Title

Decomposition of nonnegative singular matrices into product of nonnegative idempotent matrices

Title

Decomposition of nonnegative singular matrices into product of nonnegative idempotent matrices and mORE...(skew) codes.

ALGEBRAIC METHODS IN CODING THEORY

Ubatuba July 2017

Pioneers

- J.M.Howie (1966) The maps from a finite set to itself that are not onto can be presented as products of idempotents.
- J.A. Erdos (1968): singular matrices over fields.
- J. Laffey (1983): singular matrices over commutative euclidean domains.
- Hannah and O'Meara decomposition of some elements in a von Neumann ring into product of idempotent elements.
- Bhaskara Rao (2009) considered matrices over commutative PID's.
- W. Ruitenberg (1993) Matrices over Hermite domains.
- There are connections between decompositions into products of idempotents and factorizations of invertible matrices into product of elementary matrices. (Facchini-Leroy(2016), Salce-Zanardo,...)

Examples and particular decompositions

Examples

(a) $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 0 \end{pmatrix}.$

Examples and particular decompositions

Examples

(a) $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 0 \end{pmatrix}.$

(a') $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$

Examples and particular decompositions

Examples

(a) $$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 0 \end{pmatrix}.$$

(a') $$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

(b) $$\begin{pmatrix} a & ac \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1+c \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1-ca+c & c-cac+c^2 \\ a-1 & ac-c \end{pmatrix}.$$

Examples and particular decompositions

Examples

(a) $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 0 \end{pmatrix}.$

(a') $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$

(b) $\begin{pmatrix} a & ac \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1+c \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1-ca+c & c-cac+c^2 \\ a-1 & ac-c \end{pmatrix}.$

(c) $\begin{pmatrix} ac & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix},$

Examples and particular decompositions

Examples

(a) $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 0 \end{pmatrix}$.

(a') $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$.

(b) $\begin{pmatrix} a & ac \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1+c \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1-ca+c & c-cac+c^2 \\ a-1 & ac-c \end{pmatrix}$.

(c) $\begin{pmatrix} ac & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix}$,

(d) with $b \in U(R)$, $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b(b^{-1}a) & b \\ 0 & 0 \end{pmatrix}$ is factorized as in (c).

Particular matrices

Theorem

(a) If R is a ring and $A \in M_n(R)$ is strictly upper triangular then A is a product of idempotent matrices.

(b) If $n > 1$ and a matrix $A \in M_n(\mathbb{R})$ (resp. $A \in M_n(\mathbb{R}^+)$) has only one nonzero row, then it is a product of (resp. nonnegative) idempotent matrices.

Question and particular matrices

Question

Main Question : Can real **nonnegative** singular matrices be decomposed into product of **nonnegative** idempotents ?

Question and particular matrices

Question

Main Question : Can real **nonnegative** singular matrices be decomposed into product of **nonnegative** idempotents ?

Lemma (Particular matrices)

(a) If $B \in M_{n\times n}(\mathbb{R}^+)$ is an $n \times n$ matrix which is a product of nonnegative idempotents, then the same is true for the matrix $\begin{pmatrix} B & C \\ 0 & 0 \end{pmatrix}$ where $C \in M_{n\times 1}(\mathbb{R})$ (resp. $C \in M_{n\times 1}(\mathbb{R}^+)$) and the other blocks are of appropriate sizes.

(b) If $A \in M_n(\mathbb{R})$ (resp. $A \in M_n(\mathbb{R}^+)$), $n \geq 3$, has all its i^{th} rows and columns zero whenever $i \geq 3$, then A is a product of (resp. nonnegative) idempotent matrices.

Rank one

Proposition

Let $A \in M_n(\mathbb{R}^+)$, $n > 1$, be a nonnegative matrix of rank 1. Then A is a product of nonnegative idempotent matrices.

Rank one

Proposition

Let $A \in M_n(\mathbb{R}^+)$, $n > 1$, be a nonnegative matrix of rank 1. Then A is a product of nonnegative idempotent matrices.

Remark (A.Alahamadi,S.K. Jain, A.L., Sathaye,2016)

It can be shown that in fact rank 1 nonnegative matrices can be decomposed into a product of *three* idempotent nonnegative matrices.

Rank two

Theorem

Let $A \in M_n(\mathbb{R}^+)$, $n > 2$, be a nonnegative singular matrix of rank 2. Then A is a product of nonnegative idempotent matrices.

Rank two

Theorem

Let $A \in M_n(\mathbb{R}^+)$, $n > 2$, be a nonnegative singular matrix of rank 2. Then A is a product of nonnegative idempotent matrices.

The proof is based on the following easy lemma:

Lemma

Let $S \subset (\mathbb{R}^+)^n$ be a finite set such that $dim_{\mathbb{R}} < S > \leq 2$. Then there exist $s_1, s_2 \in S$ such that every element of S is a positive linear combination of s_1 and s_2.

Counter-example

For singular nonnegative matrices of higher rank the decomposition does not necessarily exist:

Example

$$A_\alpha := \begin{pmatrix} \alpha & \alpha & 0 & 0 \\ 0 & 0 & \alpha & \alpha \\ \alpha & 0 & \alpha & 0 \\ 0 & \alpha & 0 & \alpha \end{pmatrix}, \quad \textit{where } \alpha \in \mathbb{R}^+, \ \alpha \neq 0.$$

If $A_\alpha = E_1 \dots E_n$ is such that $E_i^2 = E_i \in M_n(\mathbb{R}^+)$ then $A_\alpha = A_\alpha E_n$ and a direct computation shows that $E_n = Id$.. Remark that $A_{\frac{1}{2}}$ is a positive doubly stochastic matrix.

Nilpotent matrices

Proposition

If A is Nonnegative nilpotent there exists a permutation matrix such that PAP^t is an upper triangular nonnegative matrix.

Nilpotent matrices

Proposition

If A is Nonnegative nilpotent there exists a permutation matrix such that PAP^t is an upper triangular nonnegative matrix.

Corollary

Nonnegative nilpotent matrices are product of nonnegative idempotent matrices.

quasi-permutation matrices

Definition

A matrix $A \in M_{n,n}(\mathbb{R}^+)$ is a quasi-permutation matrix if each row and each column has *at most* one nonzero element.

quasi-permutation matrices

Definition

A matrix $A \in M_{n,n}(\mathbb{R}^+)$ is a quasi-permutation matrix if each row and each column has *at most* one nonzero element.

Theorem

A nonnegative singular quasi-permutation matrix is always a product of nonnegative idempotent matrices.

Nonnegative Von Neumann inverses

Definition

A nonnegative matrix A has a nonngative von Neumann inverse if there exists a nonnegative matrix X such that $A = AXA$.

Nonnegative Von Neumann inverses

Definition

A nonnegative matrix A has a nonngative von Neumann inverse if there exists a nonnegative matrix X such that $A = AXA$.

For a nonnegative matrix A to have a nonegative von Neumann inverse, it must be of a very special form (quasi permutation by block with all blocks of rank one). Using this form and the previous result on quasi-permutation matrices we get the following theorem.

Nonnegative Von Neumann inverses

Definition

A nonnegative matrix A has a nonngative von Neumann inverse if there exists a nonnegative matrix X such that $A = AXA$.

For a nonnegative matrix A to have a nonegative von Neumann inverse, it must be of a very special form (quasi permutation by block with all blocks of rank one). Using this form and the previous result on quasi-permutation matrices we get the following theorem.

Theorem

A nonnnegative singular matrix with nonnegative von Neumann inverse is a product of nonnegative idempotent matrices.

Periodic matrices

Definitions

1. A matrix A is periodic if there exist positive integers $l < s$, such that $A^l = A^s$

Periodic matrices

Definitions

1. A matrix A is periodic if there exist positive integers $l < s$, such that $A^l = A^s$
2. The index of $A \in M_n(\mathbb{R})$ is the smallest $k \geq 0$ such that $rank(A^k) = rank(A^{k+1})$

Periodic matrices

Definitions

1. A matrix A is periodic if there exist positive integers $l < s$, such that $A^l = A^s$
2. The index of $A \in M_n(\mathbb{R})$ is the smallest $k \geq 0$ such that $rank(A^k) = rank(A^{k+1})$

Theorem

Let A be a nonnegative periodic matrix with no zero row or zero column. If either the index of A is 1 or $A > A^n$ for some n, then A is a product of nonnegative idempotent matrices.

0-1 definite matrices

Definition

A matrix is a $0 - 1$ matrix if its entries consist only of O and 1's.

0-1 definite matrices

Definition

A matrix is a $0-1$ matrix if its entries consist only of O and 1's.

Theorem

Let $A \in M_n(\mathbb{R})$ be a singular definite $0-1$ matrix. Then A is a product of nonnegative idempotent matrices.

Plan

1. A) Ore extensions.
2. B) Polynomial maps.
3. C) Pseudo-linear transformations.
4. D) (σ, δ)-codes.
5. E) W (σ, δ)-codes.

Layout

1 History

2 Particular decompositions

3 Nonnegative singular matrices

4 special families of nonnegative matrices

5 ...and mORE

- Ore Extension
- B) Polynomial maps and roots
- C) Pseudo linear transformations
- (σ, δ)-codes

Ore extensions

A a ring, D a derivation of A, for $a \in A$ L_a is the left multiplication by a.

$$D \circ L_a = L_a \circ D + L_{D(a)}$$

Ore extensions

A a ring, D a derivation of A, for $a \in A$ L_a is the left multiplication by a.

$$D \circ L_a = L_a \circ D + L_{D(a)}$$

Formalizing;

$$Xa = aX + D(a)$$

Ore extensions

A a ring, D a derivation of A, for $a \in A$ L_a is the left multiplication by a.

$$D \circ L_a = L_a \circ D + L_{D(a)}$$

Formalizing;

$$Xa = aX + D(a)$$

More generally:
Assume the polynomials in X can be written as $\sum a_i X^i$ and there are maps σ, δ from A to A such that

$$Xa = \sigma(a)X + \delta(a)$$

Then associativity of the product will give that $\sigma \in End(A)$ and δ is a σ derivation

Ore extensions

A a ring, D a derivation of A, for $a \in A$ L_a is the left multiplication by a.

$$D \circ L_a = L_a \circ D + L_{D(a)}$$

Formalizing;

$$Xa = aX + D(a)$$

More generally:
Assume the polynomials in X can be written as $\sum a_i X^i$ and there are maps σ, δ from A to A such that

$$Xa = \sigma(a)X + \delta(a)$$

Then associativity of the product will give that $\sigma \in End(A)$ and δ is a σ derivation i.e. $\delta \in End(A, +)$ and

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$$

Examples

The set of these polynomials form a ring denoted by $R = A[X; \sigma, \delta]$ (O. Ore, 1930's)

1. $R = \mathbb{C}[t; -]$; we have $ti = -it$ and $t^2 a = t(\overline{a}t) = at^2$. $\frac{R}{R(t^2+1)} \cong \mathbb{H}$.

Examples

The set of these polynomials form a ring denoted by $R = A[X; \sigma, \delta]$ (O. Ore, 1930's)

1. $R = \mathbb{C}[t; -]$; we have $ti = -it$ and $t^2a = t(\overline{a}t) = at^2$. $\frac{R}{R(t^2+1)} \cong \mathbb{H}$.
2. p a prime, $q = p^l$ and $R = \mathbb{F}_q[t; \sigma]$; where $\sigma(x) = x^p$. The center of R is $\mathbb{F}_p[t^l]$.

Examples

The set of these polynomials form a ring denoted by $R = A[X; \sigma, \delta]$ (O. Ore, 1930's)

1. $R = \mathbb{C}[t; -]$; we have $ti = -it$ and $t^2 a = t(\bar{a}t) = at^2$. $\frac{R}{R(t^2+1)} \cong \mathbb{H}$.
2. p a prime, $q = p^l$ and $R = \mathbb{F}_q[t; \sigma]$; where $\sigma(x) = x^p$. The center of R is $\mathbb{F}_p[t^l]$.
3. k a field, $A_1 = k[x][y; Id., \frac{d}{dx}]$ the first Weyl algebra.
   - If $char(k) = p > 0, Z(A_1) = k[x^p, y^p]$
   - If $char(k) = 0$ then $Z(A_1) = k$ and A_1 is simple.

Inner and not inner

The σ inner derivation induced by an element $a \in A$ is defined by$\delta_a \in End(A, +)$ by $\delta_a(x) = ax - \sigma(x)a$, for $x \in A$.

Inner and not inner

The σ inner derivation induced by an element $a \in A$ is defined by$\delta_a \in End(A, +)$ by $\delta_a(x) = ax - \sigma(x)a$, for $x \in A$.
Such a derivation can be "erased": $A[t, \sigma, \delta_a] = A[t - a, \sigma]$.

Inner and not inner

The σ inner derivation induced by an element $a \in A$ is defined by$\delta_a \in End(A, +)$ by $\delta_a(x) = ax - \sigma(x)a$, for $x \in A$.
Such a derivation can be "erased": $A[t, \sigma, \delta_a] = A[t - a, \sigma]$. Finite ring can have non inner σ-derivation even if $\sigma \neq Id$..

Example

Let $q = p^l$, p a prime and A be the subring of $M_2(\mathbb{F}_q)$ given by

$$A = \{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, b \in \mathbb{F}_q,\ c \in \mathbb{F}_p \}.$$

Define σ and δ as follows:

$$\sigma(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = \begin{pmatrix} a^p & b^p \\ 0 & c \end{pmatrix} \quad \text{and} \quad \delta(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = \begin{pmatrix} 0 & b^p \\ 0 & 0 \end{pmatrix}$$

Layout

1. History
2. Particular decompositions
3. Nonnegative singular matrices
4. special families of nonnegative matrices
5. ...and mORE
   - Ore Extension
   - B) Polynomial maps and roots
   - C) Pseudo linear transformations
   - (σ, δ)-codes

Polynomial maps

$f(t) \in R = A[t; \sigma, \delta]$, $a \in A$, there exist $q(t) \in R$ such that $f(t) - q(t)(t - a) \in A$. This element is naturally defined to be the evaluation of $f(t)$ at a, denoted $f(a)$.

$$f(t) = q(t)(t - a) + f(a)$$

Polynomial maps

$f(t) \in R = A[t; \sigma, \delta]$, $a \in A$, there exist $q(t) \in R$ such that $f(t) - q(t)(t-a) \in A$. This element is naturally defined to be the evaluation of $f(t)$ at a, denoted $f(a)$.

$$f(t) = q(t)(t-a) + f(a)$$

Let us compute: $t^2 = t(t-a) + ta = t(t-a) + \sigma(a)t + \delta(a) = t(t-a) + \sigma(a)(t-a) + \sigma(a)a + \delta(a)$

$$\text{Hence} \quad t^2(a) = \sigma(a)a + \delta(a)$$

We will write $N_i(a)$ instead of $t^i(a)$.

Polynomial maps

$f(t) \in R = A[t;\sigma,\delta]$, $a \in A$, there exist $q(t) \in R$ such that $f(t) - q(t)(t-a) \in A$. This element is naturally defined to be the evaluation of $f(t)$ at a, denoted $f(a)$.

$$f(t) = q(t)(t-a) + f(a)$$

Let us compute: $t^2 = t(t-a) + ta = t(t-a) + \sigma(a)t + \delta(a) = t(t-a) + \sigma(a)(t-a) + \sigma(a)a + \delta(a)$

$$\text{Hence} \quad t^2(a) = \sigma(a)a + \delta(a)$$

We will write $N_i(a)$ instead of $t^i(a)$. Exercise: Compute $N_3(a)$

Polynomial maps

$f(t) \in R = A[t;\sigma,\delta]$, $a \in A$, there exist $q(t) \in R$ such that $f(t) - q(t)(t-a) \in A$. This element is naturally defined to be the evaluation of $f(t)$ at a, denoted $f(a)$.

$$f(t) = q(t)(t-a) + f(a)$$

Let us compute: $t^2 = t(t-a) + ta = t(t-a) + \sigma(a)t + \delta(a) = t(t-a) + \sigma(a)(t-a) + \sigma(a)a + \delta(a)$

$$\text{Hence} \quad t^2(a) = \sigma(a)a + \delta(a)$$

We will write $N_i(a)$ instead of $t^i(a)$. Exercise: Compute $N_3(a)$
Recurrence formulas:

$$N_0(a) = 1, \quad N_1(a) = a, \quad N_{i+1}(a) = \sigma(N_i(a))a + \delta(N_i(a))$$

Roots

For $f(t) = \sum_{i=0}^{n} a_i t^i \in R$ and $a \in A$ we have $f(a) = \sum_{i=0}^{n} a_i N_i(a)$. $a \in A$ is a *right* root of $f(t)$ if $f(a) = 0$.

Roots

For $f(t) = \sum_{i=0}^{n} a_i t^i \in R$ and $a \in A$ we have $f(a) = \sum_{i=0}^{n} a_i N_i(a)$. $a \in A$ is a *right* root of $f(t)$ if $f(a) = 0$.

Examples

1. If $\sigma = Id.$ and $\delta = 0$ we have the usual evaluation $N_i(a) = a^i$. But A can be non commutative so j is not a right root of $(x - j)(x - i) \in \mathbb{H}[x]$.
2. Many (right) roots: $f(x) = x^2 + 1 \in \mathbb{H}[x]$ then $f(yiy^{-1}) = 0$ for $0 \neq y \in \mathbb{H}$.
3. (Wedderburn) D a division ring $f(x) \in Z(D)[x]$ and $d \in D$ such that $f(d) = 0$ then there exists elements $a_1, \dots a_n \in D \setminus 0$ such that

$$f(x) = (x - d^{a_1}) \dots (x - d^{a_n}).$$

Examples

More examples:

Examples

1. Consider $t^2 \in A_1(k) = k[x][t; Id., \frac{d}{dx}]$ we have $t^2 = (t - \frac{1}{x})(t + \frac{1}{x})$.
2. Gordon Motzkin: Let D be a division ring and $f(x) \in D[x]$ the roots of $F(x)$ in D belong to at most $deg(f)$ conjugacy classes

Examples

More examples:

Examples

1. Consider $t^2 \in A_1(k) = k[x][t; Id., \frac{d}{dx}]$ we have $t^2 = (t - \frac{1}{x})(t + \frac{1}{x})$.
2. Gordon Motzkin: Let D be a division ring and $f(x) \in D[x]$ the roots of $F(x)$ in D belong to at most $deg(f)$ conjugacy classes

A nice formula: let $f(t), g(t) \in R = D[t; \sigma, \delta]$ where D is a dvision ring and $a \in D$.

$$(fg)(a) = \begin{cases} 0 & \text{if } g(a) = 0 \\ f(a^{g(a)})g(a) & \text{if } g(a) \neq 0 \end{cases}$$

where for $a \in D$ and $c \in D^*$ we define $a^c = \sigma(c)ac^{-1} + \delta(c)c^{-1}$

Layout

1 History

2 Particular decompositions

3 Nonnegative singular matrices

4 special families of nonnegative matrices

5 ...and mORE
- Ore Extension
- B) Polynomial maps and roots
- C) Pseudo linear transformations
- (σ, δ)-codes

Pseudo linear transformations

A, σ, δ, as usual $R = A[t; \sigma, \delta]$

Definition

Let ${}_AV$ be a left module. A map $T \in End(V, +)$ is a P.L.T. if

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v \quad \forall \alpha \in A, \forall v \in V$$

${}_AV$ then becomes a left R-module: $(\sum_{i=0}^{n} a_i t^i).v = \sum_{i=0}^{n} a_i T^i(v)$ for $v \in V$

Pseudo linear transformations

A, σ, δ, as usual $R = A[t; \sigma, \delta]$

Definition

Let ${}_AV$ be a left module. A map $T \in End(V, +)$ is a P.L.T. if

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v \quad \forall \alpha \in A, \forall v \in V$$

${}_AV$ then becomes a left R-module: $(\sum_{i=0}^{n} a_i t^i).v = \sum_{i=0}^{n} a_i T^i(v)$ for $v \in V$

Left R-modules $\Leftrightarrow$ Left A-module and a P.L.T.

Pseudo linear transformations

A, σ, δ, as usual $R = A[t; \sigma, \delta]$

Definition

Let ${}_AV$ be a left module. A map $T \in End(V, +)$ is a P.L.T. if

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v \quad \forall\alpha \in A, \forall v \in V$$

${}_AV$ then becomes a left R-module: $(\sum_{i=0}^n a_i t^i).v = \sum_{i=0}^n a_i T^i(v)$ for $v \in V$

Left R-modules $\Leftrightarrow$ Left A-module and a P.L.T.

Examples

1. δ is a P.L.T. defined on $V = A$
2. Let $C \in M_n(A)$ then $T_C : A^n \longrightarrow A^n$ defined by $T_C(v) = \sigma(v)C + \delta(v)$ for any $v \in A^n$, is a P.L.T.

More PLT

Proposition

Let $R = A[t;\sigma,\delta]$.

1. $p(t) \in R$, $a \in A$, $p(a) = p(T_a)(1)$
2. *For* $x \in U(R)$ $p(a^x)x = p(T_a)(x)$
3. *If* $T :_A V \longrightarrow_A V$ *is a PLT, then the map*

$$\phi_T : R \longrightarrow End(V,+) : f(t) \mapsto f(T)$$

   is a ring homomorphism.

4. *for* $f, g \in R$ *and* $a \in A$, *we have* $(fg)(a) = f(T_a)(g(a))$
5. *If* $A = D$ *is a division ring and* $a \in D$ *then* $ker(P(T_a))$ *is a right vector space over the division ring* $C(a) := \{x \in D^* | a^x = a\} \cup \{0\}$

Factorizations

Theorem {Lam, L.}

Let D be a division ring, $\sigma \in End(D)$ and δ a σ-derivation. A polynomial $f(t) \in D[t; \sigma, \delta]$ has roots in l (σ, δ)-conjugacy classes $\Delta(a_i) := \{a_i^x = \sigma(x)a_i x^{-1} + \delta(x)x^{-1} | x \in D^*\}$. We have

$$\sum_{i=1}^{l} Dim_{C_i} Ker(f(T_{a_i})) \leq deg(f(t))$$

The equality occurs if an only if $f(t)$ is a Wedderburn polynomial.

Layout

1. History
2. Particular decompositions
3. Nonnegative singular matrices
4. special families of nonnegative matrices
5. ...and mORE
   - Ore Extension
   - B) Polynomial maps and roots
   - C) Pseudo linear transformations
   - (σ, δ)-codes

Ulmer, Boucher

Just to give an idea: there are 603 different nontrivial right divisors of $t^{14} - 1 \in \mathbb{F}_4[t;\theta]$ with $\theta(z) = z^2$ comparing with 25 different factors of $x^{14} - 1 \in \mathbb{F}_4[x]$.
F. Ulmer, D. Boucher started to use skew polynomial rings ($\delta = 0$) to create codes and study them. As an alphabet they not only used fields but also cyclic modules of the form $\frac{R}{Rf(t)}$ where $R = F[t;\sigma]$.

Example

In $\mathbb{F}_4[t;\theta]$ with $\theta(z) = z^2$ where $\alpha \in \mathbb{F}_4$ satisfies $\alpha^2 + \alpha + 1 = 0$, we have: $t^4 + t^2 + 1 = (t^2 + t + 1)^2 = (t^2 + \alpha^2)(t^2 + \alpha) = (t^2 + \alpha)(t^2 + \alpha^2) = (t^2 + \alpha^2 t + 1)^2 = (t^2 + \alpha t + 1)^2$,

$C < \frac{R}{Rf}$ with $R = A[t;\sigma,\delta]$

Definition

Let $f(t), g(t) \in R = A[t;\sigma,\delta]$ monic and such that $f(t) \in Rg(t)$. A subset of $C \subseteq A^n$ consisting of the coordinates of the elements of Rg/Rf in the basis $\{1, t, \ldots, t^{n-1}\}$ is called a cyclic (f, σ, δ)-code.

Theorem

Let $g(t) := \sum_{i=0}^{r} g_i t^i \in R$ be a monic right divisor of $f(t)$.

(a) *The code corresponding to Rg/Rf is a free left A-module of dimension $n - r$ where $\deg(f) = n$ and $\deg(g) = r$.*

(b) *If $v := (a_0, a_1, \ldots, a_{n-1}) \in C$ then $T_f(v) \in C$.*

(c) *The rows of the matrix generating the code C are given by*

$$(T_f)^k(g_0, g_1, \ldots, g_r, 0, \ldots, 0), \quad \text{for } 0 \le k \le n-r-1.$$

Example

Consider $f(t) = t^5 - 1 \in R = \frac{\mathbb{F}_5[X]}{X^5-1}[t; Id., \frac{d}{dX}]$. In this case $f(x) = f(x + x^4) = 0$ (with $x = X + (X^5 - 1)$) and $g(t) = [t - x, t - (x + x^4)]_l = t^2 - 2xt + x^2 - 1$. The generating matrix of the code corresponding to the module Rg/Rf is given by:

$$\begin{pmatrix} x^2 - 1 & -2x & 1 & 0 & 0 \\ 2x & x^2 + 2 & -2x & 1 & 0 \\ 2 & 4x & x^2 & -2x & 1 \end{pmatrix}$$

Lemma

$f(t), p(t), q(t) = \sum_{i=0}^{n-1} \in R = A[t; \sigma, \delta]$ such that $deg(q(t)) < deg(f(t)) = n$. Then $p(t)q(t) \in Rf(t) \Leftrightarrow p(T_f)(q_0, \dots, q_{n-1}) = (0, \dots, 0)$

Theorem

Let $f, g, h, h' \in R$ monic such that $f = gh = h'g$ and let C denote the code corresponding to the cyclic module Rg/Rf. Then the following statements are equivalent:

(i) $(c_0, \dots, c_{n-1}) \in C$,

(ii) $(\sum_{i=0}^{n-1} c_i t^i) h(t) \in Rf$,

(iii) $\sum_{i=0}^{n-1} c_i T_f^i(\underline{h}) = \underline{0}$,

Definition

For a left (resp. right) linear code $C \subseteq A^n$, we say that a matrix H is a control matrix if $C = lann(H)$ (resp. $C = rann(H)$).

Corollary

$f, g, h, h' \in R = A[t;\sigma,\delta]$ monic such that $f = gh = h'g$. Then $H =^t (\underline{h}, T_f(\underline{h}), \ldots, T_f^{deg(f)-1}(\underline{h}))$ is a control matrix of the code corresponding to Rg/Rf.

Corollary

$f, g, h, h' \in R = A[t;\sigma,\delta]$ monic such that $f = gh = h'g$. Then $H =^t (\underline{h}, T_f(\underline{h}), \ldots, T_f^{deg(f)-1}(\underline{h}))$ is a control matrix of the code corresponding to Rg/Rf.

Example

$f(t) = t^5 - 1 = g(t)h(t) = h(t)g(t) \in R := \mathbb{F}_5[x]/(x^5-1)[t; \frac{d}{dx}]$, with $h(t) = t^3 + 2xt^2 + (3x^2+2)t + (4x^3+3x)$ and $g(t) := t^2 - 2xt + x^2 - 1$. C corresponding to $Rg(t)/(t^5-1)$.

$$H = \begin{pmatrix} 4x^3+3x & 3x^2+2 & 2x & 1 & 0 \\ 2x^2+3 & 4x^3+4 & 3x^2+4 & 2x & 1 \\ 4x+1 & 4x^2+2 & 4x^3 & 3x^2+1 & 2x \\ 2x+4 & 2x+1 & x^2+2 & 4x^3+6x & 3x^2+3 \\ 3x^2 & 2x+1 & 4x+1 & 3x^2+3 & 4x^3+2x \end{pmatrix}$$

(σ, δ) W codes

Definitions

a) $f(t) \in R = A[t; \sigma, \delta]$ is a W-polynomial if $f(t)$ is monic and there exist elements $a_1, \ldots, a_n \in A$ such that $Rf(t) = \cap_{i=0}^{i=n} R(t - a_i)$.

(σ, δ) W codes

Definitions

a) $f(t) \in R = A[t; \sigma, \delta]$ is a W-polynomial if $f(t)$ is monic and there exist elements $a_1, \ldots, a_n \in A$ such that
$Rf(t) = \cap_{i=0}^{i=n} R(t - a_i)$.
b) The $n \times r$ generalized Vandermonde matrix defined by $a_1, \ldots, a_r$ is given by:

$$V_n(a_1, \ldots, a_r) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_r \\ \ldots & \ldots & \ldots & \ldots \\ N_{n-1}(a_1) & N_{n-1}(a_2) & \ldots & N_{n-1}(a_r) \end{pmatrix}.$$

The Wedderburn polynomials play the role of separable polynomials.

Proposition

Let $f(t), g(t) \in R = A[t; \sigma, \delta]$ be monic polynomials of degree n and r respectively. Suppose that $g(t)$ is a Wedderburn polynomial with $f(t) \in Rg(t)$ and let C be the (σ, δ)-W-code of length n corresponding to the left cyclic R-module $Rg(t)/Rf(t)$. Let $a_1, \ldots, a_r \in A$ be such that $Rg(t) = \bigcap_{i=0}^{r} R(t - a_i)$. Then $(c_0, c_1, \ldots, c_{n-1}) \in C$ if and only if $(c_0, c_1, \ldots, c_{n-1})V_n(a_1, \ldots, a_r) = (0, \ldots, 0)$.

Thanks

Thank you for your kind attention and ...

Thanks

Thank you for your kind attention and ...
very mild winter