



Konv.koodit

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Esimerkkejä luvusta 1, 21.11.2019-



Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Tarvittavia algebrallisia rakenteita



Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen
algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Polynomeista



Polynomirengas

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen
algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Olkoon $\mathbb{F}$ kahden alkion kunta. Siis $\mathbb{F} = \{0, 1\}$, yhteen- ja kertolasku modulo 2. Kuten Algebran PK II:lla nähtiin tuntemattoman D $\mathbb{F}$ -kertoimiset polynomit muodostavat polynomirenkaan $\mathbb{F}[D]$.

- $(1 + D) + (1 + D + D^2) = 2 + 2D + D^2 = D^2$, sillä kertoimille $1 + 1 = 2 = 0$.
- $(1 + D)(1 + D + D^2) = (1 + D + D^2) + (D + D^2 + D^3) = 1 + D^3$.
- Yleisesti voimassa "Freshman's dream"

$$(a(D) + b(D))^2 = a(D)^2 + b(D)^2$$

kaikille polynomeille $a(D), b(D) \in \mathbb{F}[D]$. Vielä yleisemmin voimassa kaikissa kommutatiivisissa renkaissa, joissa $1 + 1 = 0$.



Jaoton polynomi

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen
algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Sanotaan, että polynomi $p(D) \in \mathbb{F}[D]$ on jaoton, jos sitä ei voi kirjoittaa kahden polynomin tulona $p(D) = g(D)h(D)$ siten, että $g(D)$ ja $h(D)$ ovat molemmat vähintään astetta yksi. Jos $p(D) = g(D)h(D)$, niin sanotaan, että $g(D)$ jakaa $p(D)$:n, merkintä $g(D) \mid p(D)$.

- Astetta 1 olevat polynomit ovat jaottomia.
- $1 + D^2 = (1 + D)^2$ ei ole jaoton. $D^2 + D = D(1 + D)$ ei ole jaoton.
- Ainoa jaoton toisen asteen polynomi on $1 + D + D^2$.
- Hieman työläämpää on osoittaa, että ainoat kolmannen asteen jaottomat polynomit ovat $1 + D^2 + D^3$ ja $1 + D + D^3$.
- Jos $p(0) = 0$ niin D jakaa $p(D)$:n.
- Jos $p(1) = 0$ niin $1 + D$ jakaa $p(D)$:n. Näin käy silloin, kun $p(D)$:ssä on parillinen määrä termejä.



Tekijöihinjako

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen

algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin

normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Jokainen polynomi $p(D) \in \mathbb{F}[D]$, jonka aste on vähintään yksi, voidaan kirjoittaa jaottomien polynomien tulona.

- $1 + D + D^2 + D^3 = (1 + D) + D^2(1 + D) = (1 + D^2)(1 + D) = (1 + D)^2(1 + D) = (1 + D)^3.$
- $D + D^5 = D(1 + D^4) = D(1 + D^2)^2 = D(1 + D)^4.$
- $1 + D + D^5 = (1 + D + D^2) + (D^2 + D^5) = (1 + D + D^2) + D^2(1 + D^3) = (1 + D + D^2)(1 + D^2 + D^3).$
- Tekijöihinjako on yksikäsitteinen samassa mielessä kuin kokonaislukujen tekijöihinjako alkulukujen avulla. Todistus menee samalla tavalla kuin kokonaislukujen tapauksessa käyttämällä Eukleideen algoritmia. Algoritmista alla, mutta yksikäsitteisyystodistus sivuutetaan.



Syt (1/2)

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen

algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin

normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Sanotaan, että $d(D) = \text{syt}(a(D), b(D))$ jos $d(D)$ on korkea-asteisin polynomien $a(D)$ ja $b(D)$ yhteinen tekijä.

- Jos $d(D) \mid a(D)$ ja $d(D) \mid b(D)$, niin kaikilla polynomeilla $q(D), r(D) \in \mathbb{F}[D]$ on voimassa $d(D) \mid q(D)a(D) + r(D)b(D)$.
- Muotoa $q(D)a(D) + r(D)b(D)$ olevat polynomit muodostavat renkaan $\mathbb{F}[D]$ ihanteen. Itse asiassa kyseessä on polynomien $a(D)$ ja $b(D)$ generoima ihanne.
- Algebran PKII $\implies$ tällainen ihanne on aina yhden polynomin generoima. Ja osoittautuu (Bezout'n identiteetti), että ainoa mahdollinen generaattori on $d(D)$.



Syt (2/2)

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen
algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

- $\text{synt}(1 + D^2, 1 + D^3) = 1 + D$, sillä $(1 + D^2) = (1 + D)^2$,
 $(1 + D^3) = (1 + D)(1 + D + D^2)$, joten korkeampiasteisia
yhteisiä tekijöitä ei ole. Huomaamme, että

$$1 + D = D \cdot (1 + D^2) + 1 \cdot (1 + D^3)$$

on kuvattua muotoa.



Jakoalgoritmi

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen
algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Jos $a(D), b(D) \in \mathbb{F}[D]$ ovat mielivaltaisia, $b(D) \neq 0$, niin on olemassa yksikäsitteiset polynomit $q(D)$ (=quotient) ja $r(D)$ (=remainder), joille

$$a(D) = q(D)b(D) + r(D),$$

ja $\deg r(D) < \deg b(D)$.

Ajatus:

$$\frac{a(D)}{b(D)} = q(D) + \frac{r(D)}{b(D)},$$

missä jäännöstermissä osoittajan aste on pienempi kuin nimittäjän. Jako $a(D)/b(D)$ menee tasan, joss $r(D) = 0$.



Eukleideen algoritmi

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen
algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Jos $g(D) \mid a(D)$ ja $g(D) \mid b(D)$, niin koska

$$r(D) = a(D) - q(D)b(D),$$

voimme päätellä, että $g(D) \mid r(D)$. Kääntäen, jos $g(D) \mid r(D)$ ja $g(D) \mid b(D)$, niin $g(D) \mid a(D)$.

$$\text{synt}(a(D), b(D)) = \text{synt}(b(D), r(D)).$$

Eukleideen algoritmi perustuu tämän tuloksen käyttöön. Koska jakojäännösten asteet koko ajan pienenevät, päästään lopulta tilanteeseen, jossa $r(D) = 0$, ja algoritmi päättyy.



Esimerkki 1A

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Polynomirengas

Jaoton polynomi

Tekijöihinjako

Syt (1/2)

Syt (2/2)

Jakoalgoritmi

Eukleideen
algoritmi

Esimerkki 1A

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Lasketaan $\text{syt}(1 + D^6, 1 + D^4)$.

Ratkaisu: Koska

$$1 + D^6 = D^2 \cdot (1 + D^4) + (1 + D^2),$$

niin $\text{syt}(1 + D^6, 1 + D^4) = \text{syt}(1 + D^4, 1 + D^2)$. Koska $1 + D^2 \mid 1 + D^4$, niin $\text{syt}(1 + D^4, 1 + D^2) = 1 + D^2$.



Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Potenssisarjojen
rengas

Esimerkki 1B

Ominaisuuksia

Esimerkki 1C.1

Esimerkki 1C.2

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Potenssisarjoista



Potenssisarjojen rengas

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Potenssisarjojen
rengas

Esimerkki 1B

Ominaisuuksia

Esimerkki 1C.1

Esimerkki 1C.2

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Ns. *formaaliset potenssisarjat*

$$\sum_{n=0}^{\infty} a_n D^n, a_n \in \mathbb{F} \forall n \geq 0,$$

muodostavat renkaan $\mathbb{F}[[D]]$.

- "Formaalinen" tarkoittaa suurin piirtein sitä, ettemme lainkaan ole kiinnostuneita suppenemiskysymyksistä.
- Potenssisarjoja lasketaan yhteen kuten polynomejakin laskemalla vastinkertoimet yhteen.
- Potenssisarjoja kerrotaan kuten polynomejakin. Se onnistuu koska tulossa

$$\left(\sum_i a_i D^i\right)\left(\sum_j b_j D^j\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) D^k$$

astetta $i + j = k$ olevia termejä on kullakin k :n arvolla vain äärellinen määrä.



Esimerkki 1B

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Potenssisarjojen
rengas

Esimerkki 1B

Ominaisuuksia

Esimerkki 1C.1

Esimerkki 1C.2

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Polynomi on potenssisarja, jossa on vain äärellisen monta termiä. Voimme siis laskea esimerkiksi

$$\begin{aligned} & (1 + D) \sum_{k=0}^{\infty} D^k \\ &= (1 + D)(1 + D + D^2 + D^3 + D^4 + \dots) \\ &= 1 \cdot (1 + D + D^2 + D^3 + \dots) \\ & \quad + D \cdot (1 + D + D^2 + D^3 + \dots) \\ &= 1 + D + D^2 + D^3 + \dots \\ & \quad + 0 + D + D^2 + D^3 + \dots \\ &= 1. \end{aligned}$$



Ominaisuuksia

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Potenssisarjojen
renkas

Esimerkki 1B

Ominaisuuksia

Esimerkki 1C.1

Esimerkki 1C.2

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Potenssisarjojen renkaalla on seuraavia ominaisuuksia

- Ne muodostavat kokonaisalueen, eli kommutatiivisen renkaan, jossa ei ole nollanjakajia.
- Potenssisarjalla $\sum_{n=0} a_n D^n$ on käänteisalkio renkaassa $\mathbb{F}[[D]]$ jos ja vain jos $a_0 = 1$. Esimerkin 1B lasku osoittaa, että potenssisarja $1 + D + D^2 + D^3 + \dots$ ja polynomi $1 + D$ ovat toistensa käänteisalkioita. Vertaa tätä geometrisen sarjan summakaavaan

$$1 + D + D^2 + D^3 + \dots = \frac{1}{1 - D} = \frac{1}{1 + D},$$

koska karakteristika 2 renkaassa $-D = +D$.

- Potenssisarjojen renkaan ihanteet ovat alkioiden $D^k, k \geq 0$, generoimat ihanteet. Erityisesti ainoat "jaottomat" potenssisarjat ovat D :n potensseja. Tätä emme juurikaan tarvitse, mutta se tulee vastaan mm. *kommutatiivisessa algebrassa*.



Esimerkki 1C.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Potenssisarjojen
renkas

Esimerkki 1B

Ominaisuuksia

Esimerkki 1C.1

Esimerkki 1C.2

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Etsitään potenssisarjan $(1 + D + D^2 + D^3)$ käänteisalkio renkassa $\mathbb{F}[[D]]$.

Ratkaisu: Tässä $(1 + D + D^2 + D^3) = (1 + D)^3$, joten

$$(1 + D + D^2 + D^3)(1 + D) = 1 + D^4.$$

Geometrisen sarjan summakaavalla saamme

$$\frac{1}{1 + D^4} = 1 + D^4 + D^8 + D^{12} + \dots = \sum_{n=0}^{\infty} D^{4n}.$$



Esimerkki 1C.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Potenssisarjojen
rengas

Esimerkki 1B

Ominaisuuksia

Esimerkki 1C.1

Esimerkki 1C.2

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Kertomalla tämä yhtälö polynomilla $1 + D$ saamme tuloksen

$$\begin{aligned}\frac{1}{1 + D + D^2 + D^3} &= \frac{1 + D}{1 + D^4} \\ &= (1 + D) \cdot \sum_{n=0}^{\infty} D^{4n} \\ &= (1 + D) + (D^4 + D^5) + (D^8 + D^9) + \dots \\ &= \sum_{n=0}^{\infty} a_n D^n,\end{aligned}$$

missä $a_n = 1$, jos $n \equiv 0 \pmod{4}$ tai $n \equiv 1 \pmod{4}$, ja $a_n = 0$, jos $n \equiv 2 \pmod{4}$ tai $n \equiv 3 \pmod{4}$.



Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Smithin normaalimuoto



Mitä?

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?

Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Oletetaan, että A on $k \times n$ -matriisi, $k < n$, jonka alkiot ovat polynomeja $\in \mathbb{F}[D]$. Tällöin on olemassa sellaiset matriisit $P \in M_{k \times k}(\mathbb{F}[D])$ ja $Q \in M_{n \times n}(\mathbb{F}[D])$, että

- $\det P = 1 = \det Q$,
- $PAQ = \text{diag}_{k \times n}(d_1(D), d_2(D), \dots, d_k(D))$,
- ja $d_i(D) \mid d_{i+1}(D)$ kaikilla i :n arvoilla.



Invariantit tekijät

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?

Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Tässä esiintyvät polynomit $d_i(D)$, $i = 1, 2, \dots, k$, ovat matriisin A *invariantit tekijät*.

- $d_1(D)$ on matriisin A alkioden $a_{ij}(D)$ syt (renkaassa $\mathbb{F}[D]$),
- $d_1(D)d_2(D)$ on matriisin A 2×2 -alideterminanttien syt,
- $d_1(D)d_2(D)d_3(D)$ on matriisin A 3-rivisten alideterminanttien syt, jne.



Miksi?

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

- Tehdään matriisille sellaisia alkeismuunnoksia (riveille tai sarakkeille!), jotka ovat polynomikertoimisia ja kääntyviä (eli riviin tai sarakkeeseen voidaan lisätä toinen rivi/sarake polynomilla kerrottuna, tai vaihdetaan kaksi riviä/saraketta keskenään), niin uuden matriisin alkiot ovat vanhan polynomikertoimisia lineaarikombinaatioita.
- Näin ollen kääntyvässä alkeismuunnoksessa alkioden syt säilyy (vanha yhteinen tekijä jakaa uudet alkiot, koska muunnos oli kääntyvä sama on voimassa myös kääntäen).
- Sama havainto koskee tiettyä kokoa olevia alideterminantteja.
- Jos diagonalisointi onnistuu, niin invarianttien tekijöiden tulkinta alideterminanttien syttinä seuraa tästä.



Miten?

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät
Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

- Vaakarivimuunnosten sarjalla voidaan tuottaa matriisi, jossa esiintyy kahden samalla sarakkeella olevan polynomin syt.
- Sarakemuunnoksilla saadaan aikaan kahden samalla rivillä olevan polynomin syt.
- Tekemällä sopivia muunnoksia saadaan siis aikaan kaikkien alkioden syt, ja siirrettyä se vasempaan ylänurkkaan.
- Tämän jälkeen voidaan muut alkiot 1. rivillä ja 1. sarakkeessa nollata alkeismuunnoksilla.
- Sen jälkeen unohdetaan 1. rivi/sarake, ja käsitellään jäljellä olevaa matriisia. Sen alkioden syt saadaan samaan tapaan jäljellä olevan lohkon vasempaan ylänurkkaan (paikkaan $(2, 2)$), jne.



Esimerkki 1D.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät

Miksi?
Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Määrätään matriisin

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & D & D^2 \\ 1 & D^2 & D^4 \end{pmatrix}$$

invariantit tekijät, ja vastaavat matriisit P ja Q .

Ratkaisu: Selvästi matriisin A alkioden $\text{synt} = 1$, joten alkioden synt on jo positiossa $(1, 1)$. Lisäämällä 1. vaakarivi toiseen ja kolmanteen saadaan 1. vaiheessa 1. sarake kuntoon

Esimerkki 1D.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?

Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

$$\rightarrow \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 + D & 1 + D^2 \\ 0 & 1 + D^2 & 1 + D^4 \end{pmatrix}.$$

Seuraavaksi hoidetaan 1. rivi kuntoon lisäämällä 1. sarake toiseen ja kolmanteen

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 + D & 1 + D^2 \\ 0 & 1 + D^2 & 1 + D^4 \end{pmatrix}.$$

Huomaamme seuraavaksi, että oikean alanurkan 2×2 -lohkon kaikki alkiot ovat jaollisia polynomilla $1 + D$, mikä on niiden syt. Koska kyseinen polynomi on jo positiossa $(2, 2)$, niin siirrymme toisen sarakkeen käsittelyyn.

$(1 + D^2)/(1 + D) = 1 + D$, joten lisätään 2. rivi kolmanteen kerrottuna polynomilla $1 + D$.



Esimerkki 1D.3

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?

Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 + D & 1 + D^2 \\ 0 & 0 & D + D^2 + D^3 + D^4 \end{pmatrix}.$$

Seuraavaksi lisätään 2. saraka kolmanteen kerrottuna polynomilla $1 + D$, jolloin myös 2. rivi tulee valmiiksi

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 + D & 0 \\ 0 & 0 & D + D^2 + D^3 + D^4 \end{pmatrix}.$$



Esimerkki 1D.4

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

1. vaiheessa kerroimme matriisin A vasemmalta matriisilla

$$P_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

kolmannessa vaiheessa puolestaan kerroimme vasemmalta matriisilla

$$P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 + D & 1 \end{pmatrix}.$$



Esimerkki 1D.5

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Muista, että rivimuunnoksessa kerrotaan vasemmalta alkeismatriisilla, ja sarakemuunnoksessa puolestaan oikealta. Kaiken kaikkiaan laskun aikana matriisi A kerrottiin vasemmalta matriisilla

$$P = P_2 P_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ D & 1 + D & 1 \end{pmatrix}.$$

Toisessa vaiheessa kerroimme matriisin A oikealta alkeismatriisilla

$$Q_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$



Esimerkki 1D.5

ja viimeisessä vaiheessa puolestaan alkeismatriisilla

$$Q_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 + D \\ 0 & 0 & 1 \end{pmatrix},$$

joten kaiken kaikkiaan oikealta kerrottiin matriisilla

$$Q = Q_1 Q_2 = \begin{pmatrix} 1 & 1 & D \\ 0 & 1 & 1 + D \\ 0 & 0 & 1 \end{pmatrix}.$$

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi



Esimerkki 1D.5

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Harjoitustehtävän voit tarkistaa, että

$$PAQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 + D & 0 \\ 0 & 0 & D + D^2 + D^3 + D^4 \end{pmatrix}.$$

Huomaa alkeismatriisien järjestys tuloissa:

- Rivimuunnokset vaikuttavat matriisiin P , joka muodostuu rivimuunnoksia vastaavien alkeismatriisien tulona, ensin tehty muunnos tulossa oikealla.
- Sarakemuunnokset vaikuttavat matriisiin Q , joka saadaan sarakemuunnoksia vastaavien alkeismatriisien tulona, ensin tehty muunnos tulossa vasemmalla.



Esimerkki 1E.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?

Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Määrätään matriisin

$$B = \begin{pmatrix} 1 & 1 + D + D^2 & 1 + D^2 & 1 + D \\ D & 1 + D + D^2 & D^2 & 1 \end{pmatrix}$$

invariantit tekijät.

Ratkaisu: Jälleen matriisin alkioden $\text{synt} = 1$, mikä on sopivasti positiossa $(1, 1)$. Ilmeinen vaakarivimuunnos tuottaa matriisin

$$\rightarrow \begin{pmatrix} 1 & 1 + D + D^2 & 1 + D^2 & 1 + D \\ 0 & 1 + D^3 & D + D^2 + D^3 & 1 + D + D^2 \end{pmatrix}.$$



Esimerkki 1E.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät
Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Ilmeiset sarakemuunnokset johtavat sitten matriisiin

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 + D^3 & D + D^2 + D^3 & 1 + D + D^2 \end{pmatrix}.$$

Tarkastellaan jäljellä olevaa 1×3 lohkoa. Ensimmäistä kertaa meillä ei ole näiden kolmen polynomin syttiä valmiina lohkon vasemmassa ylänurkassa. Aletaan laskea polynomien $1 + D^3$ ja $1 + D + D^2 + D^3$ syttiä sarakemuunnoksia tekemällä.



Esimerkki 1E.3

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Mitä?
Invariantit
tekijät

Miksi?

Miten?

Esimerkki 1D.1

Esimerkki 1D.2

Esimerkki 1D.3

Esimerkki 1D.4

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1D.5

Esimerkki 1E.1

Esimerkki 1E.2

Esimerkki 1E.3

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Lisäämällä 3. sarake toiseen, saadaan polynomista $1 + D^3$ poistettua kolmannen asteen termi:

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 + D + D^2 & D + D^2 + D^3 & 1 + D + D^2 \end{pmatrix}.$$

Tässä vaiheessa huomaamme, että toisen rivin kaikki polynomit ovat jaollisia position $(2, 2)$ polynomilla $1 + D + D^2$, joten ko. polynomien on oltava etsitty syt. Nollaamme 2. rivin myöhemmät alkiot ilmeisillä sarakemuunnoksilla

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 + D + D^2 & 0 & 0 \end{pmatrix}.$$



Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Määritelmä

Vapaa etäisyys

Esimerkki 1F.1

Esimerkki 1F.2

Generaattorin
valinnasta

Optimaalinen
koodi

Käsitteitä



Määritelmä

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Määritelmä

Vapaa etäisyys

Esimerkki 1F.1

Esimerkki 1F.2

Generaattorin
valinnasta

Optimaalinen
koodi

Sanomme, että (n, k) -konvoluutiokoodi on sellainen vektoriavaruuden $\mathbb{F}((D))^n$ k -ulotteinen aliavaruus, jolla on kanta, jonka alkioden kaikki komponentit ovat polynomeja.

- Monisteessa selitetään, miten määritelmä tila-avaruuden avulla johtaa siihen, että tällainen kanta löytyy $\mathbb{F}((D))$ -avaruudelle.
- Tämän vuoksi konvoluutiokoodiin liittyy yksikäsitteinen $\mathbb{F}(D)$ -aliavaruus.
- Myöhemmin näemme, miten tästä määritelmästä päädytään tapaan määritellä konvoluutiokoodi tila-avaruuden kautta. Sen jälkeen tiedämm, että määritelmät ovat ekvivalentit.



Vapaa etäisyys

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Määritelmä

Vapaa etäisyys

Esimerkki 1F.1

Esimerkki 1F.2

Generaattorin
valinnasta

Optimaalinen
koodi

Määritelmistämme seuraa, että (n, k) konvoluutiokoodissa esiintyy vektoreita, joiden kaikki komponentit ovat polynomeja.

- Sanotaan, että polynomin $\in \mathbb{F}[D]$ Hamming paino on sen nollasta eroavien termien lukumäärä.
- Yleistetään tämä vektoreille $\in \mathbb{F}[D]^n$ laskemalla yhteen komponenttipolynomien painot.
- (n, k) -konvoluutiokoodin *vapaa etäisyys* on pienin nollasta eroava koodisanan paino.
- Joukon $\mathbb{F}[[D]] \setminus \mathbb{F}[D]$ alkiot ovat ääretöntä painoa.
- Konvoluutiokoodin vapaa etäisyys on jonkinlainen mittari sen virheenkorjauskyvystä (mutta ei aivan niin keskeisessä roolissa kuin lohkokoodien puolella).



Esimerkki 1F.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Määritelmä
Vapaa etäisyys

Esimerkki 1F.1

Esimerkki 1F.2

Generaattorin
valinnasta

Optimaalinen
koodi

Näimme, että monisteen johdannon $(2, 1)$ -esimerkkikoodiin kuuluu sana $G(D) = (1 + D^2, 1 + D + D^2)$, mikä vastaa syötettä $u(D) = 1$ (eli $u(0) = 1$ ja muut syötebitit nolliä). Näin ollen $G(D)$ on kyseisen koodin eräs polynomiaalinen generaattorimatriisi. Osoitetaan sen avulla, että tämän koodin vapaa etäisyys $d = 5$.

Ratkaisu: Generaattorimatriisin ainoan vaakarivin paino on viisi, joten vapaa etäisyys ei voi olla > 5 . Oletetaan $\mathbf{x}(D) = (x_1(D), x_2(D)) = u(D)G(D)$ on pienipainoisin sana. Ensimmäinen havainto, jonka teemme on, että generaattorimatriisin alkioden summa on $(1 + D^2) + (1 + D + D^2) = D$. Näin ollen

$$x_1(D) + x_2(D) = Du(D).$$



Esimerkki 1F.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Määritelmä

Vapaa etäisyys

Esimerkki 1F.1

Esimerkki 1F.2

Generaattorin
valinnasta

Optimaalinen
koodi

Koska $x_1(D) + x_2(D)$ polynomina on äärellistä painoa, tästä seuraa, että syöte $u(D)$ on sekin äärellistä painoa. Syötteen kertominen D :n potenssilla ainoastaan liikuttaa koodisanaa pitkin aika-akselia muuttamatta sen painoa, joten rajoituksetta voimme olettaa, että $u(D)$ on polynomi, jonka vakiotermi on 1.

Tällöin $x_1(D) = (1 + D^2)u(D)$ ja $x_2(D) = (1 + D + D^2)u(D)$. Jos $u(D)$ on astetta $j \geq 0$, niin tuloissa $(1 + D^2)u(D)$ ja $(1 + D + D^2)u(D)$ on molemmissa väistämättä asteita 0 ja $j + 2$ vastaavat termit, yhteensä siis vähintään 4 termiä. Lisäksi jommassa kummassa on jokin muu termi, koska $(1 + D^2)u(D) \neq (1 + D + D^2)u(D)$. Näin ollen koodisanan $\mathbf{x}(D)$ paino on vähintään viisi.



Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Generaattorin valinnasta



Yleistä

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

- Kuten lohkokoodinkin tapauksessa generaattorimatriisilla on useita valintoja, koska *koodi* = *generaattorimatriisin vaakariviavaruus*.
- Myöhemmin saadaan "teknisiä" selityksiä sille, miksi meidän on syytä preferoida sellaista generaattorimatriisia, jossa esiintyy mahdollisimman matala-asteisia polynomeja.
- Saman (n, k) -konvoluutiokoodin eri generaattorimatriiseja verrataan toisiinsa käyttäen kahta eri tapaa mitata niiden "kompleksisuutta". Voimme yrittää pienentää k -rivisten alideterminanttien syttejä, tai rivien maksimiasteiden summaa. Tai itse asiassa molempia.

Seuraavan esimerkin (monisteen Esimerkki 1.5) on tarkoitus johdatella tavoiteltaviin ominaisuuksiin, ja havainnollistaa esiintyviä mahdollisuuksia. Huomaa, että koska emme halua muuttaa koodia (=vaakariviavaruutta), niin voimme käyttää vain vaakarivimuunnoksia.



Esimerkki 1G.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Yritetään yksinkertaistaa Esimerkissä 1E esiintynyttä $(4, 2)$ -konvoluutiokoodin polynomiaalista generaattorimatriisia mahdollisimman pitkälle

$$G_1 = \begin{pmatrix} 1 & 1 + D + D^2 & 1 + D^2 & 1 + D \\ D & 1 + D + D^2 & D^2 & 1 \end{pmatrix}.$$

Ratkaisu: Huomaamme, että matriisin G_1 kummallakin vaakarivillä korkeimman asteiset termit esiintyvä sarakkeissa 2 ja 3. Näin ollen eräs ilmeinen yksinkertaistus olisi lisätä 1. rivi jälkimmäiseen. Tämän rivioperaation seurauksena saadaan matriisi

$$G_2 = \begin{pmatrix} 1 & 1 + D + D^2 & 1 + D^2 & 1 + D \\ 1 + D & 0 & 1 & D \end{pmatrix}.$$



Esimerkki 1G.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Mutta tämäntyyppinen rivioperaatio ei muuta matriisin invariantteja tekijöitä. Esimerkin 1E laskun inspiroimana voisimme ensin lisätä 1. rivin toiseen kerrottuna D :llä. Näimme, että sen jälkeen 2. rivin alkiot olivat kaikki jaollisia polynomilla $1 + D + D^2$. Kun jaamme tämän yhteisen tekijän pois ko. rivistä saamme toisenlaisen yksinkertaisemman matriisin

$$G_3 = \begin{pmatrix} 1 & 1 + D + D^2 & 1 + D^2 & 1 + D \\ 0 & 1 + D & D & 1 \end{pmatrix}.$$

Tärkeää: Määrittelimme konvoluutiokoodin generaattorimatriisin rivien generoimaksi $\mathbb{F}(D)$ -avaruudeksi. Koska $1/(1 + D + D^2)$ on kerroinkunnan alkio (ja kääntyvä), sillä kertominen ei muuta matriisin vaakariviavaruutta.



Esimerkki 1G.3

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Huomaamme, että ensimmäiseksi bongaamamme temppu on käytettävissä myös matriisissa G_3 . Voimme pienentää 1. rivin astetta lisäämällä siitä 2. rivin kerrottuna polynomilla D . Sen jälkeen meillä onkin alkuperäistä huomattavasti yksinkertaisempi matriisi

$$G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 + D & D & 1 \end{pmatrix}.$$



Määritelmiä

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaaliomuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Olkoon $\mathcal{C}$ jokin (n, k) koodi, ja $G(D)$ sen polynomiaalinen generaattorimatriisi.

- Matriisin $G(D)$ *sisäinen aste* on korkein sen $k \times k$ -alideterminanttien asteista.
- Matriisin $G(D)$ *ulkoinen aste* on sen vaakariviasteiden summa.
- Matriisi $G(D)$ on *basic*, jos sen sisäistä astetta ei voi pienentää kertomalla sitä $\mathbb{F}(D)$ -kertoimisella matriisilla (tulokseksi pitää tulla polynomimatriisi)
- Matriisi $G(D)$ on *reduced*, jos sen ulkoista astetta ei voi pienentää tekemällä siihen $\mathbb{F}[D]$ -kertoimisia vaakarivimuunnoksia.



Havaintoja

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

- Koska konvoluutiokoodi voidaan ajatella vektoriavaruudeksi yli kunnan $\mathbb{F}(D)$, kaikki sen generaattorimatriisit saadaan toisistaan kertomalla vasemmalta $\mathbb{F}(D)$ -kertoimisilla matriisilla. Näin ollen basic -matriiseilla on kaikilla sama sisäinen aste.
- Jokainen unimodulaarinen ($\det = 1$) polynomiaalinen $k \times k$ matriisi saadaan muutettua identiteettimatriisiksi $\mathbb{F}[D]$ -kertoimisilla, joten reduced-ominaisuuden testaamiseen voidaan käyttää kaikkia unimodulaarimatriiseja alkeismatriisien asemesta. Perustelu: Unimodulaarimatriisin 1. sarakkeen alkioiden $\text{synt} = 1$ (kyseinen synt on selvästi determinantin tekijä), joten vaakarivimuunnoksilla siihen saadaan 1, ja sen jälkeen $k - 1$ nollaa. Induktio hoitaa loput.



Basic

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Monisteen Theorem 1.2:n nojalla polynomimatriisin $G(D)$ *Basic*-ominaisuus on ekvivalentti usean testin kanssa:

- Invariantit tekijät kaikki ykkösiä.
- $k \times k$ -alideterminanttien $\text{synt} = 1$.
- On olemassa oikeanpuoleinen polynomiaalinen käänteismatriisi $H(D)$, jolle $G(D)H(D) = I_k$.
- *Poly out – poly in*-ominaisuus: jos $\mathbf{x}(D) = \mathbf{u}(D)G(D) \in \mathbb{F}[D]^n$, niin $\mathbf{u}(D) \in \mathbb{F}[D]^k$.
- $G(D)$ voidaan täydentää unimodulaariseksi $n \times n$ -matriisiksi.

Detaljoitnut todistukset näille löytyvät monisteesta. Valoitan yhteyksiä esimerkeillä, koska ne eräissä tapauksissa ovat valaisevampia kuin notationaalisesti hankala todistus.



Esimerkki 1H.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Esimerkin 1G matriisi

$$G_3 = \begin{pmatrix} 1 & 1 + D + D^2 & 1 + D^2 & 1 + D \\ 0 & 1 + D & D & 1 \end{pmatrix}$$

on basic, koska sen sarakkeiden 1. ja 2. muodostamalla alideterminantilla $1 + D$ ei ole yhteisiä tekijöitä 1. j 3.

sarakkeen muodostaman alideterminantin D kanssa.

Konstruoimme näiden tietojen avulla sille polynomiaalisen oikeanpuoleisen käänteismatriisin.

Ratkaisu: Muistamme lineaarialgebrasta 2×2 -matriiseja koskevan tuloksen

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (ad - bc)I_2.$$



Esimerkki 1H.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Sen avulla saamme vastaaville "osamatriiseille" vakiokerrointa vaille käänteismatriisit:

$$\begin{pmatrix} 1 & 1 + D + D^2 \\ 0 & 1 + D \end{pmatrix} \begin{pmatrix} 1 + D & 1 + D + D^2 \\ 0 & 1 \end{pmatrix} = (1 + D)I_2,$$

ja

$$\begin{pmatrix} 1 & 1 + D^2 \\ 0 & D \end{pmatrix} \begin{pmatrix} D & 1 + D^2 \\ 0 & 1 \end{pmatrix} = DI_2.$$

Koska 1 voidaan esittää (Bezout) polynomien $1 + D$ ja D polynomikertoimisena lineaarikombinaationa

$$1 \cdot (1 + D) + 1 \cdot D = 1,$$



Esimerkki 1H.3

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

saamme oikeanpuoleisen käänteismatriisin (joka on 4×2 vastaavana osittaisten käänteismatriisien lineaarikombinaationa. Huomaa, että siirrämme yo. osittaiset käänteismatriisit käytettyjä sarakkeita vastaaville riveille:

$$H(D) = 1 \cdot \begin{pmatrix} 1 + D & 1 + D + D^2 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} D & 1 + D^2 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

eli

$$H(D) = \begin{pmatrix} 1 & D \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Tarkista kertomalla :-)



Esimerkki 1I.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Kansikuvakoodilla on generaattorimatriisi

$G(D) = (1 + D^2 \ 1 + D + D^2)$. Täydennetään se unimodulaarimatriisiksi, tuotetaan sen avulla oikeanpuoleinen polynomiaalinen käänteismatriisi $H(D)$ ja osoitetaan, että tätä generaattorimatriisia käytettäessä PolyOut–PolyIn-ominaisuus on voimassa.

Ratkaisu: Matriisin $G(D)$ alkioiden $\text{syk} = 1$. Eukleideen algoritmilla löydetään sopiva Bezout'n identiteetti

$$1 = (1 + D) \cdot (1 + D^2) + D(1 + D + D^2).$$



Esimerkki 1I.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

2×2 -matriisin tapauksessa (yleisemmin joudumme käyttämään Smithin normaalimuotoa tässä vaiheessa) tämä kertoo heti, että matriisi

$$U(D) = \begin{pmatrix} 1 + D^2 & 1 + D + D^2 \\ D & 1 + D \end{pmatrix}$$

on unitaarinen. Näin ollen sillä on polynomiaalinen käänteismatriisi, mikä tutun kaavan (vrt. Esimerkki 1H) nojalla on

$$U(D)^{-1} = \begin{pmatrix} 1 + D & 1 + D + D^2 \\ D & 1 + D^2 \end{pmatrix}.$$

Bongaamalla matriisikertolaskusta $U(D)U(D)^{-1} = I_2$ vain tulon paikkaa $(1, 1)$ koskeva kertolasku, saamme



Esimerkki 1I.3

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

$$\begin{pmatrix} 1 + D^2 & 1 + D + D^2 \end{pmatrix} \begin{pmatrix} 1 + D \\ D \end{pmatrix} = (1),$$

eli saimme tätäkin kautta oikeanpuoleisen käänteismatriisin $H(D) = (1 + D \ D)^T$.

Jos koodisana $\mathbf{x}(D) = (x_1(D), x_2(D)) = u(D)G(D) \in \mathbb{F}[D]^2$ on polynomiaalinen, niin kertomalla puolittain oikealta $H(D)$:llä saamme

$$\begin{aligned} u(D) &= u(D) \cdot 1 = u(D)G(D)H(D) \\ &= \mathbf{x}(D)H(D) = (1 + D)x_1(D) + Dx_2(D), \end{aligned}$$

mikä on selvästi polynomi.



Reduced

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Polynomiaallinen generaattorimatriisi $G(D)$ on reduced, jos jokin seuraavista ekvivalenteista ehdoista toteutuu

- Matriisin $G(D)$ sisäinen ja ulkoinen aste yhtyvät.
- Matriisilla $G(D)$ on ns. *ennustetun asteen ominaisuus*: Jos matriisin $G(D)$ vaakarivien asteet ovat $e_1, e_2, \dots, e_k$, ja $\mathbf{u}(D) = (u_1(D), \dots, u_k(D)) \in \mathbb{F}[D]^k$, missä $f_i = \deg u_i(D)$, niin koodisanan $\mathbf{x}(D) = \mathbf{u}(D)G(D)$ korkea-asteisimman komponentin aste $= \max_{1 \leq i \leq k} (e_i + f_i)$.
- Jos merkitään $\overline{G}$:llä matriisia $\in M_{k \times n}(\mathbb{F})$, jossa vaakarivin i alkiot ovat matriisin $G(D)$ kyseisen rivin alkioden (maksimaalista) astetta e_i olevien termien kertoimet, niin $\overline{G}$ on täysiasteinen (eli sen vaakarivit ovat lineaarisesti riippumattomia yli kunnan $\mathbb{F}$).



Esimerkki 1J.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Jos

$$G(D) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ D & 0 & 1 + D & 1 \\ D & D^2 & 1 + D + D^2 & 1 \end{pmatrix},$$

niin vaakarivein asteet ovat $e_1 = 0$, $e_2 = 1$ ja $e_3 = 2$. Näin ollen

$$\overline{G} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$



Esimerkki 1J.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Matriisin $\overline{G}$ viimeinen vaakarivi on kahden ensimmäisen summa, joten tämä ei ole täysiasteinen. Näin ollen $G(D)$ ei ole reduced. Hyödyntämällä tätä lineaarista riippuvuutta voimmekin alentaa $G(D)$:n ulkoista astetta lisäämällä 1. rivin viimeiseen kerrottuna D^2 :lla ja 2. rivin viimeiseen D :llä kerrottuna:

$$\rightarrow \begin{pmatrix} 1 & 1 & 0 & 0 \\ D & 0 & 1+D & 1 \\ D & 0 & 1 & 1+D \end{pmatrix}.$$



Kanoninen

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

(n, k) -konvoluutiokoodin $\mathcal{C}$ polynomiaalista generaattorimatriisia sanotaan *kanoniseksi*, jos sen ulkoinen aste on mahdollisimman pieni

- Monisteessa todistetaan, että matriisi on kanoninen, jos se on sekä reduced että basic.
- Monisteessa todistetaan, että kaikilla koodin $\mathcal{C}$ kanonisilla generaattorimatriiseilla on (järjestystä vaille) samat vaakariviasteet, joita lähteeni kirjoittaja Robert McEliece nimesi *Forneyn indekseiksi*.



Esimerkki 1K

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Yleistä

Esimerkki 1G.1

Esimerkki 1G.2

Esimerkki 1G.3

Määritelmiä

Havaintoja

Basic

Esimerkki 1H.1

Esimerkki 1H.2

Esimerkki 1H.3

Esimerkki 1I.1

Esimerkki 1I.2

Esimerkki 1I.3

Reduced

Esimerkki 1J.1

Esimerkki 1J.2

Kanoninen

Esimerkin 1G matriiseista ainoastaan G_4 on kanoninen.

- G_1 ei ole basic, koska $1 + D + D^2$ on sen invariantti tekijä. Se ei ole myöskään reduced, koska ulkoinen aste pieneni muunnoksessa $G_1 \rightarrow G_2$.
- Matriisi G_2 on reduced sillä $\overline{G_2}$ on täysiasteinen, mutta ei basic, sillä sen invariantit tekijät ovat samat kuin G_1 :n.
- Matriisi G_3 on basic, koska invariantti tekijä $1 + D + D^2$ jaettiin pois. Se ei ole reduced, sillä muunnos $G_3 \rightarrow G_4$ pienensi sen ulkoista astetta.



Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Esimerkki 1J.1

Esimerkki 1J.2

Esimerkki 1J.3

Optimaalinen koodi



Esimerkki 1J.1

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Esimerkki 1J.1

Esimerkki 1J.2

Esimerkki 1J.3

Osoitetaan, että generaattorimatriisi

$$G(D) = (1 + D^2, 1 + D^2, 1 + D + D^2, 1 + D + D^2, 1 + D + D^2)$$

generoiman $(5, 1)$ -koodin $\mathcal{C}$ vapaa etäisyys on 13. Osoitetaan lisäksi, että minkä tahansa $(5, 1, 2)$ -koodin vapaa etäisyys on $d \leq 13$ (eli $\mathcal{C}$ on optimaalinen).

Ratkaisu: Koska $\text{syt}(1 + D^2, 1 + D + D^2) = 1$, niin $G(D)$ on basic. Triviaalisti $\overline{G}$ on astetta yksi, joten se on myös reduced, ja siis kanoninen. Koodisana $G(D) = 1 \cdot G(D)$ on painoa 13, joten $d \leq 13$.

Olkkoon $\mathbf{x}(D)$ minimipainoinen koodisana. Rajoituksetta voimme olettaa, että $\mathbf{x}(D)$:n komponentit ovat polynomeja. PolyOut–PolyIn -ominaisuuden nojalla $u(D) \in \mathbb{F}[D]$.



Esimerkki 1J.2

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Esimerkki 1J.1

Esimerkki 1J.2

Esimerkki 1J.3

Merkitään komponenttien painoja $a = w((1 + D^2)u(D))$ ja $b = w((1 + D + D^2)u(D))$, jolloin $w(\mathbf{x}(D)) = 2a + 3b$. Kuten Esimerkissä 1F näemme, että $a \geq 2$, $b \geq 2$ ja lisäksi ainakin toinen ≥ 3 .

- Jos $b \geq 3$, niin $2a + 3b \geq 4 + 9 = 13$, ja tämä tapaus on käsitelty.
- Jos $b = 2$, niin $a \geq 3$. Toisaalta $D = 1$ on polynomin $1 + D^2$ nollakohta. Näin ollen se on myös polynomin $(1 + D^2)u(D)$ nollakohta. Tämä tarkoittaa sitä, että a on välttämättä parillinen. Näin ollen $a \geq 4$ ja edelleen $2a + 3b \geq 8 + 6 = 14$. Ensimmäinen väite on todistettu.



Esimerkki 1J.3

Konv.koodit

Tarvittavia
algebrallisia
rakenteita

Polynomeista

Potenssisarjoista

Smithin
normaalimuoto

Käsitteitä

Generaattorin
valinnasta

Optimaalinen
koodi

Esimerkki 1J.1

Esimerkki 1J.2

Esimerkki 1J.3

Koodin $\mathcal{C}$ optimaalisuus seuraa kun osoitamme, ettei sellaista astetta 2 olevaa generaattorimatriisia $G(D)$ ole, joka generoisi koodin, jonka vapaa etäisyys ≥ 14 . Matriisin $G(D)$ paino on enintään $3 \cdot 5$. Se ei voi olla tasan 15, sillä silloin olisi

$$G(D) = (1+D+D^2, 1+D+D^2, 1+D+D^2, 1+D+D^2, 1+D+D^2),$$

mikä ei ole kanoninen (ja $(1, 1, 1, 1, 1)$ kuuluu ko. matriisin generoimaan koodiin). Jäljelle jää vaihtoehto, jossa 4 komponenteista on $1 + D + D^2$ ja viides jokin astetta 2 oleva binomi. Koska $(1 + D)(1 + D + D^2) = 1 + D^3$, niin sanan $(1 + D)G(D)$ komponenteista neljä on $1 + D^3$ ja painoa 2. Viides komponentti on astetta ≤ 3 eli painoa ≤ 4 . Näin ollen $w((1 + D)G(D)) \leq 4 + 4 \cdot 2 = 12$, ja väite seuraa.