A recursive MEAT-AXE algorithm

Stephen P. Glasby

Central Washington University

November 2009

Overview

1. Four Meat-axe problems: Invar, Cent, Iso, Subfield
2. Non-recursive Meat-axe algorithm
3. Changing field: scaling up $F \rightsquigarrow E$; scaling down $E \rightsquigarrow F$
4. Recursive Meat-axe algorithm
5. Examples
6. Solving norm equations

Input/Output

Motivation:

- Braid group cryptography $\rightsquigarrow$ representations over $\mathbb{Q}(t, q)$
- Integral representation theory

Input:

- $A = \langle X_1, \ldots, X_k \rangle_F$ a f.g. F-subalgebra of $F^{d \times d}$
- F_0 prime subfield; $F_0 \subseteq F_0(B) \subseteq F$ where $F_0(B) : F_0$ purely trans'l $|B| < \infty$ and $|F : F_0(B)| < \infty$ e.g. $F = \mathbb{Q}(x_1, \ldots, x_n)/(f)$

Familiar: $F = \mathbb{Q}$, A is an epimorphic image of gp algebra FG, $|G| < \infty$.

Output: Subspace of $F^{1 \times d}$ invariant under A, or isomorphism, or matrix that conjugates A over a proper subfield, or ...

Algorithms/Applications ($|F| = \infty$): Parker; Holt; Plesken, Souvignier, Schultz, Nebe, Müller; Nickerson; Steel; Cohen; Fieker; Glasby, ...

Goals

Maxim

Aschbacherization applied to MEAT-AXE (induction on d)

Goals

Maxim

Aschbacherization applied to MEAT-AXE (induction on d)

Goals

- MEAT-AXE implementation in GAP and MAGMA for arbitrary fields (for non-experts; moderately efficient; arbitrary algebras)

Goals

Maxim

Aschbacherization applied to MEAT-AXE (induction on d)

Goals

- MEAT-AXE implementation in GAP and MAGMA for arbitrary fields (for non-experts; moderately efficient; arbitrary algebras)
- Improved complexity analysis of MEAT-AXE (especially if $|F| = \infty$)

Goals

Maxim

Aschbacherization applied to MEAT-AXE (induction on d)

Goals

- MEAT-AXE implementation in GAP and MAGMA for arbitrary fields (for non-experts; moderately efficient; arbitrary algebras)
- Improved complexity analysis of MEAT-AXE (especially if $|F| = \infty$)
- Develop constructive representation theory of algebras

Goals

Maxim

Aschbacherization applied to MEAT-AXE (induction on d)

Goals

- MEAT-AXE implementation in GAP and MAGMA for arbitrary fields (for non-experts; moderately efficient; arbitrary algebras)
- Improved complexity analysis of MEAT-AXE (especially if $|F| = \infty$)
- Develop constructive representation theory of algebras
- Unify fields (rep thy of gps and algebras, division algebras, Galois cohomology, second cohomology, computational ANT)

Meat-axe problems: Invar, Cent, Iso, Subfield

Algorithm MeatAxeInvar
Input $A = \langle X_1, \ldots, X_k \rangle_F \leqslant F^{d\times d}$ (f.g. F-subalgebra)
Output A proper non-zero invariant A-invariant subspace of $V := F^{1\times d}$, or a certificate that V is irreducible.

Algorithm MeatAxeCent
Input $A = \langle X_1, \ldots, X_k \rangle_F \leqslant F^{d\times d}$ irreducible
Output The centralizer $C_{F^{d\times d}}(A) = \mathrm{End}_A(V) \leqslant F^{d\times d}$

Algorithm MeatAxeIso
Input An ring iso $\langle X_1, \ldots, X_k \rangle_F \to \langle X'_1, \ldots, X'_k \rangle_F : X_i \mapsto X'_i$, where $\langle X_1, \ldots, X_k \rangle_F$ is irreducible (e.g. Galois isomorphism)
Output $Z \in \mathrm{GL}(d, F)$ such that $Z^{-1}AZ = A'$, or "`NotConjugate`"

Algorithm MeatAxeSubfield
Input $E : F$ (finite & Galois); $A = \langle X_1, \ldots, X_k \rangle_E \leqslant E^{d\times d}$ (abs irred).
Output $Z \in \mathrm{GL}(d, E)$ such that $Z^{-1}AZ \leqslant F^{d\times d}$, or "`NotConjugate`"

Notation

- $V = F^{1\times d}$ right A-mod, and $V^* = F^{d\times 1}$ left A-module
- Special case: A is simple. Then $A \cong D^{r\times r}$, D division alg/F, E max subfield of D. If $D \neq E$, then $|D : E| = |E : Z(D)| = s$ is the (Schur) index. Then $d = rs^2|Z(D) : F|$.
- General case: Then $\frac{A}{\mathrm{Rad}(A)} \cong D_1^{r_1\times r_1} \oplus \cdots \oplus D_n^{r_n\times r_n}$.

Notation

- $V = F^{1\times d}$ right A-mod, and $V^* = F^{d\times 1}$ left A-module
- Special case: A is simple. Then $A \cong D^{r\times r}$, D division alg/F, E max subfield of D. If $D \neq E$, then $|D : E| = |E : Z(D)| = s$ is the (Schur) index. Then $d = rs^2|Z(D) : F|$.
- General case: Then $\frac{A}{\mathrm{Rad}(A)} \cong D_1^{r_1\times r_1} \oplus \cdots \oplus D_n^{r_n\times r_n}$.
- $C := C_{F^{d\times d}}(A) = \mathrm{End}_A(V)$. If A is simple, then $C \cong D^{\mathrm{op}}$.
- $c_Y(t) = \det(tI - Y)$ char poly of $Y \in F^{d\times d}$, $m_Y(t)$ min poly
- If $Y \in C$ and $m_Y(t)$ irred over F, then $E = F[Y] \subseteq C$, $E \cong F[t]/(m_Y(t))$ is an extension field of F, $|E : F| = \deg(m_Y(t))$.

Non-recursive MeatAxe algorithm

Non-recursive versions of MeatAxeInvar, MeatAxeCent, MeatAxeIso, MeatAxeSubfield are similar.

Algorithm MeatAxeInvar
Input $A = \langle X_1, \ldots, X_k \rangle_F \leqslant F^{d \times d}$ (f.g. F-subalgebra)
Output A proper non-zero invariant A-invariant subspace of $V := F^{1 \times d}$, or a certificate that V is irreducible.

Non-recursive MeatAxe algorithm

Non-recursive versions of MeatAxeInvar, MeatAxeCent, MeatAxeIso, MeatAxeSubfield are similar.

Algorithm MeatAxeInvar
Input $A = \langle X_1, \ldots, X_k \rangle_F \leqslant F^{d \times d}$ (f.g. F-subalgebra)
Output A proper non-zero invariant A-invariant subspace of $V := F^{1 \times d}$, or a certificate that V is irreducible.

1. $X :=$ Random(A)
2. Search for a "good" $0 \neq v \in V$ which shows that X is "good."
   If no good v is found (unlikely if X is good), then go to Step 1
3. If $0 \neq vA \neq V$, then return vA.
   // Assume henceforth that $vA = V$ and X is "good."
4. Search for a "good" $0 \neq v^* \in V^*$ (likely to find v^*)
5. If $0 \neq Av^* \neq V^*$, then return $(Av^*)^\perp$.
   // Assume henceforth that $vA = V$ and $Av^* = V^*$ and X is "good."
6. Irreducible:=true; Certif:= (v, X, v^*) by Norton's Irreducibility Criterion

Non-termination

If there are no good $X \in A$, then the procedure loops forever!

Non-termination

If there are no good $X \in A$, then the procedure loops forever!

Definitions of a "good" matrix include:

(1) X has a 1-dimensional λ-eigenspace for some $\lambda \in F$

(2) $c_X(t)$ is divisible by an irreducible poly over F to the first power

(3) X is a cyclic matrix

(4) X is a "primary-cyclic" (or "f-cyclic") matrix

Non-termination

If there are no good $X \in A$, then the procedure loops forever!

Definitions of a "good" matrix include:

(1) X has a 1-dimensional λ-eigenspace for some $\lambda \in F$

(2) $c_X(t)$ is divisible by an irreducible poly over F to the first power

(3) X is a cyclic matrix

(4) X is a "primary-cyclic" (or "f-cyclic") matrix

Definition: Suppose the char poly of $X \in F^{d\times d}$ factors as $c_X = f_1^{k_1} \cdots f_r^{k_r}$ where $f_1, \ldots, f_r \in F[t]$ are irreducible. Then $V = V_1 \oplus \cdots \oplus V_r$ where $V_i = \ker(f_i(X)^{k_i})$ is the ith primary $F[X]$-submodule. We call X primary-cyclic (f-cyclic) if at least one V_i is cyclic. A non-zero vector $v = v_1 + \cdots + v_r$ is called "good" if $v_i F[X] = V_i$ whenever $v_i \neq 0$.

Non-termination

If there are no good $X \in A$, then the procedure loops forever!

Definitions of a "good" matrix include:

(1) X has a 1-dimensional λ-eigenspace for some $\lambda \in F$

(2) $c_X(t)$ is divisible by an irreducible poly over F to the first power

(3) X is a cyclic matrix

(4) X is a "primary-cyclic" (or "f-cyclic") matrix

Definition: Suppose the char poly of $X \in F^{d\times d}$ factors as $c_X = f_1^{k_1} \cdots f_r^{k_r}$ where $f_1, \ldots, f_r \in F[t]$ are irreducible. Then $V = V_1 \oplus \cdots \oplus V_r$ where $V_i = \ker(f_i(X)^{k_i})$ is the ith primary $F[X]$-submodule. We call X primary-cyclic (f-cyclic) if at least one V_i is cyclic. A non-zero vector $v = v_1 + \cdots + v_r$ is called "good" if $v_i F[X] = V_i$ whenever $v_i \neq 0$.

Note (1) $\subseteq$ (2) $\subseteq$ (4) and (3) $\subseteq$ (4).

Non-termination

If there are no good $X \in A$, then the procedure loops forever!

Definitions of a "good" matrix include:

(1) X has a 1-dimensional λ-eigenspace for some $\lambda \in F$

(2) $c_X(t)$ is divisible by an irreducible poly over F to the first power

(3) X is a cyclic matrix

(4) X is a "primary-cyclic" (or "f-cyclic") matrix

Definition: Suppose the char poly of $X \in F^{d\times d}$ factors as $c_X = f_1^{k_1} \cdots f_r^{k_r}$ where $f_1, \ldots, f_r \in F[t]$ are irreducible. Then $V = V_1 \oplus \cdots \oplus V_r$ where $V_i = \ker(f_i(X)^{k_i})$ is the ith primary $F[X]$-submodule. We call X primary-cyclic (f-cyclic) if at least one V_i is cyclic. A non-zero vector $v = v_1 + \cdots + v_r$ is called "good" if $v_i F[X] = V_i$ whenever $v_i \neq 0$.

Note (1) $\subseteq$ (2) $\subseteq$ (4) and (3) $\subseteq$ (4).

Use definition in [SG,CEP, J. Alg. **322**, 2009] not [SG, J. Alg. **300**, 2006]

Finding "good" vectors

Algorithm IsfCyclic in [SG,CP,J. Alg **322**, 2009] takes as input a random element of V and outputs (with high probability when X is f-cyclic) a good v. The algorithm works when $|F| = \infty$ and is Las Vegas $O(\mathrm{MM}(d) \log d)$.

Finding "good" vectors

Algorithm IsfCyclic in [SG,CP,J. Alg **322**, 2009] takes as input a random element of V and outputs (with high probability when X is f-cyclic) a good v. The algorithm works when $|F| = \infty$ and is Las Vegas $O(MM(d) \log d)$.

The certificate (v, X, v^*) for MeatAxeInvar can be used for MeatAxeCent, MeatAxeIso, MeatAxeSub.

Irreducibility criteria $A \leqslant F^{d \times d}$ is irreducible if

- Norton's irreducibility criterion (relates V and V^*)
- $C_{F^{d\times d}}(A) = F$ (proves *absolute* irreducibility)
- V^E abs irred and $(V^E)^\alpha \ncong V^E$ for each $1 \neq \alpha \in \mathrm{Gal}(E/F)$.

Changing field: scaling up $F \rightsquigarrow E$; scaling down $E \rightsquigarrow F$

Multiple ways to change field, see [SG,LK, Comm. Alg. **24**, 1996]

Changing field: scaling up $F \rightsquigarrow E$; scaling down $E \rightsquigarrow F$

Multiple ways to change field, see [SG,LK, Comm. Alg. **24**, 1996]

$V \rightsquigarrow V^E$ is called scaling up (or blowing up the field)
$V^E \rightsquigarrow (V^E)_F$ is called scaling down (or blowing up the dimension)

Changing field: scaling up $F \rightsquigarrow E$; scaling down $E \rightsquigarrow F$

Multiple ways to change field, see [SG,LK, Comm. Alg. **24**, 1996]

$V \rightsquigarrow V^E$ is called scaling up (or blowing up the field)
$V^E \rightsquigarrow (V^E)_F$ is called scaling down (or blowing up the dimension)

Scaling up

(1) $V = F^{1\times d}$, $Y \in C = C_{F^{d\times d}}(A)$, m_Y irreducible/F,
$E = F[Y] \cong F[t]/(m_Y(t))$ field. E-action on V: $v * f(Y) = vf(Y)$.
Note that V^E is an EA-module and $\dim_E(V^E) = \frac{\dim_F(V)}{|E:F|}$.

(2) $V \otimes_F E$ is an $A \otimes_F E$-module with $\dim_E(V \otimes_F E) = \dim_F(V)$

Changing field: scaling up $F \rightsquigarrow E$; scaling down $E \rightsquigarrow F$

Multiple ways to change field, see [SG,LK, Comm. Alg. **24**, 1996]

$V \rightsquigarrow V^E$ is called scaling up (or blowing up the field)
$V^E \rightsquigarrow (V^E)_F$ is called scaling down (or blowing up the dimension)

Scaling up

(1) $V = F^{1\times d}$, $Y \in C = C_{F^{d\times d}}(A)$, m_Y irreducible/F,
$E = F[Y] \cong F[t]/(m_Y(t))$ field. E-action on V: $v * f(Y) = vf(Y)$.
Note that V^E is an EA-module and $\dim_E(V^E) = \frac{\dim_F(V)}{|E:F|}$.

(2) $V \otimes_F E$ is an $A \otimes_F E$-module with $\dim_E(V \otimes_F E) = \dim_F(V)$

Scaling down (inverse of scaling up)

$(V^E)_F = V$, $\dim_F(V^E)_F = |E : F| \dim_E(V^E)$

Scaling up: increasing field and decreasing dimension

Remarks

(1) Scaling up via (1) is useful for recursion, but (2) is not. Disregard (2).

(2) Scaling down is the inverse of scaling up.

(3) $V \rightsquigarrow V^E$ improves the complexity analysis.

(4) Scaling up depends on choice of $Y \in C$, not on field $E = F[Y]$. It is used primarily when $A \cong D^{r\times r}$ and $C \cong D^{\mathrm{op}}$. If $E \cong E'$, then $E^\alpha = E'$ for some $\alpha \in \mathrm{Inn}(A)$ by Skolem-Noether Theorem.

(5) When $A \cong D^{r\times r}, C \cong D^{\mathrm{op}}$, there are many choices for the maximal subfield E, e.g. $D = \left(\frac{\mathbb{Q}}{-1,-1}\right)$ = rational quaternions. $q = q_0 + q_1 i + q_2 j + q_3 k \in D$. Then $E = \mathbb{Q}(i)$ and $E = \mathbb{Q}(\omega)$ with $\omega = \frac{1}{2}(-1 + i + j + k)$ are non-isomorphic maximal subfields. Also A^E acts on V^E and $\mathrm{trace}(X^E) = \mathrm{ReducedTrace}(X)$ indep of E.

(6) If $Y \in Z(D)$, then inner auto α in (4) acts trivially.

Recursive MEAT-AXE algorithm

. . . If no "good" $X \in A$ are found, then we suspect

$$\frac{A}{\mathrm{Rad}(A)} \cong D_1^{r_1 \times r_1} \oplus \cdots \oplus D_n^{r_n \times r_n} \quad \text{where } \forall i,\ \mathrm{Index}(D_i) = s_i > 1$$

With high prob A is central simple. Thus $n = 1$, $A \cong D^{r \times r}$, $Z(D) = F$, and $\mathrm{Index}(D) = s$. Thus $V = \bigoplus_{i=1}^{k} U$ with U unique A-irreducible.
With high probability $ks = \lfloor \frac{d}{\deg(m_Y)} \rfloor$ divides d.
Find by some means $Y \in C$. (If not abs irred, then $\deg(m_Y) > 1$ likely.)
If m_Y is reducible, then return $\ker(f(Y))$ where $f \mid m_Y$ and $1 \neq f \neq m_Y$.
Suppose m_Y is irreducible. Set $E := F[Y]$. If V^E is reducible, say $0 \neq U^E \neq V^E$, then $0 \neq U \neq V$ and U is A-invariant.
If V^E is irred, compute $S := \mathrm{Stab}_{\mathrm{Gal}(E/F)}(V^E)$. If $S = 1$, then V is irred.
If $(V^E)^\alpha \cong V^E$ for $1 \neq \alpha \in S$, and a certain norm equation can be solved, then V^E can be written over the proper fixed subfield $E^{\langle \alpha \rangle}$ (S_3-example)
If $\mathrm{Gal}(E/F)$ soluble and at least one norm equation can not be solved, then V is irreducible (Q_8-example)

S_3-example

$F = \mathbb{Q}, E \cong \mathbb{Q}(\omega)$, $\rho^E : S_3 = \langle x, y \mid x^2 = y^3 = 1, y^x = y^{-1} \rangle \to \mathrm{GL}(2, E)$

$$x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \text{ where } \omega = \zeta_3 \text{ satisfies } \omega^2 + \omega + 1 = 0.$$

$$\rho\colon S_3 \to \mathrm{GL}(4, F)\colon x \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$A = \langle \rho(r), \rho(x) \rangle_F$.

$$Y = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{pmatrix} \in C_{F^{4\times 4}}(A) \cong E^{2\times 2} \quad E = F[Y] \cong \mathbb{Q}(\omega)$$

$\alpha \in \mathrm{Gal}(E/F)$, $\alpha(Y) = Y^{-1}$. MeatAxeSubfield with $X := \rho^E(x)$ writes $\langle \rho^E(x), \rho^E(y) \rangle_F$ over F. Alt: MeatAxeIso with $X := \rho^E(x)$ conjugates $(V^E)^\alpha$ to V^E. Now $N_{E/F}(X) = XX^\alpha = I$, and $N_{E/F}(\mu) = 1$ has a sol'n. Thus V^E can be written over F, and $V = U \oplus U$ splits.

Q_8-example

$F = \mathbb{Q}$, $E \cong \mathbb{Q}(\sqrt{-1})$, $\quad \rho^E : Q_8 = \langle x, y \mid x^2 = y^2, y^x = y^{-1} \rangle \to \mathrm{GL}(2, E)$

$x \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\quad y \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ where $i = \sqrt{-1}$.

$$\rho : Q_8 \to \mathrm{GL}(4, F) : x \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$A = \langle \rho(x), \rho(y) \rangle_F \leqslant F^{4\times 4}$, $\quad A \cong \left(\begin{smallmatrix} \mathbb{Q} \\ -1, -1 \end{smallmatrix}\right)$.

$$Y = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \in C_{F^{4\times 4}}(A) \cong E^{2\times 2} \quad E = F[Y] \cong \mathbb{Q}(i)$$

$\alpha \in \mathrm{Gal}(E/F)$, $\alpha(Y) = -Y$ and $(V^E)^\alpha \cong V^E$. MeatAxeIso with $X = \rho^E(x)$ conjugates $(V^E)^\alpha$ to V^E. Now $N_{E/F}(X) = XX^\alpha = -I$ and $N_{E/F}(\mu) = -1$ has no sol'n. Thus V^E can not be written over F, and V irred.

Solving norm equations

In the previous Q_8-example the norm map $N_{E/F}\colon \mathbb{Q}(i)^\times \to \mathbb{Q}^\times$ was non-surjective. This can also happen in positive characteristic. For example: $E = \mathbb{F}_2(x)$, $F = \mathbb{F}_2(x + x^{-1})$, and $A = (E, \mathrm{Gal}(E/F), x)$.

Given $E : F$ (finite and Galois) and $\lambda \in F$ find (if possible) $\mu \in E$ such that $N_{E/F}(\mu) = \lambda$. (Norm eqns in MAGMA can be SLOW)

WMA $\mathrm{Gal}(E/F)$ is simple, commonly $\mathrm{Gal}(E/F) \cong C_p$ where p is prime. (Can have $E = \mathbb{Q}(x_1, \ldots, x_5)$, $F = E^{A_5}$, and $\mathrm{Gal}(E/F) \cong A_5$.)

Finding $Z \in \mathrm{GL}(d, E)$ s.t. $Z^{-1}\langle X_1, \ldots, X_k\rangle_F Z \leqslant F^{d\times d}$ is equivalent to splitting a 1-cocyle $C : \mathrm{Gal}(E/F) \to E^\times$ i.e. $C_\alpha = Z(Z^{-1})^\alpha$.

For each generator α of $G := \mathrm{Gal}(E/F)$ find Z_α such that $Z_\alpha^{-1} X_i Z_\alpha = X_i^\alpha$ for each i. Then $Z_{\alpha\beta} = \lambda(\alpha, \beta) Z_\alpha (Z_\beta)^\alpha$ where $\lambda \in H^2(G, E^\times)$.

Brauer-Hasse-Noether theorem says λ is a 2-coboundary iff $\lambda_P \in H^2(G_P, E_P^\times)$ is a 2-coboundary $\forall$ places P of E, c.f. [Fieker, 2009].

Finding good $X \in A$, or $Y \in C := C_{F^{d\times d}}(A)$

- Choose sufficiently many random elements of A, say $X_1', \ldots, X_m'$, such that the first rows $e_1X_1', \ldots, e_1X_m'$ are linearly dependent, say $\sum \alpha_i(e_1X_i') = 0$. If $X := \sum \alpha_i X_i' \neq 0$ has 1-dimensional 0-eigenspace, then X is good. (If $X \neq 0$ and the 0-eigenspace has dimension > 1, then use the regular representation of A on XA.)
- Used X to split V, or find $Y \in C$.
- $Y \in C$ normalizes the $F[X]$-primary submodules of V for each $X \in A$
- If m_X is irreducible, then $\dim(C_{F^{d\times d}}(X)) = d^2/\deg(m_X)$.

I will post this talk on my home page: http://www.cwu.edu/∼glasbys/

Thank you!