Minimal matrix centralizers over the field $\mathbb{Z}_2$

Damjana Kokol Bukovšek

(Joint work with David Dolžan)
University of Ljubljana

Novi Sad, June 2013

Let $M_n(\mathbb{F})$ be the algebra of $n \times n$ matrices over the field $\mathbb{F}$.

Let $M_n(\mathbb{F})$ be the algebra of $n \times n$ matrices over the field $\mathbb{F}$.

Denote by $\mathscr{C}(A) = \{B \in M_n(\mathbb{F}); AB = BA\}$ the centralizer of A.

Let $M_n(\mathbb{F})$ be the algebra of $n \times n$ matrices over the field $\mathbb{F}$.

Denote by $\mathscr{C}(A) = \{B \in M_n(\mathbb{F}); AB = BA\}$ the centralizer of A.

Let $A, B \in M_n(\mathbb{F})$. Then $A \leq B$ if and only if $\mathscr{C}(A) \subseteq \mathscr{C}(B)$.

Let $M_n(\mathbb{F})$ be the algebra of $n \times n$ matrices over the field $\mathbb{F}$.

Denote by $\mathscr{C}(A) = \{B \in M_n(\mathbb{F}); AB = BA\}$ the centralizer of A.

Let $A, B \in M_n(\mathbb{F})$. Then $A \leq B$ if and only if $\mathscr{C}(A) \subseteq \mathscr{C}(B)$.

A matrix $A \in M_n(\mathbb{F})$ is minimal if it is minimal with respect to this partial order.

Let $M_n(\mathbb{F})$ be the algebra of $n \times n$ matrices over the field $\mathbb{F}$.

Denote by $\mathscr{C}(A) = \{B \in M_n(\mathbb{F}); AB = BA\}$ the centralizer of A.

Let $A, B \in M_n(\mathbb{F})$. Then $A \leq B$ if and only if $\mathscr{C}(A) \subseteq \mathscr{C}(B)$.

A matrix $A \in M_n(\mathbb{F})$ is minimal if it is minimal with respect to this partial order.

Lemma

Let $A, B \in M_n(\mathbb{F})$. Then $\mathscr{C}(A) \subseteq \mathscr{C}(B)$ if and only if $B \in \mathbb{F}[A]$.

Let $M_n(\mathbb{F})$ be the algebra of $n \times n$ matrices over the field $\mathbb{F}$.

Denote by $\mathscr{C}(A) = \{B \in M_n(\mathbb{F}); AB = BA\}$ the centralizer of A.

Let $A, B \in M_n(\mathbb{F})$. Then $A \leq B$ if and only if $\mathscr{C}(A) \subseteq \mathscr{C}(B)$.

A matrix $A \in M_n(\mathbb{F})$ is minimal if it is minimal with respect to this partial order.

Lemma

Let $A, B \in M_n(\mathbb{F})$. Then $\mathscr{C}(A) \subseteq \mathscr{C}(B)$ if and only if $B \in \mathbb{F}[A]$.

A matrix $A \in M_n(\mathbb{F})$ is called non-derogatory if its minimal polynomial equals its characteristic polynomial. A matrix is derogatory if it is not non-derogatory.

Theorem

Let $n \geq 2$. A matrix $A \in M_n(\mathbb{C})$ is non-derogatory if and only if A is minimal.

Theorem

Let $n \geq 2$. A matrix $A \in M_n(\mathbb{C})$ is non-derogatory if and only if A is minimal.

Theorem (Dolinar, Guterman, Kuzma, Oblak, 2013)

Let $n \geq 2$ and $\mathbb{F}$ an arbitrary field. If $A \in M_n(\mathbb{F})$ is non-derogatory then A is minimal.

Theorem

Let $n \geq 2$. A matrix $A \in M_n(\mathbb{C})$ is non-derogatory if and only if A is minimal.

Theorem (Dolinar, Guterman, Kuzma, Oblak, 2013)

Let $n \geq 2$ and $\mathbb{F}$ an arbitrary field. If $A \in M_n(\mathbb{F})$ is non-derogatory then A is minimal.

Theorem (Dolinar, Guterman, Kuzma, Oblak, 2013)

Let $n \geq 2$ and $\mathbb{F}$ a field with $|\mathbb{F}| \geq n$. Then a matrix $A \in M_n(\mathbb{F})$ is non-derogatory if and only if A is minimal.

For a polynomial $m(x) = x^r + b_{r-1}x^{r-1} + \ldots + b_1 x + b_0 \in \mathbb{F}[x]$ of degree r, let $C(m) \in M_r(\mathbb{F})$ denote the companion matrix of m

$$C(m) = \begin{bmatrix} 0 & 0 & 0 & \ldots & -b_0 \\ 1 & 0 & 0 & \ldots & -b_1 \\ & \ddots & \ddots & & \vdots \\ 0 & \ldots & 1 & 0 & -b_{r-2} \\ 0 & \ldots & 0 & 1 & -b_{r-1} \end{bmatrix}.$$

For a polynomial $m(x) = x^r + b_{r-1}x^{r-1} + \ldots + b_1 x + b_0 \in \mathbb{F}[x]$ of degree r, let $C(m) \in M_r(\mathbb{F})$ denote the companion matrix of m

$$C(m) = \begin{bmatrix} 0 & 0 & 0 & \ldots & -b_0 \\ 1 & 0 & 0 & \ldots & -b_1 \\ & \ddots & \ddots & & \vdots \\ 0 & \ldots & 1 & 0 & -b_{r-2} \\ 0 & \ldots & 0 & 1 & -b_{r-1} \end{bmatrix}.$$

Example (Dolinar, Guterman, Kuzma, Oblak, 2013)

Let $A = C(m) \oplus C(m^3) \in M_8(\mathbb{Z}_2)$ for $m(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$. Then A is derogatory and minimal.

Proposition

Suppose the spectrum of A is either $\{0\}$ *or* $\{1\}$. *Then A is minimal if and only if A is non-derogatory.*

Proposition

Suppose the spectrum of A is either $\{0\}$ or $\{1\}$. Then A is minimal if and only if A is non-derogatory.

Proof: We only have to prove the implication: A is minimal $\Rightarrow$ A is non-derogatory.

Proposition

Suppose the spectrum of A is either $\{0\}$ or $\{1\}$. Then A is minimal if and only if A is non-derogatory.

Proof: We only have to prove the implication: A is minimal $\Rightarrow$ A is non-derogatory.
Suppose A is derogatory. Let λ be the only eigenvalue of A. The Jordan form of A is $J_{k_1}(\lambda) \oplus J_{k_2}(\lambda) \oplus \ldots \oplus J_{k_t}(\lambda)$, where $t \geq 2$.

Proposition

Suppose the spectrum of A is either $\{0\}$ or $\{1\}$. Then A is minimal if and only if A is non-derogatory.

Proof: We only have to prove the implication: A is minimal $\Rightarrow$ A is non-derogatory.
Suppose A is derogatory. Let λ be the only eigenvalue of A.
The Jordan form of A is $J_{k_1}(\lambda) \oplus J_{k_2}(\lambda) \oplus \ldots \oplus J_{k_t}(\lambda)$, where $t \geq 2$.
Let $X = J_{k_1}(\lambda + 1) \oplus J_{k_2}(\lambda) \oplus \ldots \oplus J_{k_t}(\lambda)$.
If $\lambda = 0$ then A is similar to $X(X + I)$; if $\lambda = 1$ then A is similar to $X(X + I) + I$.

Proposition

Suppose the spectrum of A is either $\{0\}$ or $\{1\}$. Then A is minimal if and only if A is non-derogatory.

Proof: We only have to prove the implication: A is minimal $\Rightarrow$ A is non-derogatory.
Suppose A is derogatory. Let λ be the only eigenvalue of A.
The Jordan form of A is $J_{k_1}(\lambda) \oplus J_{k_2}(\lambda) \oplus \ldots \oplus J_{k_t}(\lambda)$, where $t \geq 2$.
Let $X = J_{k_1}(\lambda + 1) \oplus J_{k_2}(\lambda) \oplus \ldots \oplus J_{k_t}(\lambda)$.
If $\lambda = 0$ then A is similar to $X(X + I)$; if $\lambda = 1$ then A is similar to $X(X + I) + I$.
So $A \in \mathbb{F}[X]$, but $X \notin \mathbb{F}[A]$, since spectrum of X is equal to $\mathbb{Z}_2$.
This implies that A is not minimal.

Example

Let

$$A = J_3(0) \oplus J_1(0) \oplus J_1(1) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then A is derogatory and minimal. This is the smallest derogatory minimal matrix.

Outline of the proof: Suppose that A is not minimal. So, $A = p(X)$ for some polynomial p and matrix X and $\mathscr{C}(X) \neq \mathscr{C}(A)$.

Outline of the proof: Suppose that A is not minimal. So, $A = p(X)$ for some polynomial p and matrix X and $\mathscr{C}(X) \neq \mathscr{C}(A)$.

Case 1: X has an eigenvalue α, which is not in $\mathbb{Z}_2$.

Outline of the proof: Suppose that A is not minimal. So, $A = p(X)$ for some polynomial p and matrix X and $\mathscr{C}(X) \neq \mathscr{C}(A)$.

Case 1: X has an eigenvalue α, which is not in $\mathbb{Z}_2$.

Then X is similar to a matrix $C(q^m) \oplus X'$, where $q(x)$ is the the minimal polynomial of α.

Outline of the proof: Suppose that A is not minimal. So, $A = p(X)$ for some polynomial p and matrix X and $\mathscr{C}(X) \neq \mathscr{C}(A)$.

Case 1: X has an eigenvalue α, which is not in $\mathbb{Z}_2$.

Then X is similar to a matrix $C(q^m) \oplus X'$, where $q(x)$ is the the minimal polynomial of α.

$p(\alpha)$ is either 0 or 1 and $p(\beta) = p(\alpha)$ for any other zero β of the polynomial q.

Outline of the proof: Suppose that A is not minimal. So, $A = p(X)$ for some polynomial p and matrix X and $\mathscr{C}(X) \neq \mathscr{C}(A)$.

Case 1: X has an eigenvalue α, which is not in $\mathbb{Z}_2$.

Then X is similar to a matrix $C(q^m) \oplus X'$, where $q(x)$ is the the minimal polynomial of α.

$p(\alpha)$ is either 0 or 1 and $p(\beta) = p(\alpha)$ for any other zero β of the polynomial q.

So, $A = p(X)$ is similar to $J_m(p(\alpha)) \oplus \ldots \oplus J_m(p(\alpha)) \oplus p(X')$. A contradiction.

Case 2: The spectrum of X is equal to $\mathbb{Z}_2$.

Case 2: The spectrum of X is equal to $\mathbb{Z}_2$.

The polynomial p either maps 0 to 0 and 1 to 1 or vice versa.

Case 2: The spectrum of X is equal to $\mathbb{Z}_2$.

The polynomial p either maps 0 to 0 and 1 to 1 or vice versa.

Assume $p(0) = 0$ and $p(1) = 1$.

Case 2: The spectrum of X is equal to $\mathbb{Z}_2$.

The polynomial p either maps 0 to 0 and 1 to 1 or vice versa.

Assume $p(0) = 0$ and $p(1) = 1$.

X is similar to $X_0 \oplus X_1$, where X_0 and $X_1 + I$ are nilpotents.

Case 2: The spectrum of X is equal to $\mathbb{Z}_2$.

The polynomial p either maps 0 to 0 and 1 to 1 or vice versa.

Assume $p(0) = 0$ and $p(1) = 1$.

X is similar to $X_0 \oplus X_1$, where X_0 and $X_1 + I$ are nilpotents.

$J_1(1)$ is similar to $p(X_1)$, so $X_1 = J_1(1)$, and $J_3(0) \oplus J_1(0)$ is similar to $p(X_0)$.

Case 2: The spectrum of X is equal to $\mathbb{Z}_2$.

The polynomial p either maps 0 to 0 and 1 to 1 or vice versa.

Assume $p(0) = 0$ and $p(1) = 1$.

X is similar to $X_0 \oplus X_1$, where X_0 and $X_1 + I$ are nilpotents.

$J_1(1)$ is similar to $p(X_1)$, so $X_1 = J_1(1)$, and $J_3(0) \oplus J_1(0)$ is similar to $p(X_0)$.

X_0 has at most two Jordan blocks. It is easy to verify, that it cannot have only one.

Case 2: The spectrum of X is equal to $\mathbb{Z}_2$.

The polynomial p either maps 0 to 0 and 1 to 1 or vice versa.

Assume $p(0) = 0$ and $p(1) = 1$.

X is similar to $X_0 \oplus X_1$, where X_0 and $X_1 + I$ are nilpotents.

$J_1(1)$ is similar to $p(X_1)$, so $X_1 = J_1(1)$, and $J_3(0) \oplus J_1(0)$ is similar to $p(X_0)$.

X_0 has at most two Jordan blocks. It is easy to verify, that it cannot have only one.

So X_0 is similar to $J_3(0) \oplus J_1(0)$, and X is similar to A.

Case 2: The spectrum of X is equal to $\mathbb{Z}_2$.

The polynomial p either maps 0 to 0 and 1 to 1 or vice versa.

Assume $p(0) = 0$ and $p(1) = 1$.

X is similar to $X_0 \oplus X_1$, where X_0 and $X_1 + I$ are nilpotents.

$J_1(1)$ is similar to $p(X_1)$, so $X_1 = J_1(1)$, and $J_3(0) \oplus J_1(0)$ is similar to $p(X_0)$.

X_0 has at most two Jordan blocks. It is easy to verify, that it cannot have only one.

So X_0 is similar to $J_3(0) \oplus J_1(0)$, and X is similar to A.

Since $\mathscr{C}(X) \subseteq \mathscr{C}(A)$, it follows $\mathscr{C}(A) = \mathscr{C}(X)$. A contradiction.

Theorem

Suppose the spectrum of A is equal to $\mathbb{Z}_2$ and the Jordan form of A is $J_{k_1}(0) \oplus J_{k_2}(0) \oplus \ldots \oplus J_{k_t}(0) \oplus J_{l_1}(1) \oplus J_{l_2}(1) \oplus \ldots \oplus J_{l_s}(1)$ for some integers $k_1 \geq k_2 \geq \ldots \geq k_t$ and $l_1 \geq l_2 \geq \ldots \geq l_s$. Then A is not minimal if and only if at least one of the following statements holds.

1. *t is even and $k_1 = k_2 + 1$, $k_3 = k_4 + 1$, $\ldots$, $k_{t-1} = k_t + 1$.*
2. *$t \geq 3$ is odd and $k_1 = k_2 + 1$, $k_3 = k_4 + 1$, $\ldots$, $k_{t-2} = k_{t-1} + 1$, $k_t = 1$.*
3. *s is even and $l_1 = l_2 + 1$, $l_3 = l_4 + 1$, $\ldots$, $l_{s-1} = l_s + 1$.*
4. *$s \geq 3$ is odd and $l_1 = l_2 + 1$, $l_3 = l_4 + 1$, $\ldots$, $l_{s-2} = l_{s-1} + 1$, $l_s = 1$.*
5. *A has at least two equal Jordan blocks, so $k_m = k_{m+1}$ for some m or $l_m = l_{m+1}$ for some m.*

Rational canonical form of a matrix over an arbitrary field:

Every matrix $A \in M_n(\mathbb{F})$ is similar to a unique (up to the order of the blocks) block diagonal matrix

$$C = C({m_1}^{k_{11}}) \oplus \ldots \oplus C({m_1}^{k_{1k}}) \oplus \ldots \oplus C({m_l}^{k_{l1}}) \oplus \ldots \oplus C({m_l}^{k_{lk}}) \in M_n(\mathbb{F}),$$

where $m_1, \ldots, m_l \in \mathbb{F}[x]$ are the distinct, monic irreducible divisors of the characteristic polynomial $f \in \mathbb{F}[x]$ of A and k_{ij} is the largest power of m_i, which divides the j-th invariant factor f_j of A.

Rational canonical form of a matrix over an arbitrary field:

Every matrix $A \in M_n(\mathbb{F})$ is similar to a unique (up to the order of the blocks) block diagonal matrix

$$C = C({m_1}^{k_{11}}) \oplus \ldots \oplus C({m_1}^{k_{1k}}) \oplus \ldots \oplus C({m_l}^{k_{l1}}) \oplus \ldots \oplus C({m_l}^{k_{lk}}) \in M_n(\mathbb{F}),$$

where $m_1, \ldots, m_l \in \mathbb{F}[x]$ are the distinct, monic irreducible divisors of the characteristic polynomial $f \in \mathbb{F}[x]$ of A and k_{ij} is the largest power of m_i, which divides the j-th invariant factor f_j of A.

Suppose now that the minimal polinomial of $A \in M_n(\mathbb{Z}_2)$ is a power of an irreducible polynomial $m(x) \in \mathbb{Z}_2[x]$.

Rational canonical form of a matrix over an arbitrary field:

Every matrix $A \in M_n(\mathbb{F})$ is similar to a unique (up to the order of the blocks) block diagonal matrix

$$C = C(m_1{}^{k_{11}}) \oplus \ldots \oplus C(m_1{}^{k_{1k}}) \oplus \ldots \oplus C(m_l{}^{k_{l1}}) \oplus \ldots \oplus C(m_l{}^{k_{lk}}) \in M_n(\mathbb{F}),$$

where $m_1, \ldots, m_l \in \mathbb{F}[x]$ are the distinct, monic irreducible divisors of the characteristic polynomial $f \in \mathbb{F}[x]$ of A and k_{ij} is the largest power of m_i, which divides the j-th invariant factor f_j of A.

Suppose now that the minimal polinomial of $A \in M_n(\mathbb{Z}_2)$ is a power of an irreducible polynomial $m(x) \in \mathbb{Z}_2[x]$.

Then A is similar to a unique block diagonal matrix

$$C(m^{k_1}) \oplus C(m^{k_2}) \oplus \ldots \oplus C(m^{k_t})$$

for some integers $k_1 \geq k_2 \geq \ldots \geq k_t$.

Theorem

Let $A \in M_n(\mathbb{Z}_2)$. If the rational canonical form of A is of the form $C(m^k) \oplus C(m^k)$ or $C(m^k) \oplus C(m^{k+1})$ for some irreducible polynomial $m(x) \in \mathbb{Z}_2[x]$ of degree $t \geq 1$ and $k \in \mathbb{N}$, then A is not minimal.

Theorem

Let $A \in M_n(\mathbb{Z}_2)$. If the rational canonical form of A is of the form $C(m^k) \oplus C(m^k)$ or $C(m^k) \oplus C(m^{k+1})$ for some irreducible polynomial $m(x) \in \mathbb{Z}_2[x]$ of degree $t \geq 1$ and $k \in \mathbb{N}$, then A is not minimal.

Theorem

Suppose the minimal polynomial of A is $p(x) = m(x)^k$, where $m(x)$ is an irreducible polynomial of degree $r \geq 3$ and $k \in \mathbb{N}$. Then A is minimal if and only if A is non-derogatory.

Example

Let $m_1, m_2 \in \mathbb{Z}_2[x]$ denote the polynomials $m_1(x) = x^3 + x + 1$, $m_2(x) = x^3 + x^2 + 1$, and let

$$B = C(m_1^3) \oplus C(m_1).$$

Then B is not minimal by above Theorem. However, the matrix

$$A = \begin{bmatrix} B & 0 \\ 0 & C(m_2) \end{bmatrix},$$

is minimal.

Theorem

Let $n \geq 2$. Suppose the minimal polynomial of $A \in M_n(\mathbb{Z}_2)$ is of the form $p(x) = m(x)^k$, where $k \in \mathbb{N}$ and $m(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ is the irreducible quadratic polynomial and let $C(m^{k_1}) \oplus C(m^{k_2}) \oplus \ldots \oplus C(m^{k_t})$ be the rational canonical form of A for some integers $k = k_1 \geq k_2 \geq \ldots \geq k_t$. Then A is not minimal if and only if one of the following statements holds.

1. *There exists some $s \in \{1, 2, \ldots, t-1\}$ such that $k_s = k_{s+1}$.*
2. *t is even and $k_1 = k_2 + 1$, $k_3 = k_4 + 1$, $\ldots$, $k_{t-1} = k_t + 1$.*
3. *$t \geq 3$ is odd and $k_1 = k_2 + 1$, $k_3 = k_4 + 1$, $\ldots$, $k_{t-2} = k_{t-1} + 1$, $k_t = 1$.*

Thank you!