Matrices over Differential-difference Algebras

Yang Zhang

Department of Mathematics

University of Manitoba, Canada

(with Q. W. Feng and Q. W. Wang)

Ore (Skew) Polynomials

☞ Let σ be an automorphism of a ring R, *i.e.*, σ is 1-1 and

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \sigma(ab) = \sigma(a)\sigma(b) \quad \forall a, b \in R.$$

☞ A σ-derivation δ of R is a mapping $R \to R$ satisfying: $\forall a, b \in R$,

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

☞ Ore (skew) polynomial ring $R[x; \sigma, \delta]$ over R is the set of usual polynomials in x over R, *i.e.*, $\{\sum r_i x^i \mid r_i \in R\}$, with usual "$+$" and

$$xr = \sigma(r)x + \delta(r), \quad \forall r \in R.$$

☞ Appeared in Noether and Schmeidler (1920). More discussion given in Ore (1933, Ann. of Math.).

Definitions

Let D be a ring with an involution "$-$", that is, an anti-automorphism on D of order 2, i.e., $\overline{a+b} = \bar{a}+\bar{b}$, $\overline{(ab)} = \bar{b}\bar{a}$, $\bar{\bar{a}} = a$.

For $A \in (D)^{m\times n}$, define $\overline{A} = (\bar{a}_{ij})$, and $A^* = (\bar{A})^T$, the involution transpose of A.

Let $A \in (D)^{m\times n}$ and $B \in (D)^{n\times m}$.

$$(1)\ AGA = A \quad (2)\ GAG = G \quad (3)\ (AG)^* = AG \quad (4)\ (GA)^* = GA$$

$$(5)\ AG = GA \quad (6)\ A^k = A^{k+1}G,\ k \in \mathbb{N}$$

G is called a $\{i,j,k...\}$-inverse of A if G satisfies $\{i,j,k..\}$.

G is called a Moore-Penrose inverse if G satisfies $\{1,2,3,4\}$.

History

Computing various generalized inverses of given matrices:

- very active research areas:
  Ring Theory,
  Matrix Theory,
  Linear Algebra, Numerical Linear Algebra,
  Numerical Analysis, etc.

- many applications in Statistics, Engineering, etc.

The Field of Rational Functions

Consider $K(t)[x;\sigma,\delta]$, where $K(t)$ is the rational function field over a field K. It is well-known that every automorphism ϕ of $K(t)$ can be induced by

$$\phi(t) = \frac{at+b}{ct+d} \quad \text{or} \quad \phi(t) = t,$$

where $a,b,c,d \in K$ and $ad-bc \neq 0$.

Lemma Every involution ϕ on $K(t)$ can be written as

$$\phi(t) = \frac{at+b}{ct-a} \quad \text{or} \quad \phi(t) = t,$$

where $a,\ b,\ c \in K$ and $a^2+bc \neq 0$.

Ore Polynomials

In skew polynomial rings, we always assume that σ and δ commute.

In $K(t)$, this condition will force σ to be a shift operator.

Lemma In $K(t)$, let $\delta(t) = 1$. Then $\sigma\delta = \delta\sigma$ if and only if $\sigma(t) = t + k$, for some $k \in K$.

In $K(t)[x]$

Theorem Let $S = K(t)[x]$. Then every involution ϕ on S with $\phi(t) = t$ can be written as

$$\phi\left(\sum_{i=0}^{n} r_i(t)x^i\right) = \sum_{i=0}^{n} r_i(t)\left[-x + a(t)\right]^i \quad \text{or}$$

$$\phi\left(\sum_{i=0}^{n} r_i(t)x^i\right) = \sum_{i=0}^{n} r_i(t)\left(cx\right)^i,$$

where $a(t) \in K(t)$ and $c \in K$ with $c^2 = 1$.

In $K(t)[x]$

Theorem Let $S = K(t)[x]$. Then the form of the involution ϕ on S with $\phi(t) = \frac{at+b}{ct-a}$ $a,\ b,\ c \in K$ and $a^2+bc \neq 0$ is

$$\phi\left(\sum_{i=0}^{n} r_i(t)x^i\right) = \sum_{i=0}^{n} \phi(r_i(t))\left[a_1(t)x + b_1(t)\right]^i,$$

for some $a_1(t) \in K(t) \setminus \{0\}$, $b_1(t)$.

Furthermore, ϕ is an involution on S if and only if $a_1(t)$ and $b_1(t)$ satisfy

$$a_1(t)\phi[a_1(t)] = 1 \quad \text{and} \quad b_1(t)\phi(a_1(t)) + \phi(b_1(t)) = 0.$$

Involutions on $S = K(t)[x;\delta]$

We would extend all the involutions ϕ on $K(t)$ (i.e., $\phi(t) = \frac{at+b}{ct-a}$ and $\phi(t) = t$) to $K(t)[x;\delta]$ (i.e., $\sigma = 1$ and $\delta \neq 0$ in $K(t)[x;\sigma,\delta]$).

The following Leibniz formula in $S = K(t)[x;\delta]$ is well-known.

$$x^m [a(t)] = \sum_{i=0}^{m} \binom{m}{i} \delta^{m-i}[a(t)] x^i, \text{ for any } a(t) \in K(t).$$

Lemma Let $S = K(t)[x;\delta]$. For any $a(t), b(t) \in K(t)$,

$$b(t)[-x + a(t)]^m = \sum_{i=0}^{m} \binom{m}{i} [-x + a(t)]^i \delta^{m-i}[b(t)].$$

Involutions on $S = K(t)[x;\delta]$

Lemma Let $a_1(t) = \frac{(ct-a)^2}{a^2+bc} \in K(t)$ and $\phi(t) = \frac{at+b}{ct-a}$, where $a,\ b,\ c \in K$ and $a^2+bc \neq 0$, then

$$\phi[s(t)]\,[a_1(t)x+b_1(t)]^m = \sum_{i=0}^{m} \binom{m}{i} [a_1(t)x+b_1(t)]^i \phi[\delta^{m-i}(s(t))],$$

for any $b_1(t), s(t) \in K(t)$.

Involutions on $S = K(t)[x;\delta]$

Theorem Let $S = K(t)[x;\delta]$. Then every involution ϕ on S with $\phi(t) = t$ can be written as

$$\phi\left(\sum_{i=0}^{n} r_i(t)x^i\right) = \sum_{i=0}^{n} [-x + d(t)]^i r_i(t),$$

for some $b(t) \in K(t)$.

Involutions on $S = K(t)[x;\delta]$

Theorem Let $S = K(t)[x;\delta]$, $a,\ b,\ c \in K$ and $a^2+bc \neq 0$. Then any involution ϕ on S with $\phi(t) = \frac{at+b}{ct-a}$ can be written in

$$\phi\left(\sum_{i=0}^{n} r_i(t)x^i\right) = \sum_{i=0}^{n} [a_1(t)x + b_1(t)]^i \phi(r_i(t)),$$

where $a_1(t) \in K(t)\setminus\{0\}$, $b_1(t) \in K(t)$.

Conversely, let ϕ be a mapping defined above. Then ϕ is an involution on $K(t)[x;\delta]$ *if and only if* $a_1(t) = \frac{(ct-a)^2}{a^2+bc}$, and $b_1(t)$ satisfies

$$\frac{-2c}{ct-a} + b_1(t)\frac{a^2+bc}{(ct-a)^2} + \phi(b_1(t)) = 0.$$

Involutions on $S = K(t)[x;\sigma]$

Consider pure difference operator case, that is, $\delta(t) = 0$.

Theorem Let $S = K(t)[x;\sigma]$. Then any involution ϕ on S with $\phi(t) = t$ can be written as

$$\phi\left(\sum_{i=0}^{n} r_i(t)x^i\right) = \sum_{i=0}^{n} [a_1(t)x]^i r_i(t),$$

where $a_1(t) \in K(t) \setminus \{0\}$ and $r_i(t) \in K(t)$, $i = 0, 1, \ldots, n$.

Conversely, a mapping ϕ defined by above is an involution on $K(t)[x;\sigma]$ if and only if $a_1(t)\sigma(a_1(t)) = 1$ and $\sigma^2(t) = t$.

Involutions on $S = K(t)[x;\sigma]$

Theorem. Let $S = K(t)[x;\sigma]$, $a,\ b,\ c \in K$ and $a^2 + bc \neq 0$. Then any involution ϕ on S with $\phi(t) = \frac{at+b}{ct-a}$ can be written as

$$\phi\left(\sum_{i=0}^{n} r_i(t)x^i\right) = \sum_{i=0}^{n} [a_1(t)x]^i \phi(r_i(t)),$$

where $a_1(t) \in K(t) \setminus \{0\}$.

Furthermore, a mapping ϕ defined aboveis an involution if and only if

$$\sigma(\phi[\sigma(t)]) = \phi(t),\ a_1(t)\sigma[\phi(a_1(t))] = 1.$$

Involutions on $S = K(t)[x;\sigma,\delta]$

For a mixed form,

Theorem Let $S = K(t)[x;\sigma,\delta]$. If $\sigma \neq 1$, $\delta \neq 0$ and $\sigma\delta = \delta\sigma$, then ϕ couldn't be extended to be an involution on S.

Moore-Penrose Inverses

Theorem Let A be an $m \times n$ matrix over S with $m \geq n$ and $\rho(A) = n$ ($m \leq n$ and $\rho(A) = m$, resp.). Then

(i) A has a MP-inverse if and only if A^*A (AA^*, resp.) is invertible.

(ii) If A^*A (AA^*, resp.) is invertible, then $G := (A^*A)^{-1}A^*$ ($G := A^*(AA^*)^{-1}$, resp.) is the MP-inverse of A, and GG^* (G^*G, resp.) is the inverse of A^*A (AA^*, resp.) over S.

Jacobson Form

Let $f, g \in R[x;\sigma,\delta]$. f and g are called similar if there exist $a, b \in R[x;\sigma,\delta]$ such that

$$af = gb,$$

$$R[x;\sigma,\delta] = aR[x;\sigma,\delta] + gR[x;\sigma,\delta],\ R[x;\sigma,\delta] = R[x;\sigma,\delta]b + R[x;\sigma,\delta]f.$$

$A \in R[x;\sigma,\delta]^{n\times n}$ is called unimodular if there exists an $A^{-1} \in R[x;\sigma,\delta]^{n\times n}$ such that $AA^{-1} = A^{-1}A = I$.

Jacobson Form

For $A \in R[x;\sigma,\delta]^{m\times n}$, there exist unimodular matrices $U \in R[x;\sigma,\delta]^{m\times m}$, $V \in R[x;\sigma,\delta]^{n\times n}$ such that

$$UAV = \begin{bmatrix} f_1 & 0 & & \\ 0 & f_2 & & \\ & & \ldots & \\ & & & f_k \\ & & & \end{bmatrix}$$

where $R[x;\sigma,\delta]f_{i+1}R[x;\sigma,\delta] \subseteq f_iR[x;\sigma,\delta] \cap R[x;\sigma,\delta]f_i$, for $f_i \in R[x;\sigma,\delta]$ $i = 1,\ldots,k$, and other entries are zero's.

$\mathrm{Diag}(f_1,\ldots,f_k,0,\ldots,0)$ is called a Jacobson normal form of A.

The simplest form: $\mathrm{Diag}(0,\ldots,g_k,0,\ldots,0)$.

Jacobson Form

Theorem For any $A \in S^{m\times n}$, A has a $\{1\}$-inverse over $S \iff$ there exist invertible matrices $P \in S^{m\times m}$ and $Q \in S^{n\times n}$ such that

$$A = P \begin{bmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} Q,$$

in which case if X is a $\{1\}$-inverse of A over S, then X can be written as

$$Q^{-1} \begin{bmatrix} I_r & W_2 \\ W_3 & W_4 \end{bmatrix} P^{-1},$$

where $W_2 \in S^{r\times(m-r)}$, $W_3 \in S^{(n-r)\times r}$ and $W_4 \in S^{(n-r)\times(m-r)}$ are arbitrary Ore matrices.

Jacobson Form

Corollary For $A \in R[x;\sigma,\delta]^{m\times n}$, if Jacobson form of A is $[I_m, 0]$, then $A\{1\} = A\{1,2,3\}$.

Corollary For $A \in R[x;\sigma,\delta]^{m\times n}$, if Jacobson form of A is $[I_n, 0]^T$, then $A\{1\} = A\{1,2,4\}$.

Jacobson Form

Algorithms for computing Jacobson froms:

- Elementary row and column transformations.
- GCD and LCM methods.
- Using other normal forms.
- LLL algorithm, Lattice reductions, Gröbner bases.

Roth Theorem

Roth Theorem I For any $G \in \mathbb{C}^{m\times n}$, $E \in \mathbb{C}^{m\times p}$ and $F \in \mathbb{C}^{q\times n}$,

$$EX - YF = G,$$

is consistent over $\mathbb{C} \iff \begin{bmatrix} E & G \\ \mathbf{0} & F \end{bmatrix}$ *and* $\begin{bmatrix} E & \mathbf{0} \\ \mathbf{0} & F \end{bmatrix}$, are equivalent.

Roth Theorem II For any $G \in \mathbb{C}^{n\times n}$, $E \in \mathbb{C}^{n\times n}$ and $F \in \mathbb{C}^{n\times n}$,

$$EX - XF = G,$$

is consistent over $\mathbb{C} \iff \begin{bmatrix} E & G \\ \mathbf{0} & F \end{bmatrix}$ *and* $\begin{bmatrix} E & \mathbf{0} \\ \mathbf{0} & F \end{bmatrix}$, are similar.

Roth Theorem

Theorem. For any $G \in S^{m\times n}$, if $E \in S^{m\times p}$ and $F \in S^{q\times n}$ both have $\{1\}$-inverses over S, then

$$EX - YF = G,$$

is consistent over $S \iff \rho\left(\begin{bmatrix} E & G \\ \mathbf{0} & F \end{bmatrix}\right) = \rho\left(\begin{bmatrix} E & \mathbf{0} \\ \mathbf{0} & F \end{bmatrix}\right).$

Equivalence

Definition Two Ore matrices U and $V \in S^{m\times n}$ are called equivalent if $U = MVN$, where $M \in S^{m\times m}$ and $N \in S^{n\times n}$ are two invertible matrices.

Theorem For any $G \in S^{m\times n}$, if $E \in S^{m\times p}$ and $F \in S^{q\times n}$ both have $\{1\}$-inverses over S, then

$$U = \begin{bmatrix} E & G \\ \mathbf{0} & F \end{bmatrix}, \quad V = \begin{bmatrix} E & \mathbf{0} \\ \mathbf{0} & F \end{bmatrix},$$

are equivalent over $S \Longleftrightarrow \rho(U) = \rho(V)$.

Unimodular

An Ore matrix $A \in S^{m\times n}$ is called right (left) unimodular over S if there exists an Ore matrix $B \in S^{n\times m}$ such that $BA = I$ ($AB = I$).

Lemma For any $A \in S^{m\times n}$, A is left unimodular over $S \iff A \in S_m^{m\times n}$ and A has a $\{1\}$-inverse over S.

Lemma For any $A \in S^{m\times n}$, A is right unimodular over $S \iff A \in S_n^{m\times n}$ and A has a $\{1\}$-inverse over S.

$AXB+CYD=E$

Next, we discuss the solutions of $AXB+CYD=E$ over S.

Lemma Let $A \in S^{m\times n}$, $B \in S^{p\times q}$, $C \in S^{m\times t}$, $D \in S^{w\times q}$ and $E \in S^{m\times q}$.

If $\begin{bmatrix} A & C \end{bmatrix} \in S_m^{m\times(n+t)}$ and $\begin{bmatrix} A & C \end{bmatrix}$ has a $\{1\}$-inverse over S, then there exist $M_1 \in S^{n\times m}$, $M_2 \in S^{t\times m}$, $M_3 \in S^{t\times(n+t-m)}$, $M_4 \in S^{n\times(n+t-m)}$, $M_5 \in S^{(n+t-m)\times t}$ and $M_6 \in S^{(n+t-m)\times n}$ such that

$$\begin{bmatrix} A & C \\ M_6 & -M_5 \end{bmatrix} \begin{bmatrix} M_1 & M_4 \\ M_2 & -M_3 \end{bmatrix} = I_{n+t}.$$

$AXB + CYD = E$

Lemma Let $A \in S^{m\times n}$, $B \in S^{p\times q}$, $C \in S^{m\times t}$, $D \in S^{w\times q}$ and $E \in S^{m\times q}$.

If $\begin{bmatrix} B \\ D \end{bmatrix} \in S_q^{(p+w)\times q}$ and $\begin{bmatrix} B \\ D \end{bmatrix}$ has a $\{1\}$-inverse over S, then there exist $M_7 \in S^{q\times w}$, $M_8 \in S^{q\times p}$, $M_9 \in S^{(p+w-q)\times w}$, $M_{10} \in S^{(p+w-q)\times p}$, $M_{11} \in S^{p\times(p+w-q)}$ and $M_{12} \in S^{w\times(p+w-q)}$ such that

$$\begin{bmatrix} M_9 & M_{10} \\ M_7 & -M_8 \end{bmatrix} \begin{bmatrix} M_{12} & D \\ M_{11} & -B \end{bmatrix} = I_{p+w}.$$

$AXB+CYD=E$

Theorem Suppose that Ore matrices A, B, C and D satisfy the conditions of above two lemmas, if A, B, C and D all have $\{1\}$-inverses over S, then the following assertions are equivalent:

1. The matrix equation

$$AXB+CYD=E,$$

has solutions over S.

2. The matrix equation

$$AM_4X_0+Y_0M_{10}B=EM_8B-AM_1E,$$

has solutions over S.

3. The matrix equations

$$AX_1+Y_1D=E, \qquad X_2B+CY_2=E,$$

have solutions over S.

4.

$$\rho\left(\begin{bmatrix} C & E & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & B & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & A & E \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & D \end{bmatrix}\right) = \rho\left(\begin{bmatrix} C & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & B & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & A & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & D \end{bmatrix}\right),$$

over S.

5. The matrix equation

$$\begin{bmatrix} C & \mathbf{0} \\ \mathbf{0} & A \end{bmatrix} X_3 + Y_3 \begin{bmatrix} B & \mathbf{0} \\ \mathbf{0} & D \end{bmatrix} = \begin{bmatrix} E & \mathbf{0} \\ \mathbf{0} & E \end{bmatrix},$$

has solutions over S.

Remark: we assume that A, B, C and D all have $\{1\}$-inverses over S.

$AXB+CYD=E$

Theorem Let $A \in S^{m\times n}$, $B \in S^{p\times q}$, $C \in S^{m\times t}$, $D \in S^{w\times q}$, $E \in S^{m\times q}$, $P = \begin{bmatrix} A & C \end{bmatrix}$ and $Q = \begin{bmatrix} B \\ D \end{bmatrix}$. If $P^{(1)}$ and $Q^{(1)}$ both exist over S, then a necessary and sufficient condition for the matrix equation

$$AXB+CYD=E,$$

to have solutions over S is that there are $P^{(1)}$ and $Q^{(1)}$ over S such that

$$PP^{(1)}EQ^{(1)}Q=E,$$

in which case

$$\begin{bmatrix} X & \mathbf{0} \\ \mathbf{0} & Y \end{bmatrix} = P^{(1)}EQ^{(1)}+Z-P^{(1)}PZQQ^{(1)},$$

is the general solution, where $Z \in S^{(n+t)\times(p+w)}$ is an arbitrary Ore matrix.

Group Inverses

Recall that $A, G \in S^{m\times m}$. G is called a group inverse of A if

$$AGA = A, \quad GAG = G, \quad AG = GA$$

- The group inverse of a given A is unique.

Group Inverses

Theorem Let A be a square matrix over S. The following statements are equivalent.

1. A has a group inverse over S.
2. A has a $\{1\}$-inverse of the form AC for some matrix C over S.
3. A has a $\{1\}$-inverse of the form CA for some matrix C over S.
4. A has a $\{1\}$-inverse of the form ACA for some matrix C over S.
5. $\rho(A) = \rho(A^2)$ and A^2 has $\{1\}$-inverse.
6. $\rho(A) = \rho(A^n)$ and A^n has $\{1\}$-inverse.

Furthermore, if ACA is a $\{1\}$-inverse of A over S, then ACA is the group inverse of A.

Drazin Inverses

Recall that $A, G \in S^{m\times m}$. G is called a Drazin inverse of A with index k if

$$A^{k+1}G = A^k, \quad GAG = G, \quad AG = GA$$

- The Drazin inverse of a given A is unique.

Drazin Inverses

Theorem Let A be an $n \times n$ matrix over S.

1. If A has a Drazin inverse over S with index p, then A^{p+1} has $\{1\}$-inverse over S.

2. If A^{p+k} has $\{1\}$-inverse over S for some integer $k \geq 1$, then both A^{p+k+1} and A^{p+k-1} has $\{1\}$-inverse over S, and A has a Drazin inverse over S.

3. If A^{2p+1} has a $\{1\}$-inverse over S, then $A^p(A^{2p+1})^{\{1\}}A^p$ is the Drazin inverse of A over S.

Group and Drazin Inverses

Theorem Let A be a square matrix over S and let $k \geq p$, $k \in \mathbb{N}$.

Then A has a Drazin inverse with index p over S if and only if A^k has a group inverse over S.