Het Euclidisch algoritme: varianten en toepassingen*

Adhemar Bultheel en Marc Van Barel

laatste versie bij MVB

Samenvatting

Uitgaande van het oorspronkelijk algoritme van Euclides geven we aan hoe dezelfde recursiebetrekking te herkennen is in het algoritme van Chebyshev voor het opstellen van kettingbreukontwikkelingen, in de recursie voor formele orthogonale veeltermen, in het Lanczos algoritme voor het iteratief oplossen van stelsels lineaire vergelijkingen en eigenwaardeproblemen, in het Berlekamp-Massey algoritme voor minimale partiële realisatie, in algoritmen voor foutenverbeterende codes, in de stabiliteitsanalyse van veeltermen en in snelle algoritmen voor Hankel matrices.

Voor Prof. ir. Ludo Buyst, in dankbaarheid en bewondering.

1 Het Euclidisch algoritme

Het algoritme van Euclides (EA) is door de meesten waarschijnlijk gekend als een rekenschema om de grootste gemene deler (ggd) te berekenen van twee natuurlijke getallen. Het is één van de oudste niet-triviale algoritmen, en het is de bedoeling van deze tekst om aan te tonen dat het, in één of andere vorm of veralgemening, terug te vinden is als de basis voor heel wat moderne toepassingen en algoritmen.

De eigenschappen waarop het algoritme steunt staan geformuleerd als stelling 1 en 2 van boek 7 van de *Elementen* [47, p. 115-128], die dateren van ongeveer 300 jaar v. Chr. Volgens sommige bronnen was het algoritme ook gekend door andere Griekse wiskundigen [16, p.6] en kan men zelfs al bij de Babyloniërs sporen terugvinden [3, p.27].

De behandeling door Euclides (zoals met veel wiskunde van die tijd) was zeer meetkundig. We zouden het door hem gestelde probleem als volgt kunnen omschrijven. Gegeven twee lijnstukken L_0 en L_1, waarvan verondersteld wordt dat de lengtes gehele veelvouden zijn van een ondeelbare eenheid. Hoe construeert

*Dit onderzoek werd gesteund door het NFWO project Lanczos, contract #2.0042.93

men een (zo groot mogelijke) gemeenschappelijke maatstaf voor deze lijnstukken? Dat laatste betekent een lijnstuk zodanig dat zowel L_0 als L_1 een geheel veelvoud is van de gemeenschappelijke maat. De oplossing gebeurt door de volgende constructie: Stel dat L_0 het langste lijnstuk is van de twee. Men legt dan L_1 langs L_0 en knipt van L_0 een stuk weg met de lengte van L_1. Indien het resterende stuk van L_0 nog groter is dan L_1 herhaalt men dit, enzovoort tot men uiteindelijk een stuk overhoudt dat kleiner is dan L_1. Noem die rest L_2. Dan herbegint men de hele procedure door L_2 (het kleinste) een aantal keer van L_1 (het grootste) af te trekken. Op die manier zal men dus in elke stap het kleinere lijnstuk van het grotere aftrekken. Volgens Euclides zal men steeds eindigen met een lijnstuk dat men een geheel aantal keer van het vorige kan aftrekken. Dit kan in twee gevallen: ofwel is dit voor een lijnstuk met lengte 1, en dan is dit triviaal vermits elk lijnstuk als een veelvoud van de eenheid wordt beschouwd (stelling 1) ofwel vindt men een "echte" gemeenschappelijke maat groter dan 1 (stelling 2). Wij zouden zeggen dat het eerste geval overeenstemt met het geval van onderling ondeelbare lengtes en in het tweede geval is er een niet-triviale ggd. Als men niet a priori veronderstelt dat er voor de lengtes van de lijnstukken zo een ondeelbare eenheid bestaat, dan is er in feite een derde mogelijkheid: indien de lengtes van de lijnstukken zich niet verhouden als rationale getallen, dan zal de constructie nooit eindigen en is er geen gemeenschappelijke maat, maar dit geval wordt door Euclides niet behandeld.

We kunnen dit algoritme herformuleren in termen van gehele getallen en de opeenvolgende aftrekkingen samenvatten in een (gehele) deling. Bijvoorbeeld om $\text{ggd}(8,6)$ te vinden merken we dat 6 één keer van 8 kan afgetrokken worden en er rest 2. Dit noteren we als $8/6{=}1{+}2/6$ of $8 \bmod 6 = 2$. Nadien zien we dat de 2 drie keer kan afgetrokken worden van 6 en er rest 0, wat samengevat wordt in $6/2 = 3 + 0/2$ of $6 \bmod 2 = 0$, dus $\text{ggd}(8,6) = 2$. We krijgen dus het volgende algoritme:

EA : $\text{ggd}(s,r)$
$r_{-1} = s, r_0 = r$
$k = 1$
zolang $r_{k-1} \neq 0$
  $r_k = r_{k-2} \bmod r_{k-1}$
  $k = k + 1$
einde
$\text{ggd}(s,r) = r_{k-2}$

De formulering van dit algoritme werkt ook voor veeltermen. Bijvoorbeeld als $r = z^4 - z^3 - z^2 + 3z - 2$ en $s = z^3 + z^2 - z - 1$, dan vinden we opeenvolgend

$$\begin{aligned} r_1 &= r_{-1} \bmod r_0 = 2z^2 + 2z + 4 \\ r_2 &= r_0 \bmod r_1 = z - 1 \\ r_3 &= r_1 \bmod r_2 = 0. \end{aligned}$$

waaruit men kan besluiten dat $\text{ggd}(s, r) = z - 1$. In feite kan men het algoritme toepassen in een willekeurige ring waar men een zinvolle betekenis kan geven aan de mod-bewerking. Men noemt zoiets een Euclidisch domein. Dit is een integriteitsdomein, dat is een commutatieve ring D zonder nuldelers [33] zodanig dat men voor elk stel $a, b \in D$ met $b \neq 0$ een quotiënt q en een rest r kan vinden zodat $a = bq + r$. Bovendien moet de rest r "kleiner" zijn dan deler b. Dit laatste meet men met een valuatie: $\partial(r) < \partial(b)$. Een valuatie is een afbeelding $\partial : D \to \mathbb{N}$ zodanig dat $\partial(a) = 0$ enkel en alleen als $a = 0$ en zodat $\partial(ab) \geq \partial(a)$ voor alle $a, b \neq 0$. Als voorbeeld kan men voor D de verzameling der gehele getallen $\mathbb{Z}$ nemen met als valuatie $\partial(a) = |a|$. Voor de veeltermen in z over een veld $\mathbb{F}$, namelijk $D = \mathbb{F}[z]$, kan men als valuatie $\partial(a) = 2^{\text{gr}(a)}$ nemen waarin $\text{gr}(a)$ de graad van a voorstelt en we bij conventie $\text{gr}(0) = -\infty$ stellen.

Net zoals bij Euclides zal een ggd voor $r, s \in D$ steeds bestaan. Inderdaad zal tijdens het algoritme $\partial(r_k)$ monotoon dalend zijn in de verzameling $\mathbb{N}$. Daarom zal men steeds met $\partial(r_n) = 0$ eindigen en dan volgt uit de stellingen van Euclides dat $r_{n-1} = \text{ggd}(s, r)$.

Een ggd hoeft echter niet uniek te zijn. In $\mathbb{Z}$ is de ggd slechts bepaald op het teken na. In $\mathbb{F}[z]$ is hij eenduidig op een constant veelvoud ($\neq 0$) na. In het algemeen is de ggd slechts bepaald op een eenheid na. Een eenheid van D is een inverteerbaar element van D. In $\mathbb{Z}$ zijn de enige eenheden ± 1 en in $\mathbb{F}[z]$ zijn de eenheden alle constante veeltermen verschillend van 0, dus $\mathbb{F} \setminus \{0\}$. Dus als we over *de* ggd willen spreken moeten we eigenlijk werken in de verzameling der equivalentieklassen van elementen in D die slechts door een factor verschillen die een eenheid is. Dikwijls kiest men in deze klasse een vertegenwoordiger met een bepaalde normalisatie en noemt men die vertegenwoordiger *de* ggd. Bijvoorbeeld in $\mathbb{Z}$ kan men steeds de positieve ggd nemen en in $\mathbb{F}[z]$ steeds de monische ggd.

Een Euclidisch domein is niet de meest algemene structuur waarin men het Euclidisch algoritme kan toepassen. We zullen verder een rationaal approximatieveld definiëren waarin we toelaten dat het EA niet eindigt. Men zou ook kunnen werken in de veronderstelling dat de vermenigvuldiging niet commutatief is. In dat geval moet men spreken over een linkse en een rechtse ggd. Dit is bijvoorbeeld nodig als men met matrixveeltermen wil werken. Zie [82, 119]. Sommige toepassingen vereisen meerdimensionale versies van het EA. Zie bijvoorbeeld [14]. Op deze veralgemeningen zullen we in deze tekst niet verder ingaan.

2 Kettingbreuken

Men kan eenvoudig alle berekeningen van het EA volgen in de opstelling van een (afbrekende) kettingbreuk. Bijvoorbeeld

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

of in het voorbeeld met de veeltermen

$$\frac{r_{-1}}{r_0} \;=\; z-2+\frac{r_1}{r_0} = z-2+\frac{1}{\frac{r_0}{r_1}} = \cdots = z-2+\cfrac{1}{\frac{1}{2}z+\cfrac{1}{2z+4+\cfrac{0}{z-1}}}.$$

Dit steunt op het herhaald toepassen van

$$\frac{s_{k-1}}{r_{k-1}} = q_k + \frac{r_k}{s_k} \quad \text{met} \quad s_k = r_{k-1}$$

of nog

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

Als we gebruik maken van het feit dat we in elke stap van het algoritme met een eenheid kunnen vermenigvuldigen, dan kunnen we V_k in elke stap vervangen door

$$V_k = \begin{bmatrix} 0 & 1 \\ 1 & -q_k \end{bmatrix} \begin{bmatrix} x_k & 0 \\ 0 & c_k \end{bmatrix} = \begin{bmatrix} y_k & c_k \\ x_k & a_k \end{bmatrix}$$

met $a_k = -q_k c_k$, $y_k = 0$, q_k is het quotiënt van s_{k-1}/r_{k-1} en x_k en c_k zijn willekeurige eenheden. Deze laatste zouden we kunnen gebruiken om in elke stap van het algoritme een zekere normalisatie voor het koppel (s_k, r_k) te bekomen. Om met dezelfde normalisatie te kunnen starten heeft men ook een V_0 nodig waarin y_0 en a_0 eenheden zijn en $x_0 = c_0 = 0$. Men kan zo de juiste normalisatie voor $[s_0 \;\; r_0] = [s \;\; r]V_0$ verkrijgen. Met deze normalisaties krijgt men een kettingbreuk van de vorm

$$-\frac{r}{s} = \frac{y_0}{a_0}\left(\left\lfloor\frac{c_1}{a_1}\right\rfloor + x_1\left\lfloor\frac{c_2}{a_2}\right\rfloor + \cdots + x_{k-1}\left\lfloor\frac{c_k}{a_k}\right\rfloor - x_k\left\lfloor\frac{r_k}{s_k}\right\rfloor\right).$$

Door deze kettingbreuk af te breken na de $k$de term krijgt men een benadering c_{0k}/a_{0k} voor $f = -r/s$ waarbij vanwege de voorwaartse recursiebetrekking voor kettingbreuken [37, p. 508]

$$G_k = G_{-1}\underbrace{V_0 V_1 \ldots V_k}_{V_{0k}} = \begin{bmatrix} y_{0k} & c_{0k} \\ x_{0k} & a_{0k} \\ s_k & r_k \end{bmatrix}; \quad G_{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ s & r \end{bmatrix}.$$

Hieruit kan men een aantal eigenschappen halen. Bijvoorbeeld door het nemen van determinanten ziet men dat de determinanten $\det V_k$ eenheden zijn (in het geval van veeltermmatrices noemt men dit unimodulaire matrices) en dit impliceert dat deze matrices inverteerbaar zijn in D, dus ook V_{0k} is inverteerbaar en er volgt ook dat $\text{ggd}(y_{0k}, c_{0k}) = \text{ggd}(x_{0k}, a_{0k}) = 1$.

Uit de laatste lijn van de formule volgt verder dat als $r_n = sc_{0n} + ra_{0n} = 0$ dan $s_n = sy_{0n} + rx_{0n} = \text{ggd}(s, r)$. Dus $\text{ggd}(s, r)$ is te schrijven als een lineaire combinatie van s en r. De optredende cofactoren zijn precies y_{0n} en x_{0n}.

Men kan met deze elementen een eenvoudig bewijs geven van het EA, zelfs in een heel algemene vorm. Dit bewijs steunt erop dat een unimodulaire transformatie de ggd behoudt. Vermits het EA slechts unimodulaire transformaties uitvoert, wordt de ggd in elke stap behouden. Bijvoorbeeld in het geval van matrixveeltermen is g een linkse ggd van s en r indien er een unimodulaire matrix V_{0n} bestaat zodat $[s \;\; r]V_{0n} = [g \;\; 0]$. Het EA is in feite een ontbinding in elementaire unimodulaire factoren van de matrix V_{0n} (als een soort Gauss-eliminatie [35, p. 82-86]) die als doel hebben de r tot 0 te herleiden [82, 119]. Merk op dat het bewijs ook werkt as r en s matrixveeltermen zijn met eenzelfde aantal rijen maar met een verschillend aantal kolommen.

3 Het uitgebreide Euclidisch algoritme

Het EA berekende van de recursie voor de matrix G_k in feite slechts de laatste lijn, dus de staart van de kettingbreuk. In het uitgebreide Euclidisch algoritme (UEA) wordt ook de informatie V_{0k} opgebouwd en de ganse G_k matrix aangepast. Er zijn meerdere redenen waarom het UEA interessanter is dan het EA.

- *Rationale benadering:* Zoals gezegd levert de afgebroken kettingbreuk een benadering waar we later (§ 5) op terugkomen.
- *Differentievergelijking:* De rijen van de matrix V_{0k} vormen ook een fundamenteel stel voor de oplossing van deze eerste orde vectorrecursiebetrekking $X_k = X_{k-1}V_k$. Een combinatie van de voor- en achterwaartse recursie betrekkingen leveren dan een numeriek stabiele manier om een niet dominante oplossing van de recursiebetrekking te berekenen. Door een veralgemening naar matrix-kettingbreuken kunnen ook hogere-orde recursiebetrekkingen behandeld worden [91, 93, 90, 92].
- *Diophantische vergelijking:* Dat is een vergelijking van de vorm $sy + rx = t$ voor gegeven r, s en t met de beperking dat $\text{ggd}(x, y) = 1$. Een dergelijke vergelijking heeft een oplossing als en slechts als $t = cg$ met c een eenheid en $g = \text{ggd}(s, r)$ en alle oplossingen worden dan gegeven door $[x \;\; y] = [c \;\; d]V_{0n}^T$ waarbij V_{0n} een unimodulaire matrix is zodanig dat $[s \;\; r]V_{0n} = [s_n \;\; r_n] = [g \;\; 0]$.
- *Partieelbreuksplitsing:* Het vorige probleem heeft op zijn beurt toepassingen bij het berekenen van partieelbreuksplitsingen [34, p. L30]. Stel dat $rx + sy = t$, dan is $x/s + y/r = t/(rs)$. Dus als r, s en t gekend zijn, dan kan men door een diophantische vergelijking op te lossen ook een partieelbreuksplitsing vinden. Vandaar dat het UEA zijn nut heeft in allerlei getaltheoretische toepassingen maar ook in algebraïsche software systemen of in pakketten waar "exact" gerekend wordt door getallen in hun rationale vorm voor te stellen enz. [66].
- *Snelle algoritmen:* Bovendien is het UEA ook een handig middel om via een verdeel-en-heers techniek in combinatie met FFT te komen tot een snelle,

d.w.z., een $O(n \log^2 n)$, implementatie van het EA [86, 2, 13].

- *Foutenverbeterende codes:* Voor toepassing in Goppa codes is het ook belangrijk elementen uit het UEA te gebruiken (zie § 4).
- *Inverse verstrooiing:* Deze invalshoek is geïnspireerd door analoge methodes voor Toeplitz matrices zoals het Levinson en Schur algoritme [30]. In dit soort problemen wordt ook in een matrix V_{0k} informatie opgebouwd over het verstrooiingsmedium. Het medium wordt opgedeeld in verschillende lagen (hoe meer lagen hoe nauwkeuriger). Het EA berekent de verstrooiing van het resterende deel van het medium nadat de eerste lagen er zijn "afgepeld", zoiets als het economiseren van machtreeksen [36, p. 164]. Kailath en zijn medewerkers noemen dit "layer peeling" (LP) methodes [23, 43]. Als men enkel de V_{0k} matrix opbouwt (zonder de r_k en s_k) berekent men een model voor het effect van de afgepelde lagen. In dit geval spreekt men over een "layer adjoining" (LA) methode. In het UEA is alle informatie aanwezig en kan men de berekening van de recursiematrix V_k baseren op een LP of op een LA principe of zelfs op een combinatie van beiden [124].

Het ontbreekt ons aan de plaats om op deze, en nog vele andere toepassingen uitgebreid in te gaan. In de volgende paragrafen zullen we ons daarom beperken tot het invoeren van terminologie in een aantal diverse gebieden waardoor we een idee kunnen geven over hoe er het EA of UEA bij het berekenen van de oplossing, in één of andere vorm gebruikt wordt.

4 Foutenverbeterende codes

Een zeer mooie toepassing van het eeuwenoude EA op hedendaagse digitale codering van een signaal op een CD krijgt gestalte in de volgende theorie. We kunnen het probleem en de oplossing kort schetsen als volgt. Voor meer details kan men [98] raadplegen. Veralgemeningen kan men vinden in [49, 50].

Stel dat we beschikken over een verzameling van q symbolen (die we hier zonder beperking als natuurlijke getallen noteren) $F_q = \{0, 1, \ldots, q-1\}$. Stel dat F_q een (eindig) veld is. Met deze symbolen kunnen we woorden vormen. Dit is een n-tal van symbolen. De verzameling woorden noteren we als $V_n(F_q) = \{(c_0, \ldots, c_{n-1}) : c_i \in F_q\}$. Dit is een vectorruimte van dimensie n over het veld F_q. Hiervoor wordt een (n, k)-code gedefinieerd met behulp van een deelruimte $C \subset V_n(F_q)$ van dimensie $k < n$. De elementen van C noemt men codewoorden. Enkel de codewoorden worden als geldige boodschappen beschouwd. Stel nu dat men een codewoord $c = (c_0, \ldots, c_{n-1})$ verstuurt maar dat door verstoringen de boodschap $r = (r_0, \ldots, r_{n-1})$ ontvangen wordt. Er is dus een fout $e = c - r = (e_0, \ldots, e_{n-1})$ ontstaan die men zal moeten ontdekken en indien mogelijk ook verbeteren.

Voor Goppacodes [68] kiest men een aantal elementen $\{a_0, \ldots, a_{n-1}\}$ in het uitbreidingsveld F_{q^m} en beschrijft men C door een Goppaveelterm (niet te ver-

warren met de generatorveelterm) $G(x) \in F_{q^m}[x]$ zodanig dat $G(a_i) \neq 0$, $i = 0, \ldots, n-1$. Voor een element $r = (r_0, \ldots, r_{n-1}) \in V_n(F_q)$ definieert men een syndroom $S_r(x) = [\sum_{i=0}^{n-1} r_i/(x - a_i)](\mathbf{mod}(G(x))$. Merk op dat het syndroom hier als een rationale functie is gedefinieerd maar dat dit in het veld F_{q^m} altijd te herschrijven is als een veelterm. De verzameling codewoorden wordt dan beschreven door de voorwaarde $c \in C \Leftrightarrow S_c(x) = 0$.

Een bekend voorbeeld van Goppacodes is de Bose-Chaudhuri-Hocquenghem (BCH) code [12, 11, 80, 98] waarbij $q = 2$ (binaire code), $n = 2^m - 1$ en $G(x) = x^{2k}$ en voor a_i neemt men de n elementen van F_{2^m}, meestal geschreven als $a_i = \alpha^i$ met α een primitieve wortel van F_{2^m}. Het is dan mogelijk om k fouten te verbeteren. Een ander voorbeeld is de Reed-Solomon code [103] waarbij de symbolen uit een groter veld F_{q^m} genomen worden, $n = q^m - 1$. De Goppaveelterm is $G(x) = x^{2k}$ en de $a_i = \alpha^{-i}$ met α een primitieve wortel van F_{q^m}.

Voor dergelijke Goppacodes geldt dat het codewoord uit het syndroom wordt weggefilterd: $S_r(x) = S_e(x)$. Om de fout te kunnen verbeteren moet men de plaats en de waarde van de fout kennen. De plaats wordt gegeven door de foutlocatieveelterm. Dat is de veelterm $\pi(x) = \prod_{i \in E}(x - a_i)$ waarbij $E = \{i : e_i \neq 0\}$. De grootte van de fout vindt men door een foutevaluatorveelterm op te stellen $\omega(x) = \sum_{i \in E} e_i \pi_i(x)$ met $\pi_i(x) = \pi(x)/(x - a_i)$. Het is niet moeilijk in te zien dat $e_i = \omega(a_i)/\pi'(a_i)$ voor $i \in E$ (het accent duidt op de formele afgeleide). Het is hiermee duidelijk dat, als men $\pi(x)$ gevonden heeft, men via zijn nulpunten ook weet waar de fouten gebeurd zijn. Als men daarnaast ook $\omega(x)$ heeft, dan kent men bovendien de waarde van de fout. De foutlocatieveelterm kan men vinden met het Berlekamp-Massey algoritme [9, 97], en de foutevaluatorveelterm bepaalt men met het Forney algoritme [52] om de sleutelvergelijking $\pi(x)S(x) = \omega(x)(\mathbf{mod}\, G(x))$ op te lossen. Als men beiden combineert krijgt men het UEA want als men dit algoritme toepast met als gegevens $s = G$, de Goppaveelterm en $r = S$, het syndroom, en men voert k stappen uit met k zodanig dat $\mathrm{gr}(r_k) < [\mathrm{gr}(G(x))/2]$, dan verkrijgt men $a_{0k} = \pi$, de locatieveelterm en $r_k = \omega$, de evaluatorveelterm [98].

Laten we dit met een voorbeeld illustreren. Beschouw een BCH(15,3) code met $q = 2$, $m = 4$, $n = 2^m - 1 = 15$, $G(x) = x^6$. De symbolen zijn 0 en 1 en de woorden bestaan uit 15 bits. Als primitieve wortel in F_{16} hebben we $\alpha = [0010]$. De machten van α zijn

i	α^i	i	α^i	i	α^i	i	α^i	i	α^i
0	[0001]	1	[0010]	2	[0100]	3	[1000]	4	[0011]
5	[0110]	6	[1100]	7	[1011]	8	[0101]	9	[1010]
10	[0111]	11	[1110]	12	[1111]	13	[1101]	14	[1001]

De a_i zijn de elementen van $F_{16} \setminus \{0\}$ en daarom allemaal te schrijven als machten

van α: $a_i = \alpha^i$. We gaan na dat het syndroom

$$S(x) = \sum_{i=0}^{n-1} \frac{r_i}{x - a_i} \bmod x^6.$$

een veelterm is van graad $6 - 1 = 5$. Inderdaad,

$$\frac{x^6}{x-a} = -\frac{x^6}{a}(1 + \frac{x}{a} + \frac{x^2}{a^2} + \cdots) = 0 \bmod x^6$$

zodat

$$\frac{1}{x-a} = -\frac{(x/a)^6 - 1}{x-a} \bmod x^6 = -\sum_{i=1}^{6} x^{j-1}a^{-j}.$$

Bijgevolg zal het syndroom ook een veelterm zijn van graad 5. Neem bijvoorbeeld een ontvangen woord $r = [111000110011110]$. We zullen hieruit de echte boodschap (het codewoord) reconstrueren. Daartoe berekenen we het syndroom, waarvoor we vinden

$$S_r(x) = \alpha^7 + \alpha^{14}x + \alpha^{11}x^2 + \alpha^{13}x^3 + \alpha^0 x^4 + \alpha^7 x^5.$$

Met het UEA vinden we

	x^6	x^5	x^4	x^3	x^2	x	1
r_{-1}	1	0	0	0	0	0	0
r_0		α^7	1	α^{13}	α^{11}	α^{14}	α^7
r_1			α^{11}	α^9	α^2	0	α^8
r_2				α^8	α^6	α^9	0
r_3					α^7	0	α^8

	x^3	x^2	x	1
a_{00}				1
a_{01}			α^8	α
a_{02}		α^4	α^2	0
a_{03}	α^7	α^5	α^8	α

	x	1
q_0	α^8	α
q_1	α^{11}	α^{14}
q_2	α^3	0

Hier mogen we stoppen vermits $\mathrm{gr}(r_3) < 6/2 = 3$. Dus de foutlocatieveelterm is

$$\pi(x) = \alpha^7 x^3 + \alpha^5 x^2 + \alpha^8 x + \alpha.$$

De nulpunten van deze veelterm zijn α^3, α^9 en α^{12}. Er is dus een fout in de bits op positie 3,9 en 12. Vermits het hier om een binaire code gaat is het overbodig de grootte van de fout te zoeken. We moeten enkel de bits op deze positie wijzigen.

5 Rationale benaderingen

In een Euclidisch domein werd geëist dat de valuatie ∂ waarden aanneemt in $\mathbb{N}$. Dit was essentieel om de eindigheid van het EA aan te tonen. Indien men slechts geïnteresseerd is in de rationale benadering door de kettingbreukontwikkeling vroegtijdig af te breken, dan is het eigenlijk niet zo belangrijk of de ontwikkeling na een eindig aantal termen afbreekt of niet. Om de ontwikkeling op te kunnen

stellen moet men echter nog wel een deling-operatie (of, equivalent hiermee, een mod-operatie) kunnen uitvoeren. Als men zoals voorheen stelt dat $r_k = r_{k-2} - r_{k-1}q_k$ met q_k als "quotiënt" van r_{k-2}/r_{k-1} en r_k als "rest", dan zal men nog steeds eisen dat $\partial(r_k) < \partial(r_{k-1})$, maar we laten de voorwaarde $\partial(\cdot) \in \mathbb{N}$ vallen. Een algebraïsche structuur die dezelfde is als een Euclidisch domein, maar waarbij deze voorwaarde op de valuatie is afgezwakt noemen we een rationaal benaderingsveld (RBV). Laten we een voorbeeld nemen. Beschouw $a, b \in \mathbb{R}$. We definiëren het "quotiënt" q van a en $b \neq 0$ als het gehele deel van a/b: $q = [a/b]$. De rest is dan $r = a \bmod b = a - [a/b]b$. Met de valuatie $\partial(x) = |x|$, $x \in \mathbb{R}$, is voldaan aan $\partial(r) < \partial(b)$. Met deze constructie is $\mathbb{R}$ een RBV dat een uitbreiding is van het Euclidisch domein $\mathbb{Z}$. Op een analoge manier kan men de verzameling der veeltermen uitbreiden tot de verzameling der formele Laurentreeksen met slechts eindig veel positieve machten. Deze verzameling stellen we voor als $\mathbb{F}\langle z^{-1}\rangle$. Als $s, r \in \mathbb{F}\langle z^{-1}\rangle$, dan kan men als quotiënt q het veeltermstuk van de reeks s/r nemen en de mod-bewerking geeft de rest $s \bmod r = s - qr$ wat een reeks is met enkel negatieve machten. Als valuatie kan men nemen $\partial(r) = \mathrm{gr}(r)$, waarbij $\mathrm{gr}(r)$ hier de hoogste voorkomende macht in r betekent. Door de transformatie $z \mapsto z^{-1}$ kan men natuurlijk volledig analoog reeksen in $\mathbb{F}\langle z\rangle$ behandelen.

In een RBV kan men het EA of het UEA ongewijzigd toepassen, met dit verschil dat het misschien nooit eindigt en een ggd dus niet noodzakelijk bestaat. De interpretatie van rationale benadering die ontstaat na het vroegtijdig afbreken van het UEA blijft wel geldig. Vermits Euclides niet wist wat oneindige reeksen waren noemt men in het geval van reeksen het algoritme dikwijls het Chebyshev algoritme [39, § III],[41]. De kettingbreukontwikkeling wordt gebruikt in [40, 42]. In het geval van reeksen in $\mathbb{F}\langle z\rangle$, neemt men als quotiënt het kritisch deel ("Principal part") en men noemt de kettingbreuken P-breuken, ingevoerd door Arne Magnus [95, 96]. In die zin is het UEA ook een veralgemening van het Viscovatoff algoritme [126, 85].

Tot nu toe hebben we over benadering gesproken zonder te preciseren in welke zin benaderd wordt. Stel dat het UEA toegepast wordt op $r, s \in \mathbb{F}\langle z^{-1}\rangle$ en definieer $f = -r/s$. Merk op dat we steeds $r = f$ en $s = -1$ kunnen kiezen. Veronderstel voor de eenvoud dat f enkel negatieve machten van z bevat. Men kan eenvoudig nagaan dat dan $\mathrm{gr}(c_{0k}) < \mathrm{gr}(a_{0k})$ en $\mathrm{gr}(a_{0k}) = \alpha_{0k} = \alpha_1 + \cdots + \alpha_n$ met $\alpha_k = \mathrm{gr}(a_k)$. Ook is $f - c_{0k}/a_{0k} = r_k/a_{0k}$ een machtreeks met graad $-2\alpha_{0k} - \alpha_{k+1}$ waarbij $\alpha_{k+1} \geq 1$. De graden α_{0k} worden meestal Kronecker indices genoemd. We zullen de α_k Euclidische indices noemen. Gezien het aantal vrijheidsgraden in de approximant c_{0k}/a_{0k} enerzijds en het aantal interpolatievoorwaarden anderzijds, noemt men dit een Padé-benadering (op ∞) van f [7, 8, 20, 21]. Voor reeksen in $\mathbb{F}\langle z\rangle$ worden dit gewone Padé-benaderingen (in 0).

Een $[m/n]$ Padé-benadering van f in 0 is een rationale functie $r = p/q$ met $\mathrm{gr}(p) \leq m$, $\mathrm{gr}(q) \leq n$ en $f(z) - r(z) = O(z^{m+n+1})$ voor $z \to 0$. Voor een benadering op ∞ kan men in deze definitie overal z door z^{-1} vervangen.

Het EA berekent een Padé-benadering van het type $[n-1/n]$. Men kan nagaan

dat door een verschuiving van de reeks f het ook mogelijk is Padé-benaderingen van het type $[n/n+k]$ te berekenen met hetzelfde algoritme. Dit is louter een kwestie van de gepaste initialisatie te nemen. Alle $[m/n]$ Padé-benaderingen kunnen in een Padé-tabel gerangschikt worden (m geeft een rij aan en n een kolom). Het EA wandelt (weliswaar met sprongen) langs een diagonaal in deze tabel. Deze tabel heeft een welgekende struktuur. Hij is betegeld met vierkante blokken (singuliere blokken) waarbij er essentieel maar één Padé-benadering per blok is [70]. Tijdens de berekeningen komen de meeste van de klassieke recursieve algoritmes in moeilijkheden omdat een nuldeling optreedt als men binnen zo een blok terecht komt. Het EA is een algoritme dat op een natuurlijke manier over deze blokken springt die het op zijn diagonale pad tegenkomt. Als we veronderstellen dat we geen afrondingsfouten maken, dan zal het EA alle bestaande oplossingen dat het op zijn pad tegenkomt ook berekenen. Zoals we verder zullen zien doen de problemen zich voor omdat men probeert een stelsel op te lossen met singuliere matrix. Bij numerieke berekeningen is de determinant van zo een stelsel nooit exact nul, maar wel zeer klein [38]. Daardoor vervagen de randen van de singuliere blokken in de Padé-tabel en men zal de recursie slechts uitvoeren indien men springt van het ene goed geconditioneerde stelsel naar het volgende goed geconditioneerde stelsel. Dergelijke rekentechniek is recent opgedoken in de literatuur voor het iteratief oplossen van stelsels met Krylov-deelruimtemethoden (§11) en kreeg daar de naam "look-ahead" mee [116, 102]. De naam is nu ingeburgerd en wordt toegepast in heel wat gelijkaardige situaties [100, 63, 62, 53, 60, 74, 54, 56, 57, 69, 58, 19, 18, 65, 123, 121, 122]. We zouden dit kunnen vertalen als de hink-stap-sprong methode omdat, als het algoritme mank loopt omdat er een numeriek probleem is, men met een aantal voorzichtige stapjes eerst de omgeving aftast om te weten te komen waar de numerieke bodem weer stevig is, en dan pas wordt een werkelijke sprong uitgevoerd.

Een verband tussen Padé-benaderingen en het UEA werd bijvoorbeeld gegeven in [99]. In de systeemtheorie is het Padé-probleem op oneindig gekend onder de naam (minimale) partiële realisatie (zie § 10). Onder alle rationale benaderingen die een gegeven aantal momenten op oneindig (in de systeemtheorie noemt men dit Markov parameters) interpoleren, levert het EA de benadering met de laagste (McMillan) graad. Zie ook [84, 69, 72] voor een grondige studie. Voor het meerdimensionale geval zie bv. [117]. Ook andere vormen van Padé-benaderingen vinden toepassingen in de systeemtheorie. Voor een bibliografie zie [25].

6 Hankel-matrices

Er is een directe vertaling van de fundamentele relatie $fa_{0k} - c_{0k} = r_k$ voor de grootheden van het UEA in termen van Hankel-matrices. Definieer de (oneindige) Hankel-matrix met symbool f als $H = H(f) = [f_{i+j+1}]$ voor $i, j = 0, 1, \ldots$ waarbij $f(z) = f_1 z^{-1} + f_2 z^{-2} + \cdots$. Verder noteren we met $\mathbf{a}_{0k}$ de (oneindige)

kolom die de coëfficiënten van de veelterm $a_{0k}(z)$ bevat (uitgebreid met nullen) en met $\mathbf{r}_k$ de kolom met coëfficiënten van $r_k(z)$. Dus $a_{0k}(z) = [1\ z\ z^2\ \cdots]\mathbf{a}_{0k}$ en $r_k(z) = [z^{-1}\ z^{-2}\ \cdots]\mathbf{r}_k$. Als we de gelijkheid van de coëfficiënten opschrijven voor de negatieve machten in de hierboven gegeven fundamentele relatie, dan krijgen we $H\mathbf{a}_{0k} = \mathbf{r}_k$. Als $Z = [\delta_{i,j+1}]$ de verschuivingsoperator is, dan geldt voor een Hankel-matrix $Z^T H = HZ$ en dus geldt ook

$$HZ^i\mathbf{a}_{0k} = [Z^T]^i\mathbf{r}_k, \quad i = 0, 1, \ldots, \alpha_{k+1} - 1.$$

Dit geeft aanleiding tot de matrix-betrekking

$$HA = R$$

waarbij

$$A = [A_{\cdot 0}|A_{\cdot 1}|\cdots] \quad \text{met} \quad A_{\cdot k} = [\mathbf{a}_{0k}|Z\mathbf{a}_{0k}|\cdots|Z^{\alpha_{k+1}-1}\mathbf{a}_{0k}]$$

zodat A een eenheidsbovendriekoeksmatrix is en

$$R = [R_{\cdot 0}|R_{\cdot 1}|\cdots] \quad \text{met} \quad R_{\cdot k} = [\mathbf{r}_k|Z^T\mathbf{r}_k|\cdots|(Z^T)^{\alpha_{k+1}-1}\mathbf{r}_k]$$

zodat R een blok-benedendriehoeksmatrix is. Vanwege de symmetrie van H geldt bovendien dat

$$A^T HA = \text{diag}(D_{00}, D_{11}, \ldots) = D$$

waarbij D een blok-diagonaal matrix is met blokken D_{ii} die benedendriehoekige Hankels zijn met als afmetingen α_{i+1}. De elementen op de antidiagonaal van D_{ii} zijn niet nul. Dit betekent dus dat de Kronecker indices precies aanduiden welke de afmetingen zijn van de inverteerbare leidende principale deelmatrices van H. De Euclidische indices geven de sprongen daartussen.

De recursie van het UEA vertaalt zich in de relatie $ZA = AT$ waarbij T een block tridiagonale matrix is

$$T = \text{tridiag}\begin{pmatrix} T_{01}, T_{12}, \ldots \\ T_{00}, T_{11}, \ldots \\ T_{10}, T_{21}, \ldots \end{pmatrix}.$$

Hij is bovendien eenheidsbovenhessenberg. Een diagonaalblok $T_{k-1,k-1}$ is de Frobenius-matrix voor de veelterm $a_k(z)$ (de eenheden worden zo gekozen dat hij monisch is) en $T_{k-2,k-1}$ bevat enkel in de rechter bovenhoek $x_{k-1}c_k$ als enige van nul verschillende element. Als we dit afbreken by inverteerbare deelmatrices wordt dit $F(a_{0,k+1})A_k = A_k T_k$ waarin $F(a_{0,k+1})$ de Frobenius-matrix is voor de veeltem $a_{0,k+1}$. Zie [71, 72, 28].

Hierdoor is er een verband gelegd tussen het UEA en de driehoekige factorisatie van Hankel-matrices. Men noemt deze algoritmes snel omdat ze slechts

$O(n^2)$ bewerkingen vragen voor deze factorisatie in plaats van $O(n^3)$ met bv. de methode van Gauss [104, 105, 77].

De LA versie berekent de nodige elementen voor het uitvoeren van de recursiestap via de kolommen van A (Cholesky-factor van H^{-1}) terwijl de LP versie dit doet via de kolommen van R (Cholesky-factor van H). Natuurlijk is het naast deze recursieve berekening van de Cholesky-factoren mogelijk om een recursieve aanpassing te berekenen voor het oplossen van een stelsel $Hx = b$. Een andere manier is om via een inversieformule die eenvoudig uit de Cholesky-factoren kan berekend worden, op een vlugge manier $x = H^{-1}b$ uit te rekenen. Men kan daarbij immers gebruik maken van FFT technieken.

7 Formele orthogonale veeltermen

Definieer een lineaire functionaal $\mathcal{L}$ op de verzameling der veeltermen $\mathbb{F}[z]$ door de momenten $\mathcal{L}\{z^k\} = f_k$, $k = 0, 1, \ldots$. Hiermee kan een indefiniet inwendig product gedefinieerd worden met de betrekking $\langle z^k, z^l \rangle = \mathcal{L}\{z^{k+l}\}$. De Gram-matrix voor deze ruimte is dan de Hankel-matrix $H = H(f)$. Indien dit product niet ontaard is dan zullen in het EA alle $\alpha_k = 1$ en noemt men de matrix H sterk regulier. De relatie $A^T H A = D$ zegt dan dat de monische veeltermen $a_{0k}(z)$ orthogonaal zijn voor dit inwendig product. Als bovendien de matrix H positief definiet is, dan is ook het inwendig product definiet en kan men de lineaire functionaal volgens de stelling van Riesz schrijven als een integraal: $\mathcal{L}\{z^k\} = \int z^k d\mu$ waarbij μ een positieve maat is met reële drager. Dit legt het verband met momentenproblemen, quadratuurformules en de klassieke orthogonale veeltermen over een al dan niet eindig deelinterval van $\mathbb{R}$. Voor een maat op de positieve reële as spreekt men over het Stieltjes-momentenprobleem, voor een maat op de ganse reële as spreekt men over het Hamburger-momentenprobleem. In het geval waar de blokken een afmeting groter dan 1 hebben spreekt men van blok-orthogonaliteit [48, 32]. Het UEA berekent de blok-orthogonale veeltermen a_{0k}.

We kunnen dus besluiten dat de noemers van Padé-benaderingen blok-orthogonale veeltermen zijn voor een Gram-matrix met Hankel-structuur. De Padé-benaderingen waarvan sprake komen voor op een hoofddiagonaal van de Padé-tabel [15]. Om andere elementen uit de Padé-tabel te bereiken moet men werken met Hankelmatrices voor een verschoven symbool. Een bijzonder geval (namelijk verschuiven over slechts één positie geeft met behulp van de relatie $H(zf) = Z^T H(f) = H(f)Z$ aanleiding tot $A^T H(zf) A = DT = J$ waarbij J nu een symmetrische tridiagonale blokmatrix is. Deze heeft een heel symmetrische Hankelachtige structuur [72, 28] en het is de blok-versie van de symmetrische Jacobi-matrix voor het geval van klassieke orthogonale veeltermen.

Men kan, mits gepaste startwaarden te kiezen, het EA ook gebruiken voor het berekenen van Padé-benaderingen op een anti-diagonaal van de Padé-tabel. In dat geval is het UEA te zien als een veralgeming van de Stieltjes-procedure [113]

voor het oplossen van het Stieltjes-momentenprobleem. Het is ook een bijzonder geval van het Kronecker-algoritme [87] voor rationale interpolatie.

Er kan ook een verband gelegd worden met Gauss-quadratuurformules in het geval het om momenten gaat van een positieve maat. De abscissen van de quadratuurformule zijn namelijk de eigenwaarden van de Jacobi-matrix J en de bijhorende gewichten (Christoffel getallen) zijn evenredig met de kwadraten van de eerste componenten van de bijhorende eigenvectoren.

Als we de twee systemen van orthogonale veeltermen verbonden met aangrenzende diagonalen van de Padé-tabel willen combineren, kan men tot een recursie komen die een trap beschijft in deze tabel. Door twee naburige trappen te beschouwen kan men daaruit een qd-achtig algoritme [106, 37] produceren wat op zijn beurt weer aanleiding geeft tot een driehoekige ontbinding van de tridiagonale Jacobi-matrix [71, 72, 24, 101].

8 Bezout, Christoffel-Darboux, Routh-Hurwitz

Stellen we even dat de matrix H sterk regulier is. Men kan dan de formule $A^T H A = D$ voor de (inverteerbare) leidende principale deelmatrices H_n van H herschrijven als $A_n D_n^{-1} A_n^T = H_n^{-1}$ en het blijkt dat $k_n(x,y) = [1 \ \cdots \ x^n] H_n^{-1} [1 \ \cdots \ y^n]^T$ een reproducerende kern is voor de verzameling der $n$de graadsveeltermen. Dit betekent dat $\langle p(x), k_n(x,y) \rangle = p(y)$ voor elke veelterm p van graad ten hoogste n. Dit volgt heel eenvoudig uit het feit dat $H_n^{-1} = A_n D_n^{-1} A_n^T$ en dus $k_n(x,y) = \sum_{k=0}^{n} a_{0k}(x) a_{0k}(y)/D_{kk}$ met $D_{kk} = \langle a_{0k}, a_{0k} \rangle$. De inverse van een Hankel matrix is geen Hankel meer, maar hij heeft wel een speciale structuur. Hij wordt een Bezout-matrix genoemd. Een Bezout-matrix wordt (zoals een Hankel) geparameteriseerd door $2n+1$ parameters. Bijvoorbeeld de veeltermen $a_{0,n+1}$ en a_{0n}. Die veeltermen werden bekomen na n stappen van het UEA toegepast op f (en -1). Deze veeltermen bevatten dus alle informatie over H_n en dus ook over zijn inverse. Men kan echter de recursie van het UEA in omgekeerde volgorde uitvoeren, waardoor de elementen van A_n en D_n kunnen gereconstrueerd worden. Men bekomt op deze manier expliciete inversieformules voor Hankel-matrices en die zijn niets anders dan een uitdrukking voor de Christoffel-Darboux betrekking voor de onderliggende orthogonale veeltermen [77, 17]. In deze paragraaf hebben we tot nu toe geredeneerd in de veronderstelling dat de Hankel-matrix H sterk regulier was. Alles wat we gezegd hebben is echter te veralgemenen tot het algemene geval. Stel dat $\alpha = \alpha_{0,m+1} - 1$ en laat n in H_n (en alle ermee verwante grootheden) verwijzen naar de $n$de inverteerbare leidende principale deelmatrix van H. Hij heeft afmetingen α en stel dat $k_n(x,y)$ de reproducerende kern is voor alle veeltermen tot graad α, dan is bijvoorbeeld de algemene vorm van de Christoffel-Darboux betrekking [32]

$$k_n(x,y) = \frac{a_{0,n+1}(x) a_{0n}(y) - a_{0,n+1}(y) a_{0n}(x)}{(x-y)\rho_n}, \quad \rho_n = \langle z^\alpha, a_{0n} \rangle .$$

De inversieformule drukt uit dat $k_n(x,y)$ de genererende functie is voor de Bezoutmatrix H_n^{-1}

$$H_n^{-1} = \frac{1}{\rho_n} \begin{bmatrix} q'_0 & 0 & \cdots & 0 \\ q'_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ q'_\alpha & \cdots & q'_1 & q'_0 \end{bmatrix} \begin{bmatrix} q_1 & \cdots & q_\alpha & 1 \\ \vdots & .^{\cdot} & .^{\cdot} & 0 \\ q_\alpha & .^{\cdot} & .^{\cdot} & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix} - \begin{bmatrix} q_0 & 0 & \cdots & 0 \\ q_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ q_\alpha & \cdots & q_1 & q_0 \end{bmatrix} \begin{bmatrix} q'_1 & \cdots & q'_\alpha & 1 \\ \vdots & .^{\cdot} & .^{\cdot} & 0 \\ q'_\alpha & .^{\cdot} & .^{\cdot} & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

waarbij $a_{0,n}(z) = q'_0 + q'_1 z + \cdots + q'_\alpha z^\alpha$ en $a_{0,n+1}(z) = q_0 + q_1 z + \cdots + q_\alpha z^\alpha$, $\alpha = \alpha_{0,n+1}$. Dit is de zogenaamde Heinig formule [77].

Een andere toepassing van het EA is de stabiliteitsanalyse voor veeltermen. Men zegt dat een veelterm $p(z) = \sum_{k=0}^{n} p_k z^k$ stabiel is als zijn nulpunten een negatief reëel deel hebben. Men noemt

$$r(z) = \frac{p_1 + p_3 z + p_5 z^2 + \cdots}{p_0 + p_2 z + p_4 z^2 + \cdots} = \frac{1}{\sqrt{z}} \frac{p(\sqrt{z}) - p(-\sqrt{z})}{p(\sqrt{z}) + p(-\sqrt{z})}$$

de Hurwitz-alternant van p. Men bewijst dat de veelterm stabiel is dan en slechts dan als zijn Hurwitz alternant een (rationale) Stieltjes-transformatie is [78]. Dit betekent dat hij in een (eindige) Stieltjes-kettingbreuk kan ontwikkeld worden, dat is een kettingbreuk met positieve wijzergetallen. Deze ontwikkeling kan gebeuren met een vorm van het EA die in dit verband beter gekend is onder de naam Routh-algoritme. Mits wat betere analyse van het probleem kan men niet alleen de stabiliteit onderzoeken van de veelterm, maar precies zijn inertia gaan bepalen, dat is het aantal wortels met reëel deel positief, negatief of nul [67].

9 Toeplitz en Schur

Het soort recursies dat ontstaat uit het UEA en dat aanleiding geeft tot veralgemeningen van orthogonale veeltermen voor een Hankel-metriek kan aangepast worden voor Gram-matrices met een Toeplitz-structuur. Zo komt men tot veralgemeningen van algoritmes van Szegő, Schur en Levinson voor het klassieke geval van veeltermen orthogonaal ten opzichte van een positieve maat waarvan de drager ligt op de eenheidscirkel in het complexe vlak [24, 30]. De overeenkomstige rationale benaderingen benaderen 2 gegeven reeksen, één rond de oorsprong en één rond ∞. Men spreekt in dat geval van tweepunts-Padé-benaderingen [24]. Indien men dit nog verder veralgemeent en meer dan 2 punten neemt, zal men meer algemene rationale interpolatieproblemen oplossen. Men kan hier ook matrixversies voor beschouwen en daarvoor werd een module-theoretisch kader ontwikkeld om deze problemen in een heel algemene vorm op te lossen [120, 118]. Anderzijds kan men ook algemene Gram-matrices beschouwen en ook daarvoor blok-orthogonale veeltermen opstellen [29]. Het blijkt dat het Schur-algoritme, wat oorspronkelijk voor Toeplitz-matrices is opgesteld en dat kan geïnterpreteerd

worden als het berekenen van opeenvolgende Schur-complementen in een matrix, in feite equivalent is met het EA in het geval van een Hankel-matrix [32]. Net zoals de inverse van een Hankel-matrix een Bezout-matrix is, hebben ook de opeenvolgende Schur-complementen een speciale structuur. Het zijn beiden voorbeelden van quasi-Hankel matrices die in een algemeen kader van matrices met lage verplaatsingsrang kunnen geplaatst worden. De quasi-Hankel-matrices laten het gebruik van een veralgemeend EA toe [83].

10 Lineaire systeemtheorie

De klassieke toestandsruimtebeschrijving voor een scalair strikt causaal lineair tijdsinvariant systeem is

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

Hierin is $k = 0, 1, \ldots$, $x_k \in \mathbb{F}^{n\times 1}$ (met $x_0 = 0$) de toestandsvector, $u_k \in \mathbb{F}$ de invoer en y_k de uitvoer op het ogenblik k. De matrix A noemt men de toestandstransitiematrix. De vectorruimte voortgebracht door de toestandsvectoren noemt men de toestandsruimte. Als de n uit de formules gelijk is aan de dimensie van de toestandsruimte, dan noemt men het drietal $[A, B, C]$ een minimale toestandsrealisatie van het systeem. Voor minimale realisaties is de afmeting van A zo klein als mogelijk. Door z-transformaties te nemen van deze relaties, aangeduid met een hoedje, bijvoorbeeld $\hat{u}(z) = \sum_k u_k z^{-k}$, kan men dit herschrijven als

$$\begin{aligned} z\hat{x}(z) &= A\hat{x}(z) + B\hat{u}(z) \\ \hat{y}(z) &= C^T\hat{y}(z). \end{aligned}$$

Men kan hieruit de toestand elimineren en men bekomt dan het verband $\hat{y}(z) = f(z)\hat{u}(z)$ met $f(z) = C^T(zI - A)^{-1}B$ de overdrachtsfunctie van het systeem. De rij (f_k) noemt men de impulsresponsie en de $f_k = C^T A^{k-1} B$ noemt men de Markov-parameters. Merk op dat $f(z)$ rationaal is en dat de graad gelijk is aan n indien de realisatie minimaal is. De matrix $\mathcal{O} = [C \; A^T C \; (A^T)^2 C \; \cdots]^T$ noemt men de observeerbaarheidsmatrix en $\mathcal{C} = [B \; AB \; A^2 B \; \cdots]$ is de controleerbaarheidsmatrix. Het systeem is observeerbaar als $\mathcal{O}$ van volle rang is en het is controleerbaar als $\mathcal{C}$ van volle rang is. Voor een minimale realisatie is $n = \text{rang } \mathcal{C} = \text{rang } \mathcal{O} = \text{rang } \mathcal{OC}$ met $\mathcal{OC} = [C^T A^{i+j} B] = [f_{i+j+1}] = H(f)$ een Hankel-matrix.

Een minimale partiële realisatie is een benaderend systeem waarbij de benadering een aantal van de eerste Markov-parameters moet gemeen hebben met het gegeven system en onder alle benaderingen met deze eigenschap moet die met de kleinste graad gekozen worden. Dit is precies wat door het UEA berekend wordt als we dat toepassen op de reeks $f(z)$.

11 Krylov-methoden

Om een stelsel lineaire vergelijkingen $Mx = b$ op te lossen waarbij M symmetrisch en positief definiet is kan men itereren met een formule $x_k = x_{k-1} + \lambda_k s_{k-1}$. Hierin is s_{k-1} een zoekrichting en λ_k een staplengte. In de methode der toegevoegde richtingen [79] kiest men opeenvolgende s_k die orthogonaal zijn ten opzichte van de metriek M, dus $s_k^T M s_{k-1} = 0$. Meer speciaal in het geval van de methode der toegevoegde gradiënten [79] stelt men

$$s_k = r_k + \mu_k s_{k-1}, \quad \mu_k = \|r_k\|^2 / \|r_{k-1}\|^2, \quad r_k = b - Mx_k, \quad \|r\|^2 = r^T r.$$

Door het minimaliseren van $\|r_k\|^2_{M^{-1}}$ vindt men

$$\lambda_k = \frac{r_{k-1}^T s_{k-1}}{s_{k-1}^T M s_{k-1}}.$$

Het blijkt dat dan zowel s_n als r_n tot de Krylovruimte

$$\mathcal{K}_n(r_0, M) = \text{span}\{r_0, Mr_0, \ldots, M^n r_0\} = \text{span}\{y_0, y_1, \ldots, y_n\}, \quad y_i = M^i r_0$$

behoren en dat $r_k^T r_l = 0$ voor $k \neq l$, dit wil zeggen dat de residus een orthogonale basis vormen voor $\mathcal{K}_n(r_0, M)$. Vermits $r_k \in \mathcal{K}_k(r_0, M)$ zal er een comonische veelterm φ_k zijn zodanig dat $r_k = \varphi_k(M) r_0$. Daardoor ontstaat een isomorfisme tussen de ruimte der veeltermen en de Krylovruimte met inwendig product $\langle M^i r_0, M^j r_0 \rangle = \langle z^i, z^j \rangle = f_{i+j+1}$. De Gram-matrix voor deze niet-orthogonale basissen is de Hankel-matrix $H_n = H_n(f)$ omdat M symmetrisch is verondersteld. Dus het orthogonaliseren van de residus r_k is equivalent met het orthogonaliseren van de veeltermen φ_k ten opzichte van het inwendige product met metriek H. Bovendien is welbekend dat de comonische veelterm met de kleinste norm de orthogonale veelterm is [36]. Dit betekent dat $r_n = \varphi_n(M) r_0$ een oplossing is van het optimisatieprobleem

$$\min\{\|r\| : r \in r_0 + \mathcal{K}_{n-1}(y_1, M), y_1 = Mr_0\}$$

en dit correspondeert op zijn beurt met een oplossing van het probleem

$$\min\{\|b - Mx\|_{M^{-1}} : x \in x_0 + \mathcal{K}_{n-1}(r_0, M)\}.$$

We kunnen dus onze vorige technieken voor het opstellen van orthogonale veeltermen voor een Hankel-metriek ten volle aanwenden. In dit geval is $H_n = Y_n^T Y_n$ met $Y_n = [y_0 | y_1 | \cdots | y_n]$, $y_0 = r_0$ en $y_k = My_{k-1}$. De comonische orthogonale veeltermen φ_k zijn dus evenredig met de orthogonale veeltermen a_{0k} in de eerdere notatie. Bovendien is door het stellen van $\hat{Y}_n = Y_n A_n$ voldaan aan (zie vroeger)

$$\hat{Y}_n^T \hat{Y}_n = A_n^T Y_n^T Y_n A_n = A_n^T H_n(f) A_n = D_n$$

en aan

$$\hat{Y}_n^T M \hat{Y}_n = A_n^T H_n(zf) A_n = D_n T_n = J_n.$$

Indien M symmetrisch en positief definiet is, dan is H_n een positief definiete Hankel-matrix. Deze methode is het klassieke Lanczos-algoritme [89]. Als M niet symmetrisch is, dan is H_n niet meer Hankel en dan zal een Gram-Schmidt orthogonalisatie niet meer kunnen steunen op de eenvoudige recursiebetrekking van het EA. In dat geval zal in de relatie $F(a_{0,n+1})A_n = A_n J_n$, de tridiagonale matrix J_n moeten vervangen worden door een volledige bovenhessenbergmatrix. Dit voluit toepassen van de Gram-Schmidt orthogonalisatie op de kolommen van de matrix Y_n is gekend onder de naam Arnoldi-algoritme [5]. Het is echter mogelijk om toch een Hankel-matrix te bekomen voor een niet-symmetrische M indien men bereid is de orthogonaliteit van de residus te vervangen door een biorthogonaliteit. Men stelt namelijk twee Krylov-matrives op: één met M en één met M^T. Dus met $Y_n = [y_0|\cdots|y_n]$ en $Z_n = [z_0|\cdots|z_n]$ waarbij $y_k = My_{k-1}$ en $z_k = M^T z_{k-1}$, bekomt men weer een matrix $H_n = Z_n^T Y_n$ die Hankel is zodat men weer het EA kan toepassen. Deze keer zal de matrix niet noodzakelijk meer sterk regulier zijn en moeten er niet-triviale sprongen gemaakt worden. Vanwege de biorthogonaliteit werd dit algoritme het BCG ("biconjugate gradient") algoritme genoemd [51]. In het laatste decennium is er een explosie geweest van varianten en verbeteringen op deze methode en men heeft op dit ogenblik het grootste gedeelte van deze iteratieve algoritmes voor het oplossen van stelsels in kaart gebracht [73, 75, 10, 53, 60, 61, 81, 109, 111, 125, 59, 100, 107, 76, 6, 60].

Oorspronkelijk werd de methode door Lanczos voorgesteld in verband met het berekenen van eigenwaarden [88]. Om deze connectie te zien, merken we op dat voor het niet-symmetrische geval $\hat{Z}_n^T \hat{Y}_n = D_n$ en dus $\hat{Z}_n^T = D_n \hat{Y}_n^{-1}$. Bijgevolg is de relatie $\hat{Z}_n^T M \hat{Y}_n = A_n^T H_n(zf) A_n = J_n = D_n T_n$ te schrijven als $\hat{Y}_n^{-1} M \hat{Y}_n = T_n$. Dit betekent dat in het geval M een $m \times m$ matrix is en $\alpha_{0,n+1} = m$, de matrices M en T_n gelijkvormig zijn en dus dezelfde eigenwaarden hebben. De matrix T_n was blok-tridiagonaal en dus is het veel eenvoudiger om de eigenwaarden van T_n te berekenen dan van M. Praktisch zal echter het aantal kolommen $\alpha_{0,n+1}$ van A_n veel kleiner zijn dan m, en in dat geval kan men T_n beschouwen als een projectie van de matrix M op Krylov-deelruimten. Het spectrum van T_n is dan wel niet gelijk aan het spectrum van M maar het zal een benadering zijn. Het blijkt namelijk dat in eerste instantie convergentie optreedt naar de grootste eigenwaarden. Voor wie convergentie-eigenschappen kent van Padé-benaderingen is dit te begrijpen omdat impliciet een Padé-benadering op ∞ wordt opgesteld van de functie $f(z) = z_0^T (zI - M)^{-1} y_0$. Dit is de transfertfunctie van het lineair systeem met toestandsrealisatie (M, y_0, z_0). De matrices Y_∞ en Z_∞^T zijn de bijhorende controleerbaarheids– en observeerbaarheidsmatrices. De eigenwaarden van T_n, die men Ritz-waarden noemt, zijn ook de nulpunten van de veeltermen $a_{0,n+1}$ en dus de polen van de Padé-benadering. Het is dus zeer begrijpelijk dat men eerst zal convergeren naar de grootste eigenwaarden, want die liggen het dichtst

bij ∞. Hoe de rang van $H(f) = Z_\infty^T Y_\infty$, dat is hetzelfde als de graad van f, zich verhoudt tot de afmeting van M hangt af van de Jordan-structuur van M. Die is dus bepalend voor het deel van het spectrum dat theoretisch kan gerecupereerd worden uit J_n. De meervoudigheid van λ als pool van f is steeds kleiner dan of gelijk aan de algebraïsche meervoudigheid van λ als eigenwaarde van M. Anderzijds hangt het ook af van de startvectoren z_0 en y_0 wat de rangen zullen zijn van Y_∞ en Z_∞ en dat bepaalt welk deel van de rang van $H(f)$ kan teruggevonden worden in de rang van J_n. Het onderzoek over het berekenen van eigenwaarden met dit soort technieken is nog in volle ontwikkeling [108, 55, 110, 46].

12 Slotbemerkingen

We hebben getracht een zeer beknopt overzicht te geven van toepassingsdomeinen waarin men recursies gebruikt die op één of andere manier te identificeren zijn met het Euclidisch (of Chebyshev) algoritme. Het is zeker niet de bedoeling om deze toepassingen uit te leggen of de preciese toedracht te verklaren, daarvoor zou een heel boekdeel nog niet voldoende zijn. We hebben ons beperkt tot het invoeren van wat terminologie en hebben daarna aangegeven hoe het Euclidisch algoritme een rol speelt in de oplossing van het gestelde probleem. We geven grif toe dat we slechts het topje van een ijsberg tonen en dat het allemaal zeer simplistisch is voorgesteld. Voor de uitwerking en de practische toepassing van een dergelijk basisidee komt nog veel meer om het hoekje kijken waar we met geen woord over gerept hebben. Het is echter zeer boeiend om te zien hoe eenzelfde, eigenlijk zeer eenvoudig rekenschema zoveel uiteenlopende takken van de wiskunde kan verbinden zoals getaltheorie, rationale benadering, orthogonale veeltermen, complexe functieleer, codetheorie, systeemtheorie, lineaire algebra, operatortheorie, numerieke wiskunde, differentiaalvergelijkingen, signaalverwerking, netwerken, controletheorie, verstrooiïngstheorie, enz. Verbazend is het ook te merken dat bijna al deze elementen voor het eerst worden aangereikt tijdens het curriculum van de opleiding ingenieur computerwetenschappen en, zeker wat de eerste auteur betreft, was dit in een les en in een cursus van professor L. Buyst.

Referenties

[1] P. Achuthan and S. Sundar. A new application of the extended Euclidean algorithm for matrix Padé approximants. *Comput. Math. Applic.*, 16(4):287–296, 1988.

[2] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The design and analysis of computer algorithms*. Addison Wesley, Reading, Mass., 1974.

[3] R.V. Andree. *Selections from modern abstract algebra*. Holt, Rinehart and Winston, New York, 1958.

[4] A.C. Antoulas. Rational interpolation and the Euclidean algorithm. *Linear Algebra Appl.*, 108:157–171, 1988.

[5] W.E. Arnoldi. The principle of minimized iterations in the solution of the matrix eigenvalue problem. *Quart. Appl. Math,*, 9:17–29, 1951.

[6] O. Axelsson. *Iterative solution methods*. Cambridge University Press, 1994.

[7] G.A. Baker, Jr. and P.R. Graves-Morris. *Padé Approximants. Part I: Basic Theory*, volume 13 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Co., Reading, 1981.

[8] G.A. Baker, Jr. and P.R. Graves-Morris. *Padé Approximants. Part II: Extensions and Applications*, volume 14 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley, Reading, MA, 1981.

[9] E.R. Berlekamp. *Algebraic coding theory*. McGraw-Hill, New York, 1968.

[10] D.L. Boley, S. Elhay, G. H. Golub, and M.H. Gutknecht. Nonsymmetric Lanczos and finding orthogonal polynomials associated with indefinite weights. *Numer. Algorithms*, 1(1):21–44, 1991.

[11] R.C. Bose and D.K. Ray-Chaudhuri. Further results on error correcting binary group codes. *Inf. Control*, 3:68–79, 1960.

[12] R.C. Bose and D.K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Inf. Control*, 3:68–79, 1960.

[13] R.P. Brent, F.G. Gustavson, and D.Y.Y. Yun. Fast solution of Toeplitz systems of equations and computation of Padé approximants. *J. Algorithms*, 1:259–295, 1980.

[14] A.J. Brentjes. *Multi-dimensional continued fraction algorithms*, volume 145. Mathematical Centre, Amsterdam, The Netherlands, 1981.

[15] C. Brezinski. *Padé-type approximants and general orthogonal polynomials*, volume 50 of *Internat. Ser. of Numer. Math.* Birkhäuser Verlag, Basel, 1980.

[16] C. Brezinski. *History of continued fractions and Padé approximants*, volume 12 of *Springer Ser. Comput. Math.* Springer, Berlin, 1990.

[17] C. Brezinski. Generalization of the Christoffel-Darboux identity for adjacent families of orthogonal polynomials. *Appl. Numer. Meth.*, 8:193–199, 1991.

[18] C. Brezinski and M. Redivo Zaglia. Look-ahead in Bi-CGSTAB and other product-type methods for linear systems. *BIT*, 35(2):169–201, 1995.

[19] C. Brezinski and M. Redivo Zaglia. A look-ahead strategy for the implementation of some old and new extrapolation methods. *Numer. Algorithms*, 1995. To appear.

[20] C. Brezinski and J. van Iseghem. Padé approximations. In P.G. Ciarlet and J.L. Lions, editors, *Handbook of Numerical Analysis*, volume 3. North-Holland, 1993.

[21] C. Brezinski and J. van Iseghem. A taste of Padé approximation. In *Acta Numerica*, pages 53–103, 1995.

[22] W.S. Brown. On Euclid's algorithm and the computation of polynomial greatest common divisor. *J. ACM*, 18:478–504, 1971.

[23] A.M. Bruckstein and T. Kailath. Inverse scattering for discrete transmission-line models. *SIAM Rev.*, 29(3):359–389, 1987.

[24] A. Bultheel. *Laurent series and their Padé approximations*, volume OT-27 of *Oper. Theory: Adv. Appl.* Birkhäuser Verlag, Basel-Boston, 1987.

[25] A. Bultheel and M. Van Barel. Padé techniques for model reduction in linear system theory. *J. Comput. Appl. Math.*, 14:401–438, 1986.

[26] A. Bultheel and M. Van Barel. A matrix Euclidean algorithm and matrix Padé approximation. Technical Report TW104, Department of Computer Science, K.U. Leuven, January 1988.

[27] A. Bultheel and M. Van Barel. A matrix Euclidean algorithm and the matrix minimal Padé approximation problem. In C. Brezinski, editor, *Continued Fractions and Padé Approximants*, pages 11–51. North-Holland, 1990.

[28] A. Bultheel and M. Van Barel. Euclid, Padé and Lanczos, another golden braid. Technical Report TW188, Department of Computer Science, K.U. Leuven, April 1993.

[29] A. Bultheel and M. Van Barel. Formal orthogonal polynomials for an arbitrary moment matrix and Lanczos type methods. In J.D. Brown, M.T. Chu, D.C. Ellison, and R.J. Plemmons, editors, *Proceedings of the Lanczos International Centenary Conference*, pages 273–275. SIAM, 1994.

[30] A. Bultheel and M. Van Barel. Linear prediction: mathematics and engineering. *Bull. Belgian Math. Soc. Simon Stevin*, 1:1–58, 1994.

[31] A. Bultheel and M. Van Barel. Some applications of the Euclidean algorithm. In D. Bainov and V. Covachev, editors, *Proceedings of the Second International Colloquium on Numerical Analysis*, pages 45–54, Zeist, The Netherlands, 1994. VSP Inl. Sci. Publ.

[32] A. Bultheel and M. Van Barel. Formal orthogonal polynomials and Hankel/Toeplitz duality. *Numer. Algorithms*, 10:289–335, 1995.

[33] L. Buyst. *Moderne algebra voor ingenieurs*. L. Wouters, Leuven, 1967.

[34] L. Buyst. *Aanvullingen van toegepaste wiskunde: Functies van complexe veranderlijken, IV Laplace transformatie*. Standaard Wetenschappelijke Uitgeverij, Leuven, 1969.

[35] L. Buyst. *Beginselen van toegepaste wiskunde*. Acco, Leuven, 1970.

[36] L. Buyst. *Numerieke methodes in de benaderingstheorie, Deel A*. L. Wouters, Leuven, 1992.

[37] L. Buyst. *Numerieke methodes in de benaderingstheorie, Deel C: Rationale benaderingen*. L. Wouters, Leuven, 1992.

[38] L. Buyst and A. Bultheel. *Inleiding tot de numerieke wiskunde*. L. Wouters, 1989.

[39] P.L. Chebyshev. Sur l'interpolation par la méthode des moindres carrés. *Mem. Acad. Impér. des Sciences St. Petersbourg, sér. 7*, 1:1–24, 1859. See Œuvres, Tome I, Chelsea Pub. Comp. pp. 471-498.

[40] P.L. Chebyshev. Sur les fractions continues algébriques. *Journ. de Math. Pures et Appliquées, Sér II*, 10:353–358, 1865. See Œuvres, Tome I, Chelsea Pub. Comp. pp. 609-614.

[41] P.L. Chebyshev. Sur le développement de fonctions en séries à l'aide des fractions continues. In A. Markoff and N. Sonin, editors, *Œuvres de P.L. Tchebycheff, Tome I*, pages 615–631, New York, 1866. Chelsea Publishing Company.

[42] P.L. Chebyshev. Sur la détermination des fonctions d'après les valeurs qu'elles ont pour certaines valeurs de variables. *Math. Sb.*, 4:231–245, 1870. See Œuvres, Tome II, Chelsea Pub. Comp. pp. 71-82.

[43] T. Citron, A.M. Bruckstein, and T. Kailath. An inverse scattering approach to the partial realization problem. In *Proc. 23rd Conf. on Decision and Control (CDC), Las Vegas, 1984*, 1984.

[44] T. Citron and T. Kailath. Euclid's algorithm, scattering theory and VLSI architecture for decoding Reed-Solomon codes. *IEEE Trans. Inf. Th.*, IT-, 1986.

[45] G.C. Clark Jr. and J.B. Cain. *Error-correction coding for digital communications*. Plenum Press, New York, London, 1981.

[46] J.K. Cullum. Block Lanczos algorithms for large matrix eigenvalue problems: Part II. Nonsymmetric case. In *Proceedings of the Cornelius Lanczos International Centenary Conference*, pages 316–318. SIAM, 1994.

[47] E.J. Dijksterhuis. *De elementen van Euclides II.* P. Noordhoff, Groningen, 1930.

[48] A. Draux. *Polynômes orthogonaux formels – applications*, volume 974 of *Lecture Notes in Math.* Springer, Berlin, 1983.

[49] Gui-Liang Feng and K.K. Tzeng. A generalized Euclidean algorithm for multisequence shift-register synthesis. *IEEE Trans. Inf. Th.*, 35(3):584–594, 1989.

[50] Gui-Liang Feng and K.K. Tzeng. A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes. *IEEE Trans. Inf. Th.*, 37(5):1274–1287, 1991.

[51] R. Fletcher. Conjugate gradient methods for indefinite systems. In G.A. Watson, editor, *Numerical Analysis Dundee 1975*, number 506 in Lecture Notes in Math., pages 73–89. Springer, 1976.

[52] G.D. Forney Jr. Convolutional codes I : Algebraic structure. *IEEE Trans. Inf. Th.*, IT-16:720–738, 1970.

[53] R.W. Freund. The look-ahead Lanczos process for large nonsymmetric matrices and related algorithms. In M.S. Moonen, G. Golub, and B.L.R. De Moor, editors, *Linear algebra for large scale and real-time applications*, volume 232 of *NATO-ASI series E: Applied Sciences*, pages 137–163. Kluwer Acad. Publ., Dordrecht, 1993.

[54] R.W. Freund. A look-ahead Schur-type algorithm for solving general Toeplitz systems. *Z. Angew. Math. Mech.*, June 1993. AT&T Bell Labs. Numerical Analysis Manuscript 93-09.

[55] R.W. Freund. Lanczos-type algorithms for structured non-Hermitian eigenvalue problems. In *Proceedings of the Cornelius Lanczos International Centenary Conference*, pages 243–245. SIAM, 1994.

[56] R.W. Freund. A look-ahead Bareis algorithm for general Toeplitz matrices. *Numer. Math.*, 68:35–69, August 1994. AT&T Bell Labs. Numerical Analysis Manuscript 93-11.

[57] R.W. Freund. A look-ahead Bareiss algorithm for general Toeplitz matrices. *Numer. Math.*, 68(1):35–69, 1994.

[58] R.W. Freund. The look-ahead Lanczos process for nonsymmetric matrices and its applications. In *Proceedings of the Cornelius Lanczos International Centenary Conference*, pages 33–47. SIAM, 1994.

[59] R.W. Freund, G.H. Golub, and N.M. Nachtigal. Iterative solution of linear systems. *Acta Numerica*, 1:57–100, 1992.

[60] R.W. Freund, M.H. Gutknecht, and N.M. Nachtigal. An implementation of the look-ahead Lanczos algorithm for non-Hermitian matrices, Part I. *SIAM J. Sci. Statist. Comput.*, 14(1):137–158, 1993.

[61] R.W. Freund and N.M. Nachtigal. QMR: A quasi-minimal residual method for non-Hermitian matrices. *Numer. Math.*, 60:315–339, 1991.

[62] R.W. Freund and H. Zha. Formally biorthogonal polynomials and a look-ahead Levinson algorithm for general Toeplitz systems. *Linear Algebra Appl.*, 188/189:255–303, 1993.

[63] R.W. Freund and H. Zha. A look-ahead strategy for the solution of general Hankel systems. *Numer. Math.*, 64:295–322, 1993.

[64] P.A. Fuhrmann. A matrix Euclidean algorithm and matrix continued fraction expansion. *Systems Control Lett.*, 3:263–271, 1983.

[65] K. Gallivan, S. Thirumalai, and P. Van Dooren. A block Toeplitz look-ahead Schur algorithm. In M. Moonen and B. De Moor, editors, *SVD and Signal Processing III*, pages 199–206, Amsterdam, 1995. Elsevier.

[66] K.O. Geddes, S.R. Czapor, and G. Labahn. *Algorithms for computer algebra*. Kluwer Academic Publishers, 1992.

[67] Y. Genin. Euclid algorithm, orthogonal polynomials and generalized Routh-Hurwitz algorithm. *Linear Algebra Appl.*, 1994. To appear.

[68] V.D. Goppa. A new class of linear error-correcting codes. *Probl. Peredach. Inform.*, 6:24–30, 1970.

[69] W. B. Gragg and M. H. Gutknecht. Stable look-ahead versions of the Euclidean and Chebyshev algorithms. In R.V.M. Zahar, editor, *Approximation and Computation: A Festschrift in Honor of Walter Gautschi*, pages 231–260. Birkhäuser Verlag, 1994.

[70] W.B. Gragg. The Padé table and its relation to certain algorithms of numerical analysis. *SIAM Rev.*, 14:1–62, 1972.

[71] W.B. Gragg. Matrix interpretations and applications of the continued fraction algorithm. *Rocky Mountain J. Math.*, 4(2):213–225, 1974.

[72] W.B. Gragg and A. Lindquist. On the partial realization problem. *Linear Algebra Appl.*, 50:277–319, 1983.

[73] M.H. Gutknecht. A completed theory of the unsymmetric Lanczos process and related algorithms. Part I. *SIAM J. Matrix Anal. Appl.*, 13(2):594–639, 1992.

[74] M.H. Gutknecht. Stable row recurrences for the Padé table and generically superfast lookahead solvers for non-Hermitian Toeplitz systems. *Linear Algebra Appl.*, 188/189:351–422, 1993.

[75] M.H. Gutknecht. A completed theory of the unsymmetric Lanczos process and related algorithms. Part II. *SIAM J. Matrix Anal. Appl.*, 15:15–58, 1994.

[76] M.H. Gutknecht. The Lanczos process and Padé approximation. In *Proceedings of the Cornelius Lanczos International Centenary Conference*, pages 61–75. SIAM, 1994.

[77] G. Heinig and K. Rost. *Algebraic methods for Toeplitz-like matrices and operators*. Akademie Verlag, Berlin, 1984. Also Birkhäuser Verlag, Basel.

[78] P. Henrici. *Applied and computational complex analysis. Volume 2, special functions, integral transforms, asymptotics, continued fractions*, volume II of *Pure and Applied Mathematics, a Wiley-interscience series of texts, monographs and tracts*. John Wiley & Sons, New York, 1977.

[79] M.R. Hestenes and E. Stiefel. Methods of conjugate gradients for solving linear systems. *J. Res. Nat. Bur. Stand.*, 49:409–436, 1952.

[80] Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 2:147–156, 1959.

[81] W. Joubert. Lanczos methods for the solution of nonsymmetric systems of linear equations. *SIAM J. Matrix Anal. Appl.*, 13:926–943, 1992.

[82] T. Kailath. *Linear Systems*. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1980.

[83] T. Kailath and A.H. Sayed. Displacement structure: theory and applications. *SIAM Rev.*, 37:297–386, 1995.

[84] R. Kalman. On partial realizations, transfer functions, and canonical forms. *Acta Technica Scandinavica*, 31:9–32, 1979. (Zbl 424.93020, MR 80k:93022).

[85] A.N. Khovanskii. *The application of continued fractions and their generalizations to problems in approximation theory.* Noordhoff, Groningen, 1963.

[86] D.E. Knuth. *The art of computer programming, Vol 2 : Seminumerical algorithms.* Addison Wesley, Reading, Mass., 1969.

[87] L. Kronecker. Zur Theorie der Elimination einer Variabel aus zwei algebraischen Gleichungen. *Monatsber. Königl. Akad. Wiss.*, pages 535–600, 1881.

[88] C. Lanczos. An iteration method for the solution of the eigenvalue problem of linear differential and integral operators. *J. Res. Natl. Bur. Stand.*, 45:225–280, 1950.

[89] C. Lanczos. Solution of systems of linear equations by minimized iterations. *J. Res. Natl. Bur. Stand.*, 49:33–53, 1952.

[90] P. Levrie and A. Bultheel. Modification of generalized continued fractions associated with recurrence relations of Perron-Kreuser type. Technical Report TW78, Department of Computer Science, K.U. Leuven, May 1986.

[91] P. Levrie and A. Bultheel. Convergence acceleration for the numerical solution of second order linear recurence relations. *SIAM J. Numer. Anal.*, 27(1):166–177, 1990.

[92] P. Levrie and A. Bultheel. First order linear recurrence systems and matrix continued fractions. Technical Report TW235, Department of Computer Science, K.U. Leuven, December 1995.

[93] P. Levrie, M. Van Barel, and A. Bultheel. First-order linear recurrence systems and general N-fractions. In A.M. Cuyt, editor, *Nonlinear Numerical Methods and Rational Approximation II*, pages 433–446. Kluwer, 1994.

[94] E.A. Lipitakis. Euclid's algorithm and accelerated iterative methods. In E.A. Lipitakis, editor, *Advances on computer mathematics and its applications*, pages 125–149, Singapore, 1993. World Scientific. Proc. first Hellenic conference on mathematics and informatics (HERMIS'92), Athens, Greece, Sept., 1992.

[95] A. Magnus. Certain continued fractions associated with the Padé table. *Math. Z.*, 78:361–374, 1962.

[96] A. Magnus. Expansion of power series into P-fractions. *Math. Z.*, 80:209–216, 1962.

[97] J.L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Th.*, IT-15:122–127, 1969.

[98] R.J. McEliece. *The theory of information and coding: A mathematical framework for communication*, volume 3 of *Encyclopedia of mathematics*. Addison Wesley, Reading, Mass., 1977.

[99] R.J. McEliece and J.B. Shearer. A property of Euclid's algorithm and an application to Padé approximation. *SIAM J. Appl. Math.*, 34:611–616, 1978.

[100] B.N. Parlett. A new look at the Lanczos algorithm for solving symmetric systems of linear equations. *Linear Algebra Appl.*, 29:323–246, 1980.

[101] B.N. Parlett. The new qd algorithms. In *Acta Numerica*, pages 459–491. Cambridge University Press, 1995.

[102] B.N. Parlett, D.R. Taylor, and Z.A. Liu. A look-ahead Lanczos algorithm for unsymmetric matrices. *Mathematics of Comp.*, 44(169):105–124, 1985.

[103] I.S. Reed and G. Solomon. Polynomial codes over certain finite fields. *J. Soc. Ind. Appl. Math.*, 8:300–304, 1960.

[104] J. Rissanen. Algorithms for the triangular decomposition of block Hankel and Toeplitz matrices with application to factoring positive matrix polynomials. *Math. Comp.*, 27:147–154, 1973.

[105] J. Rissanen. Solution of linear equations with Hankel and Toeplitz matrices. *Numer. Math.*, 22:361–366, 1974.

[106] H. Rutishauser. Der Quotienten-Differenzen-Algorithmus. *Zeit. für Angewandte Math.*, 5:233–251, 1954.

[107] Y. Saad. The Lanczos biorthogonalization algorithm and other oblique projection methods for solving large unsymmetric systems. *SIAM J. Numer. Anal.*, 19:485–506, 1982.

[108] Y. Saad. *Numerical methods for large eigenvalue problems*. Algorithms and Architectures for Advanced Scientific Computation. Manchester University Press/ Halsted Press, 1992.

[109] Y. Saad and M.H. Schultz. GMRES: a generalized minimal residual algorithm for solving nonsymmetric linear systems. *SIAM J. Sci. Statist. Comput.*, 7:856–869, 1986.

[110] A. Sidi. Application of vector-valued rational approximations to the matrix eigenvalue problem and connections with Krylov subspace methods. In *Proceedings of the Cornelius Lanczos International Centenary Conference*, pages 246–248. SIAM, 1994.

[111] P. Sonneveld. CGS, a fast Lanczos-type solver for nonsymmetric linear systems. *SIAM J. Sci. Statist. Comput.*, 10:36–52, 1989.

[112] R. Souffli and G. Carayannis. A family of parallel Euclidean algorithms in linear prediction. *IEEE Trans. Sig. Proc.*, 1993.

[113] T.J. Stieltjes. Quelques recherches sur la théorie des quadratures dites mécaniques. *Ann. Aci. École Norm. Paris, Sér. 3*, 1:409–426, 1884. *Oeuvres* vol. 1, pp. 377-396.

[114] Y. Sugiyama. An algorithm for solving discrete-time Wiener-Hopf equations based upon Euclid's algorithm. *IEEE Trans. Inf. Th.*, IT-32(3):394–409, 1986.

[115] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa. A method for solving key equation for decoding goppa codes. *Information and Control*, 27:87–99, 1975.

[116] D.R. Taylor. *Analysis of the look ahead Lanczos algorithm.* PhD thesis, Center for Pure and Applied Mathematics, University of California, Berkeley, 1982.

[117] M. Van Barel. *Nested Minimal Partial Realizations and Related Matrix Rational Approximants.* PhD thesis, K.U. Leuven, January 1989.

[118] M. Van Barel, B. Beckermann, A. Bultheel, and G. Labahn. Matrix rational interpolation with poles as interpolation points. In A.M. Cuyt, editor, *Nonlinear Numerical Methods and Rational Approximation II*, pages 137–148. Kluwer, 1994.

[119] M. Van Barel and A. Bultheel. A matrix Euclidean algorithm for minimal partial realization. *Linear Algebra Appl.*, 121:674–682, 1989.

[120] M. Van Barel and A. Bultheel. A general module theoretic framework for vector M-Padé and matrix rational interpolation. *Numer. Algorithms*, 3:451–461, 1992.

[121] M. Van Barel and A. Bultheel. The "look-ahead" philosophy applied to matrix rational interpolation problems. In U. Helmke, R. Mennicken, and J. Saurer, editors, *Systems and networks: Mathematical theory and applications, Volume II: Invited and contributed papers*, volume 79 of *Mathematical Research*, pages 891–894. Akademie Verlag, 1994.

[122] M. Van Barel and A. Bultheel. A look-ahead algorithm for the solution of block Toeplitz systems. *Linear Algebra Appl.*, 1995. Submitted.

[123] M. Van Barel and A. Bultheel. A look-ahead method to compute vector Padé-Hermite approximants. *Constr. Approx.*, 11:455–476, 1995.

[124] M. Van Barel and A. Bultheel. Look ahead methods for block Hankel systems. *Linear Algebra Appl.*, 1995. Submitted.

[125] H.A. Van der Vorst. Bi-CGSTAB: a fast and smoothly converging variant of Bi-CGS for the solution of nonsymmetric linear systems. *SIAM J. Sci. Statist. Comput.*, 13:631–644, 1992.

[126] H. Viscovatoff. De la méthode générale pour réduire toutes sortes de quantités an fractions continues. *Mém. Acad. Sci. Imp. St. Pétersbourg*, 1:226–247, 1805.

[127] D.Y.Y. Yun and F.G. Gustavson. Fast computation of rational Hermite approximants and Toeplitz systems of equations via the extended Euclidean algorithm. In *Symbolic and algebraic computation*, pages 58–64. Springer, 1979. Lecture Notes in Computer Sci. 72.