot,1}|\ldots]$

$$A_{\cdot,k} = [\mathbf{a}_{0,k}|Z\mathbf{a}_{0,k}|Z^2\mathbf{a}_{0,k}|\ldots|Z^{\alpha_{k+1}-1}\mathbf{a}_{0,k}]$$

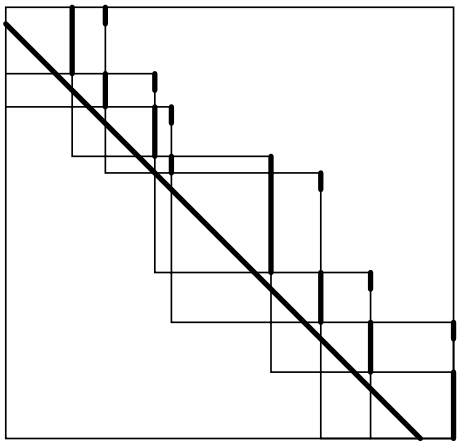
Blok triangulaire factorisatie

$$\boxed{A^T H A = \mathrm{diag}(D_{0,0}, D_{1,1}, D_{2,2}, \ldots)}$$

$D_{k,k} =$  $\alpha_{k+1} \times \alpha_{k+1}$

$\alpha_{0,k}$ = Kronecker indices
α_k = Euclidische indices
Leidende subHankels H_α niet-singular voor $\alpha = \alpha_{0,k}$'s

Recursie

$T_n =$ 

$$ZA = AT$$

eindig geval: $F(a_{0,n+1})A_n = A_n T_n$

$$\det A_n = 1 \Rightarrow a_{0,n+1} = \det(zI - T_n)$$

$$F(a_{0,n+1} = \left[\begin{array}{ccc|c} 0 & \dots & 0 & \\ 1 & & & \\ & \ddots & & -\underline{a}_{0,n+1} \\ & & 1 \quad 0 & \end{array}\right]$$

Blok orthogonale veeltermen

Voor eindige sectie van Hankel:

$$F(a_{0,k+1})A_k = A_k T_k$$

$$T_k = \begin{bmatrix} T_{0,0} & T_{0,1} & & & \\ T_{1,0} & T_{1,1} & \ddots & & \\ & \ddots & \ddots & & \\ & & & & T_{k-1,k} \\ & & & T_{k,k-1} & T_{k,k} \end{bmatrix} \quad \text{(blok Jacobi)}$$

$$\Downarrow$$

Blok 3-term recursie voor formele orthogonale veeltermen
(Brezinski – Draux)
$A^T H A = D$ geeft blok orthogonaliteit
H is momenten matrix
$ZA = AT$ geeft blok 3-term recursie

Euclidisch algoritme = vlugge Gram-Schmidt voor indefinite metriek

There is more ...

Verschoven orthogonale veeltermen
verbonden met verschoven momenten
verschoven diagonaal in de Padé tabel
Beschouw momenten matrix $H(zf)$ in plaats van $H(f)$

$$A^T H(zf) A = DT$$

(D blok diagonaal, T blok tridiagonaal)

$$\Downarrow$$

$$D_\nu T_\nu = \left[\begin{array}{cc|ccc|cccc} \times & \times & & & & & & & \\ \times & \times & & & \times & & & & \\ \hline & & 0 & \times & \times & & & & \\ & & \times & \times & \times & & & & \\ & \times & \times & \times & \times & & & & \times \\ \hline & & & & & 0 & 0 & \times & \times \\ & & & & & 0 & \times & \times & \times \\ & & & & & \times & \times & \times & \times \\ & & & & \times & \times & \times & \times & \times \end{array}\right]$$

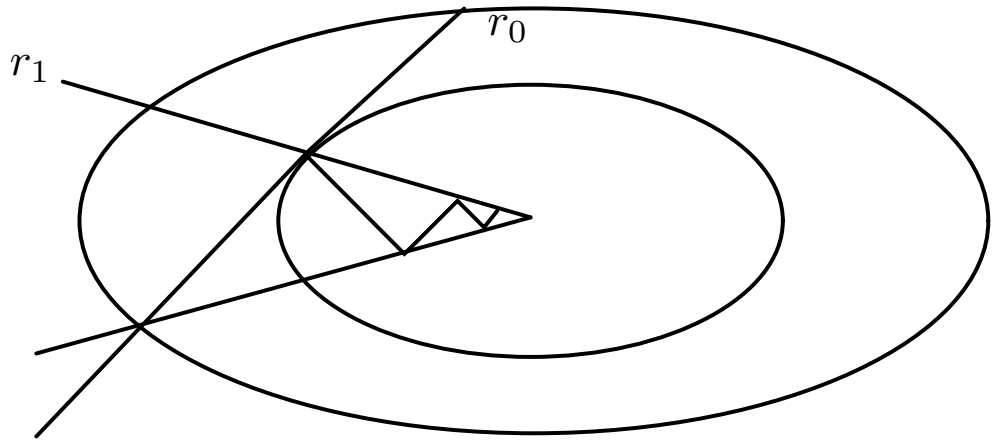
($\alpha_1 = 2, \quad \alpha_2 = 3, \quad \alpha_3 = 4$)
is weer blok tridiagonaal!

Iteratief oplossen van stelsels

$$Mx = b$$

$$\min \|b - Mx\| = \min \|r\|_{M^{-1}}; \quad M = M^H, M > 0$$

Toegevoegde gradiënt $\leftrightarrow$ steilste afdaling
(Hestenes–Stiefel)



zoekriching $= r_k = b - Mx_k =$ gradiënt
zigzaggen = eindigt niet in eindig veel stappen
maak ze toegevoegd!

$$r_k^H M r_j = \delta_{kj} \|r_k\|^2$$

$$x_k = x_{k-1} + m_k r_{k-1}$$
$$\Rightarrow$$
$$r_k = b - Mx_k = r_{k-1} - m_k M r_{k-1}$$
$$\Rightarrow x_k \in x_0 + \text{span}\{r_0, Mr_0, M^2 r_0, \ldots\}$$
$$\Rightarrow r_k \in \text{span}\{r_0, Mr_0, M^2 r_0, \ldots\}$$

Krylov ruimte (the final frontier)

$$r_k = b - Mx_k \in \mathcal{K}_n(r_0, M) = \text{span}\{r_0, Mr_0, \ldots, M^n r_0\}$$

$$\text{Dus } r_k = p_k(M) r_0$$

$$\boxed{\text{Stel } M \text{ symmetrisch}}$$

$$X_k = [x_0 | x_1 | \ldots | x_k], \qquad x_i = M^i r_0$$

$$p_k(z) = p_{ok} + p_{1k} z + \cdots + p_{kk} z^k; \quad P_k = [p_{0k}\ p_{1k}\ \cdots\ p_{kk}]^T$$

$$r_k = X_k P_k$$

$$\|r_k\|^2 = r_k^T r_k = P_k^T X_k^T X_k P_k = P_k^T H P_k = \|P_k\|_H$$

$$H = H(f), \quad f = \sum f_k z^{-k}, \quad f_k = r_0^H M^{k+1} r_0$$

$$\min \|r_k\|^2 \Leftrightarrow \min \|P_k\|_H^2$$

$$\text{minimale norm} \Leftrightarrow P_k \perp P_l, \quad k \neq l$$

$$\text{Construeer OV voor Hankel} \equiv \text{supra}$$

$$\text{Dan zijn de } P_k(z) = a_{0k}(z)$$

$$X_k A_k = \hat{X}_k \quad \text{(QR ontbinding)}$$

$$\text{en}$$

$$\hat{X}_k^T \hat{X}_k = D_k \text{ (diag)} \quad \text{en} \quad \hat{X}_k^T M \hat{X}_k = J_k \text{ (tridiag)}$$

wat als $M \neq M^T$ and $M \not> 0$?

Vrie aksidenten?

$X_n^H X_n$ niet Hankel $\Rightarrow$ "lange" recursie
volledige Gram-Schmidt $\rightarrow$ Arnoldi
GMRES (Saad, 1986)

Waarom niet Hankel?

$r_i^T r_j = r_0^T (M^T)^i M^j r_0 \Rightarrow$ hebben 2 Krylov rijen nodig

$$\mathcal{K}_n(x_0, M) \text{ and } \mathcal{K}_n(y_0, M^T)$$

$X_n = [x_0|x_1|\ldots|x_n]$ and $Y_n = [y_0|y_1|\ldots|y_n]$
weer Hankel (joepie!)

$$Y_n^T X_n = H(f); \quad f_{i+j+1} = y_0^T M^i M^j x_0$$

Construeer

$$X_n \rightarrow \hat{X}_n = [\hat{x}_0|\ldots|\hat{x}_n] \text{ and } Y_n \rightarrow \hat{Y}_n = [\hat{y}_0|\ldots|\hat{y}_n]$$

$$\hat{Y}_n^T \hat{X}_n = D_n \text{ (diag)}$$

$$\hat{Y}_n^T M \hat{X}_n = J_n \text{ (tridiag)}$$

bi-orthogonalisatie $\Rightarrow$ BCG (Lanczos, 1950,1952)

tweezijdige Gram-Schmidt + Krylov = Lanczos

Noteer M and J_n gelijkvormig $\Rightarrow \lambda(M) = \lambda(J_n)$
We kunnen dus ook eigenwaardeproblemen oplossen!!

Grotere aksidenten (deel 2)

wat als $M \neq M^T$ en $M \not> 0$?

Moment matrix $H(f)$ heefts (bijna) singuliere submatrices

(bijna) brokken (deling door nul)

Deus ex machina: Euclid ... (ca 295 BC)
(back to the future)

$$Y_n^T X_n = H(f) \qquad Y_n^T M X_n = H(zf)$$

$$\hat{X}_n = X_n A_n \qquad \hat{Y}_n = Y_n A_n$$

$$\hat{x}_k = a_{0,k}(M) x_0 \qquad \hat{y}_k = [a_{0,k}(M)]^T y_0$$

$$\hat{Y}_n^H \hat{X}_n = D_n \qquad \hat{Y}_n^H M \hat{X}_n = D_n T_n$$

blok versies!

Look Ahead Lanczos (LAL) (Parlett-Taylor, 1985)
Quasi Minimal Residuals (QMR) (Freund-Nachtigal, 1991)
Method of Recursive Zoom (MRZ) (Brezinski-M. Redivo Zaglia, 1991)

Lineair systeemtheorie

$$\text{systeem} \quad \begin{array}{ll} x_{k+1} = Ax_k + Bu_k, & A \in \mathbb{F}^{n\times n}, B \in \mathbb{F}^{n\times 1} \\ y_{k+1} = C^T x_k, & C \in \mathbb{F}^{n\times 1} \end{array}$$

toestandsruimte realizatie (A, B, C)

minimale realisatie $= n$ is minimaal

transfer funktie $f(z) = C^T(zI - A)^{-1}B$

obsereerbaarheids matrix $\mathcal{O} = [C \ A^TC \ (A^T)^2C \ \ldots]^T$

controleerbaarheids matrix $\mathcal{R} = [B \ AB \ A^2B \ \ldots]$

observeerbaar $n = \operatorname{rank}\mathcal{O}$, controleerbaar $n = \operatorname{rank}\mathcal{R}$

$H = H(f) = \mathcal{O}\mathcal{R}$, $\deg f(z) = \operatorname{rank} H$

Eigenwaarde problemen

Hier $f(z) = y_0^T (zI - M)^{-1} x_0$

realisatie (M, x_0, y_0)

niet noodzakelijk minimaal!

afmeting $M = n$
$r_O = \text{rang } \mathcal{O} = \dim \mathcal{K}_\infty(y_0, M^T)$
$r_R = \text{rang } \mathcal{R} = \dim \mathcal{K}_\infty(x_0, M)$
$r = \deg f = \text{rang } H = \text{rang } \mathcal{O}\mathcal{R} \leq \min\{r_O, r_R\}$

Spectrale info enkel van f

Bij exacte benadering van f : $\alpha_{0,n+1} = \deg f < n$

nulpunten van $a_{0,n+1}(z)$ in spectrum van M

$n > r = \min\{r_O, r_R\}$	controleerbaar of observeerbaar vinden spectrum van M beperkt tot $\mathcal{K}_\infty(y_0, M^T)$ or $\mathcal{K}_\infty(x_0, M)$
$r < \min\{r_O, r_R\}$	x_0 en/of y_0 zijn slecht gekozen geen componenten volgens max Jordan blokken vinden spectrum van M beperkt tot deelruimte.

Foutenverbeterende Codes

Symbolen

$$F_q = \{0, 1, \ldots, q-1\} \quad \text{eindig veld}$$

Woorden

$$V_n(F_q) = \{(\alpha_0, \ldots, \alpha_{n-1}); \alpha_i \in F_q\}$$

een (n, k)-code is gedefinieerd door een stel codewoorden C

$$C \subset V_n(F_q); \quad \dim C = k$$

Voor Goppa Code definieer C als

$$G \text{ generator veelt. over } GF(q^m); \quad \deg G = s$$

$$\{a_0, \ldots, a_{n-1}\} \subset GF(q^m) \text{ en } G(a_i) \neq 0$$

$$(\alpha_0, \ldots, \alpha_{n-1}) \in C \Leftrightarrow S(x) = \sum_{i=0}^{n-1} \frac{\alpha_i}{x - a_i} \equiv 0 (\mathbf{mod}\, G(x))$$

$S(x)$ is syndroom

$$\text{BCH} : q = 2;\ n = 2^m - 1;\ G(x) = x^{2t}$$

$$\text{Reed-Solomon} : n = q^m - 1;\ G(x) = \prod_{k=1}^{2t} (x - \alpha^k)$$

Codes en Euclides

zenden $c = (c_0, \ldots, c_{n-1})$
ontvangen $r = (r_0, \ldots, r_{n-1})$
fout $e = r - c = (e_0, \ldots, e_{n-1})$
syndroom

$$S(x) = \sum_{i=0}^{n-1} \frac{r_i}{x - a_i} \ (\mathbf{mod}\, G) = \sum_{i=0}^{n-1} \frac{e_i}{x - a_i} \ (\mathbf{mod}\, G)$$

$$E = \{a_i : e_i \neq 0\}$$

$$\text{plaats fout: } \pi(x) = \prod_{\beta \in E} (x - \beta)$$

$$\text{grootte fout: } \omega(x) \text{ interpoleert } \omega(a_i) = e_i, \ \ \forall a_i \in E$$

$$\pi(x)S(x) = \omega(x) \ (\mathbf{mod}\, G(x))$$

$$(G, S) \rightarrow (\pi, \omega)$$

$$G_{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ G & S \end{bmatrix}; \quad G_k = G_{-1} V_1 \ldots V_k = \begin{bmatrix} x_{0k} & c_{0k} \\ \pi(x) & a_{0k} \\ \omega(x) & r_k \end{bmatrix}$$