A similarity test for Ore polynomials

J. Gómez-Torrecillas[†], F. J. Lobillo[†] and **G. Navarro**[‡]

†Department of Algebra, University of Granada

‡**Dep. of Computer Sciences and AI, University of Granada**

EACA 2014, June 18-20, 2014

Work published in:

- Proceedings of the 39th International Symposium on International Symposium on Symbolic and Algebraic Computation (ISSAC '14)
- Arxiv (extended and improved version)...coming soon

Motivation

- Coding theory
  - Cyclic convolutional codes
  - Convolutional codes with additional structure
- Pure mathematical interest!

...need of efficient algorithms over skew/Ore polynomial

Ore polynomials

Background (Ore, 1933)

$R = D[x; \sigma, \delta]$ Ore polynomial ring

- D is a division ring
- $\sigma : D \to D$ automorphism
- $\delta : D \to D$ σ-derivation, $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$
- R is a left D-vector space with basis $\{x^i \text{ with } i \geq 0\}$
- ...so elements of R are polynomials, $a_0 + a_1 x + \cdots + a_n x^n$
- Product:

$$x^n x^m = x^{n+m} \text{ and } xa = \sigma(a)x + \delta(a)$$

Ore polynomials

Background (Ore, 1933)

$R = D[x; \sigma, \delta]$ Ore polynomial ring

- D is a division ring
- $\sigma : D \to D$ automorphism
- $\delta : D \to D$ σ-derivation, $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$
- R is a left D-vector space with basis $\{x^i \text{ with } i \geq 0\}$
- ...so elements of R are polynomials, $a_0 + a_1 x + \cdots + a_n x^n$
- Product:

$$x^n x^m = x^{n+m} \text{ and } xa = \sigma(a)x + \delta(a)$$

Basic properties

- Non-commutative ring
- Left and right Euclidean division (Euclidean domain)
- Left and right greatest common divisor and least common multiple
- ...so left and right non-commutative PID

Example

Non unique factorization

Let $\mathbb{F}_4 = \{0, 1, a, a+1\}$ and $\sigma(a) = a^2 = a + 1$, and $R = \mathbb{F}_4[x; \sigma]$. Hence

- $x^2 + 1 = (x + 1)(x + 1)$
- $x^2 + 1 = (x + a)(x + a + 1)$

Two different factorizations of $x^2 + 1$

Example

Non unique factorization

Let $\mathbb{F}_4 = \{0, 1, a, a+1\}$ and $\sigma(a) = a^2 = a + 1$, and $R = \mathbb{F}_4[x; \sigma]$. Hence

- $x^2 + 1 = (x + 1)(x + 1)$
- $x^2 + 1 = (x + a)(x + a + 1)$

Two different factorizations of $x^2 + 1$

Non unique factorization

Let $R = \mathbb{Q}(t)[X; d/dt]$ the ring of differential operators over $\mathbb{Q}(t)$

$$x^2 = \left(x + \frac{1}{t+z}\right)\left(x - \frac{1}{t+z}\right), \qquad (z \in \mathbb{Q})$$

There exist infinitely many (different) factorizations of x^2...

Similar elements

Similarity

Two elements $a, b \in R = D[x; \sigma, \delta]$ are similar ($a \sim b$) if

- $R/Ra \cong R/Rb$ as left R–modules or, equivalently,
- $R/aR \cong R/bR$ as right R–modules.

As a consequence of Jordan-Hölder's Theorem, we deduce

Theorem (Ore, Jacobson)

Any element in R may be written as a product of irreducibles, and this decomposition in unique up to reordering and similarity

Similar elements

Similarity

Two elements $a, b \in R = D[x; \sigma, \delta]$ are similar ($a \sim b$) if

- $R/Ra \cong R/Rb$ as left R–modules or, equivalently,
- $R/aR \cong R/bR$ as right R–modules.

As a consequence of Jordan-Hölder's Theorem, we deduce

Theorem (Ore, Jacobson)

Any element in R may be written as a product of irreducibles, and this decomposition in unique up to reordering and similarity

Main problem (in this talk)

Decide whether two elements a and b are similar

Index

Background

Principal Ideal Domains (Jacobson, 1943)

- R is a non commutative (left and right) PID
  - No non-zero zero divisor
  - Left ideals are principal, right ideals are principal
- Two-sided ideals are $\alpha R = R\alpha$, α two-sided
- $R(a,b)_r = Ra + Rb$ right greatest common divisor
- $R[a,b]_l = Ra \cap Rb$ left least common multiple
- $a \sim b \Leftrightarrow R/Ra \cong R/Rb$

Theorem (Structure theorem of finitely generated modules)

Any finitely generated left R-module M is of the form

$$M \cong \underbrace{R^s}_{\text{free part}} \oplus \underbrace{\frac{R}{Ra_1} \oplus \cdots \oplus \frac{R}{Ra_n}}_{\text{torsion cyclic modules}}$$

Background

Annihilator

Let M be a left R-module

$$\mathrm{Ann}_R(M) = \{a \in R : am = 0 \ \forall m \in M\}.$$

$\mathrm{Ann}_R(M)$ is a two-sided ideal

Definition

A left R-module is *bounded* if $\mathrm{Ann}_R(M) \neq 0$

Corollary

Any finitely generated and bounded left R-module is a direct sum of bounded cyclic modules

Reduction to the center

Let $C = C(R)$ be the center of R

Definition

A finitely generated bounded left R-module M is **centrally bounded** if any maximal two-sided ideal containing its annihilator is generated by an element in the center, i.e. if $\mathrm{Ann}_R(M) \subseteq P$, $P = R\alpha$ with $\alpha \in C$.

Theorem

Assume that R is free of finite rank over its center C, and M and N two centrally bounded left R-modules. The following are equivalent

- $M \cong N$ *as left R-modules*
- $M \cong N$ *as left C-modules*

Index

Back to Ore polynomials

Restrictions

In this work,

- $[D : C(D)] < \infty$
- $\delta = 0$ and $R = D[x; \sigma]$
- σ^μ is inner, for some μ, i.e. $\sigma^\mu(a) = uau^{-1}$ for some $u \in D$

Back to Ore polynomials

Restrictions

In this work,

- $[D : C(D)] < \infty$
- $\delta = 0$ and $R = D[x; \sigma]$
- σ^μ is inner, for some μ, i.e. $\sigma^\mu(a) = uau^{-1}$ for some $u \in D$

Jacobson, Cohn

Let $R = D[x; \sigma]$, then the center $C = C(R) = K[u^{-1}x^\mu]$, where

- $K = D^\sigma \cap C(D)$ (invariants by σ in the center)
- μ first power doing σ inner
- $\sigma^\mu(a) = uau^{-1}$

Under these conditions R has finite rank over its center.

Similarity of polynomials

Theorem (that we wish to obtain)

Let $f, g \in D[x;\sigma]$, the following are equivalent:

- *f and g are similar*
- *$R/Rf \cong R/Rg$ as R-modules*
  $\Uparrow$ *Theorem above*
- ***$R/Rf \cong R/Rg$ as C-modules***

Similarity of polynomials

Theorem (that we wish to obtain)

Let $f, g \in D[x;\sigma]$, the following are equivalent:

- *f and g are similar*
- *$R/Rf \cong R/Rg$ as R-modules*
  $\Uparrow$ *Theorem above*
- ***$R/Rf \cong R/Rg$ as C-modules***

Almost,

Proposition

R/Rf centrally bounded $\iff$ f x-torsionfree $\iff$ $(f,x)_r = 1$

Similarity of polynomials

Theorem (that we wish to obtain)

Let $f, g \in D[x;\sigma]$, the following are equivalent:

- *f and g are similar*
- *$R/Rf \cong R/Rg$ as R-modules*
  $\Uparrow$ *Theorem above*
- ***$R/Rf \cong R/Rg$ as C-modules***

Almost,

Proposition

R/Rf centrally bounded $\iff$ f x-torsionfree $\iff$ $(f,x)_r = 1$

Theorem

Let $f, g \in D[x;\sigma]$ x-torsionfree TFAE:

- *f and g are similar*
- *$R/Rf \cong R/Rg$ as C-modules*

Question

What about non x-torsionfree polynomials?

Question

What about non x-torsionfree polynomials?

Solution,

Proposition

Let $f, g \in D[x;\sigma]$ with $f = f'x^r$ and $g = g'x^s$ where f', g' x-torsionfree

- $\dfrac{R}{Rf} \cong \dfrac{R}{Rf'} \oplus \dfrac{R}{Rx^r}$
- $\dfrac{R}{Rg} \cong \dfrac{R}{Rg'} \oplus \dfrac{R}{Rx^s}$
- *$f \sim g$ if and only if $r = s$ and $f' \sim g'$.*

Similarity of x-torsionfree polynomials

Let $f, g \in D[x;\sigma]$ x-torsionfree.

Recall that

- $C = K[z]$ commutative polynomial ring with $z = u^{-1}x^{\mu}$
- R/Rf, R/Rg are finitely generated torsion C-modules
- There is matrix associated to any finitely generated torsion module (multiplication by z)
- Two modules are isomorphic if and only if the rational canonical forms are the same

Similarity of x-torsionfree polynomials

Let $f, g \in D[x;\sigma]$ x-torsionfree.

Recall that

- $C = K[z]$ commutative polynomial ring with $z = u^{-1}x^{\mu}$
- R/Rf, R/Rg are finitely generated torsion C-modules
- There is matrix associated to any finitely generated torsion module (multiplication by z)
- Two modules are isomorphic if and only if the rational canonical forms are the same

Procedure

- Step 1. Construct the matrices of R/Rf and R/Rg
- Step 2. Compute their rational canonical forms
- Step 3. Check equality

Matrix construction

$\mathcal{B} = \{u_0, \dots, u_{\mu-1}\}$ basis of D over K
$C = K[u^{-1}x^{\mu}]$ for some $u \in D$

Function 1 Matrix of R/Rf as C-module

```
1: function MatrixConstruction(f)
2:     n = deg(f)
3:     B_1 = {u_i x^j : 0 ≤ i < μ, 0 ≤ j < n}
4:     Let M be an "empty matrix"
5:     for 0 ≤ j < n do
6:         for 0 ≤ i < ρ do
7:             r =remainder of the left division of u^{-1} x^μ u_i x^j by f
8:             Add to M a new row with the coefficients of r with respect to B_1
9:     return M
```

Similarity test

Algorithm 2 Similarity in generic setting

Input: $f, g \in R = D[x;\sigma]$ and a basis $\{u_0, \dots, u_{\mu-1}\}$ of D over K.
Output: `True` if they are similar or `False` otherwise.

1: **if** $\deg(f) \neq \deg(g)$ **then**
2: **return** `False`
3: Decompose $f = cf'x^r$ and $g = dg'x^s$ (f', g' monic, x-torsionfree)
4: **if** $r \neq s$ **then**
5: **return** `False`
6: Let $R_{f'}$ = rational canonical form of MatrixConstruction(f')
7: Let $R_{g'}$ = rational canonical form of MatrixConstruction(g')
8: **if** $R_{f'} \neq R_{g'}$ **then**
9: **return** `False`
10: **return** `True`

Example: Quaternions

Let $R = \mathbb{H}[x;\sigma]$, where

- $\mathbb{H} = \mathbb{Q}[1, i, j, k]$ Hamilton quaternions over the rationals.
- $u = 1 + i$
- $\sigma : \mathbb{H} \to \mathbb{H}$ with $\sigma(a) = uau^{-1}$

Example: Quaternions

Let $R = \mathbb{H}[x;\sigma]$, where

- $\mathbb{H} = \mathbb{Q}[1,i,j,k]$ Hamilton quaternions over the rationals.
- $u = 1 + i$
- $\sigma : \mathbb{H} \to \mathbb{H}$ with $\sigma(a) = uau^{-1}$

Hence $C(R) = C = K[u^{-1}x^{\mu}]$, where

- $K = \mathbb{H}^{\sigma} \cap C(\mathbb{H}) = \mathbb{Q}[i] \cap \mathbb{Q} = \mathbb{Q}$
- $\mu =$ first power of σ to be inner, so $\mu = 1$

Example: Quaternions

Let $R = \mathbb{H}[x;\sigma]$, where

- $\mathbb{H} = \mathbb{Q}[1,i,j,k]$ Hamilton quaternions over the rationals.
- $u = 1 + i$
- $\sigma : \mathbb{H} \to \mathbb{H}$ with $\sigma(a) = uau^{-1}$

Hence $C(R) = C = K[u^{-1}x^{\mu}]$, where

- $K = \mathbb{H}^{\sigma} \cap C(\mathbb{H}) = \mathbb{Q}[i] \cap \mathbb{Q} = \mathbb{Q}$
- $\mu =$ first power of σ to be inner, so $\mu = 1$

so

- $C = \mathbb{Q}[z]$, where $z = u^{-1}x$.
- $b = \{1,i,j,k\}$ is a basis of $\mathbb{H}$ over $\mathbb{Q}$
- $b = \{1,i,j,k\}$ is a basis of R over C

Are similar?

$f = x^2 + \left(\frac{1}{3} + \frac{1}{4}i - 2k\right)x + \left(-\frac{1}{2} - i - 3j - \frac{1}{6}k\right)$
$g = x^2 + \left(\frac{1}{4} + \frac{1}{3}i - 2k\right)x + \left(\frac{1}{2} - i - 3j - \frac{1}{6}k\right)$

Matrix construction for f ($u^{-1} = \frac{1}{2} - \frac{1}{2}i$)

$u^{-1}xb_ix^j$		Corresponding row							
$u^{-1}x$	$\longrightarrow$	0	0	0	0	$\frac{1}{2}$	$-\frac{1}{2}$	0	0
$u^{-1}xi$	$\longrightarrow$	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0
$u^{-1}xj$	$\longrightarrow$	0	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$
$u^{-1}kxk$	$\longrightarrow$	0	0	0	0	0	0	$-\frac{1}{2}$	$\frac{1}{2}$
$u^{-1}x^2$	$\longrightarrow$	$\frac{3}{4}$	$\frac{1}{4}$	$\frac{19}{12}$	$-\frac{17}{12}$	$-\frac{7}{24}$	$\frac{1}{24}$	1	1
$u^{-1}xix$	$\longrightarrow$	$-\frac{1}{4}$	$\frac{3}{4}$	$\frac{17}{12}$	$\frac{19}{12}$	$-\frac{1}{24}$	$-\frac{7}{24}$	-1	1
$u^{-1}jxjx$	$\longrightarrow$	$-\frac{19}{12}$	$-\frac{17}{12}$	$\frac{3}{4}$	$-\frac{1}{4}$	-1	1	$-\frac{7}{24}$	$-\frac{1}{24}$
$u^{-1}kxkx$	$\longrightarrow$	$\frac{17}{12}$	$-\frac{19}{12}$	$\frac{1}{4}$	$\frac{3}{4}$	-1	-1	$\frac{1}{24}$	$-\frac{7}{24}$

$$M_f = \begin{pmatrix} 0 & 0 & 0 & 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\ \frac{3}{4} & \frac{1}{4} & \frac{19}{12} & -\frac{17}{12} & -\frac{7}{24} & \frac{1}{24} & 1 & 1 \\ -\frac{1}{4} & \frac{3}{4} & \frac{17}{12} & \frac{19}{12} & -\frac{1}{24} & -\frac{7}{24} & -1 & 1 \\ -\frac{19}{12} & -\frac{17}{12} & \frac{3}{4} & -\frac{1}{4} & -1 & 1 & -\frac{7}{24} & -\frac{1}{24} \\ \frac{17}{12} & -\frac{19}{12} & \frac{1}{4} & \frac{3}{4} & -1 & -1 & \frac{1}{24} & -\frac{7}{24} \end{pmatrix}$$

$$M_g = \begin{pmatrix} 0 & 0 & 0 & 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{4} & \frac{3}{4} & \frac{19}{12} & -\frac{17}{12} & -\frac{7}{24} & -\frac{1}{24} & 1 & 1 \\ -\frac{3}{4} & \frac{1}{4} & \frac{17}{12} & \frac{19}{12} & \frac{1}{24} & -\frac{7}{24} & -1 & 1 \\ -\frac{19}{12} & -\frac{17}{12} & \frac{1}{4} & -\frac{3}{4} & -1 & 1 & -\frac{7}{24} & \frac{1}{24} \\ \frac{17}{12} & -\frac{19}{12} & \frac{3}{4} & \frac{1}{4} & -1 & -1 & -\frac{1}{24} & -\frac{7}{24} \end{pmatrix}$$

$$R_f = \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & -\frac{185}{72} & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -\frac{137}{48} & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -\frac{313}{288} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -\frac{7}{12} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{185}{72} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -\frac{137}{48} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -\frac{313}{288} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -\frac{7}{12} \end{array}\right)$$

$$R_g = \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & -\frac{185}{72} & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -\frac{137}{48} & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -\frac{313}{288} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -\frac{7}{12} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{185}{72} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -\frac{137}{48} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -\frac{313}{288} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -\frac{7}{12} \end{array}\right)$$

Example: Rational functions over a finite field

Let $R = \mathbb{F}_{16}(t)[x;\sigma]$, where

- $\mathbb{F}_{16} = \mathbb{F}_2[a]/(a^4 + a + 1)$
- $\mathbb{F}_{16}(t)$ rational functions over $\mathbb{F}_{16}$
- $\sigma : \mathbb{F}_{16}(t) \to \mathbb{F}_{16}(t)$ with $\sigma(t) = a^5 t$

Example: Rational functions over a finite field

Let $R = \mathbb{F}_{16}(t)[x;\sigma]$, where

- $\mathbb{F}_{16} = \mathbb{F}_2[a]/(a^4 + a + 1)$
- $\mathbb{F}_{16}(t)$ rational functions over $\mathbb{F}_{16}$
- $\sigma : \mathbb{F}_{16}(t) \to \mathbb{F}_{16}(t)$ with $\sigma(t) = a^5 t$

Hence $C(R) = C = K[u^{-1}x^{\mu}]$, where

- $K = \mathbb{F}_{16}(t)^{\sigma} \cap C(\mathbb{F}_{16}(t)) = \mathbb{F}_{16}(t^3) = \mathbb{F}_{16}(s)$
- $\sigma^3 = 1$, so $u = 1$ and $\mu = 3$

Example: Rational functions over a finite field

Let $R = \mathbb{F}_{16}(t)[x;\sigma]$, where

- $\mathbb{F}_{16} = \mathbb{F}_2[a]/(a^4 + a + 1)$
- $\mathbb{F}_{16}(t)$ rational functions over $\mathbb{F}_{16}$
- $\sigma : \mathbb{F}_{16}(t) \to \mathbb{F}_{16}(t)$ with $\sigma(t) = a^5 t$

Hence $C(R) = C = K[u^{-1}x^{\mu}]$, where

- $K = \mathbb{F}_{16}(t)^{\sigma} \cap C(\mathbb{F}_{16}(t)) = \mathbb{F}_{16}(t^3) = \mathbb{F}_{16}(s)$
- $\sigma^3 = 1$, so $u = 1$ and $\mu = 3$

so

- $C = \mathbb{F}_{16}(s)[z]$, where $s = t^3$ and $z = x^3$
- $b = \{1, t, t^2\}$ is a basis of $\mathbb{F}_{16}(t)$ over $\mathbb{F}_{16}(s)$
- $\{1, t, t^2, x, tx, t^2x, x^2, tx^2, t^2x^2\}$ is a basis of R over C

Are similar?

$f = x^2 + atx + \frac{1}{t}$
$g = x^2 + \frac{1}{a^3 t}x + t$

Matrix construction for f

$b_i x^{j+3}$		Corresponding row					
x^3	$\longrightarrow$	a^6	0	0	0	0	$\frac{a^7 s + a^{10}}{s}$
$x^3 t$	$\longrightarrow$	0	a^6	0	$a^7 s + a^{10}$	0	0
$x^3 t^2$	$\longrightarrow$	0	0	a^6	0	$a^7 s + a^{10}$	0
x^4	$\longrightarrow$	0	$\frac{a^2 s + a^5}{s}$	0	$a^3 s$	0	0
$x^3 tx$	$\longrightarrow$	0	0	$\frac{a^2 s + a^5}{s}$	0	$a^3 s$	0
$x^3 t^2 x$	$\longrightarrow$	$a^2 s + a^5$	0	0	0	0	$a^3 s$

$$M_f = \begin{pmatrix} a^6 & 0 & 0 & 0 & 0 & \frac{a^7s+a^{10}}{s} \\ 0 & a^6 & 0 & a^7s+a^{10} & 0 & 0 \\ 0 & 0 & a^6 & 0 & a^7s+a^{10} & 0 \\ 0 & \frac{a^2s+a^5}{s} & 0 & a^3s & 0 & 0 \\ 0 & 0 & \frac{a^2s+a^5}{s} & 0 & a^3s & 0 \\ a^2s+a^5 & 0 & 0 & 0 & 0 & a^3s \end{pmatrix}$$

$$M_g = \begin{pmatrix} a^7 & 0 & 0 & 0 & \frac{a^5s+a^4}{s} & 0 \\ 0 & a^7 & 0 & 0 & 0 & \frac{a^5s+a^4}{s} \\ 0 & 0 & a^7 & a^5s+a^4 & 0 & 0 \\ 0 & 0 & \frac{a^{10}s+a^9}{s} & \frac{1}{a^9s} & 0 & 0 \\ a^{10}s+a^9 & 0 & 0 & 0 & \frac{a^6}{s} & 0 \\ 0 & a^{10}s+a^9 & 0 & 0 & 0 & \frac{1}{a^9s} \end{pmatrix}$$

$$R_f = \left(\begin{array}{cc|cc|cc} 0 & \frac{1}{s} & 0 & 0 & 0 & 0 \\ 1 & a^3s+a^6 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \frac{1}{s} & 0 & 0 \\ 0 & 0 & 1 & a^3s+a^6 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & \frac{1}{s} \\ 0 & 0 & 0 & 0 & 1 & a^3s+a^6 \end{array}\right)$$

$$R_g = \left(\begin{array}{cc|cc|cc} 0 & s & 0 & 0 & 0 & 0 \\ 1 & \frac{as+1}{a^9s} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & s & 0 & 0 \\ 0 & 0 & 1 & \frac{as+1}{a^9s} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & s \\ 0 & 0 & 0 & 0 & 1 & \frac{as+1}{a^9s} \end{array}\right)$$

Index

Improvement

Corollary

Let $f, g \in R = D[x;\sigma]$ and S commutative algebra with $C \subseteq S \subseteq R$, TFAE:

- $f \sim g$
- $R/Rf \cong R/Rg$ *as left modules over S (or over C, or over R)*

Improvement (finite fields)

Basics

- $\mathbb{F} = \mathbb{F}_{p^s}$, p prime
- $\sigma = \tau^h$, $\tau(a) = a^p$ (Frobenius' automorphism)
- σ has finite order $\mu = \frac{s}{(s,h)}$
- $[\mathbb{F} : \mathbb{F}^\sigma] = \mu$
- $C = \mathbb{F}^\sigma[z]$, with $z = x^\mu$

Improvement (finite fields)

Basics

- $\mathbb{F} = \mathbb{F}_{p^s}$, p prime
- $\sigma = \tau^h$, $\tau(a) = a^p$ (Frobenius' automorphism)
- σ has finite order $\mu = \frac{s}{(s,h)}$
- $[\mathbb{F} : \mathbb{F}^\sigma] = \mu$
- $C = \mathbb{F}^\sigma[z]$, with $z = x^\mu$

Corollary

Let $f, g \in R = \mathbb{F}[x;\sigma]$ *and* $\mu = [\mathbb{F} : \mathbb{F}^\sigma]$, *TFAE:*

- $f \sim g$
- $R/Rf \cong R/Rg$ *as left modules over* $C = \mathbb{F}^\sigma[z]$, *with* $z = x^\mu$
- $R/Rf \cong R/Rg$ *as left modules over* $T = \mathbb{F}[z]$, *with* $z = x^\mu$
- $R/Rf \cong R/Rg$ *as left modules over* $S = \mathbb{F}^\sigma[x]$

Module structure over T

- $T = \mathbb{F}[z]$, where $z = x^{\mu}$ and $\mu = \mathrm{ord}(\sigma)$
- T-module structure multiplying by $z = x^{\mu}$

Module structure over T

- $T = \mathbb{F}[z]$, where $z = x^\mu$ and $\mu = \mathrm{ord}(\sigma)$
- T-module structure multiplying by $z = x^\mu$

Function 4 Matrix of R/Rf as T-module

```
1: function MatrixConstructionT(f)
2:     n = deg(f)
3:     B_2 = {1, x, ..., x^{n-1}}
4:     Let M be an "empty matrix"
5:     for 0 ≤ i < n do
6:         r =remainder of the left division of x^{μ+i} by f
7:         Add to M a new row with the coefficients of r with respect to B_2
8:     return M
```

Similarity test using T

Algorithm 5 Similarity over a finite field using T

Input: $f, g \in R = \mathbb{F}[x; \sigma]$

Output: `True` if they are similar or `False` otherwise.

1: **if** $\deg(f) \neq \deg(g)$ **then**
2: **return** `False`
3: Decompose $f = cf'x^r$ and $g = dg'x^s$ (f', g' monic, x-torsionfree)
4: **if** $r \neq s$ **then**
5: **return** `False`
6: Let $R_{f'}$ = rational form of MatrixConstructionT(f')
7: Let $R_{g'}$ = rational form of MatrixConstructionT(g')
8: **if** $R_{f'} \neq R_{g'}$ **then**
9: **return** `False`
10: **return** `True`

Are similar?

- $\mathbb{F}_{2^8}[x;\tau^2]$, hence $\mu = 4$
- a primitive element of $\mathbb{F}_{2^8}$
- $f = x^8 + a^{125}x^7 + a^{36}x^6 + a^{122}x^5 + a^{218}x^4 + a^{50}x^3 + a^{238}x^2 + a^{202}x + a^{21}$
- $g = x^8 + a^{51}x^7 + a^{238}x^6 + a^{51}x^5 + x^4 + a^{153}x^3 + a^{34}x^2 + a^{51}x + 1$

Matrix construction for f

x^{i+4}		Corresponding row							
x^4	$\longrightarrow$	0	0	0	0	1	0	0	0
x^5	$\longrightarrow$	0	0	0	0	0	1	0	0
x^6	$\longrightarrow$	0	0	0	0	0	0	1	0
x^7	$\longrightarrow$	0	0	0	0	0	0	0	1
x^8	$\longrightarrow$	a^{21}	a^{202}	a^{238}	a^{50}	a^{218}	a^{122}	a^{36}	a^{125}
x^9	$\longrightarrow$	a^{11}	a^{245}	a^{37}	a^{93}	a^{145}	a^{245}	a^{231}	a^{41}
x^{10}	$\longrightarrow$	a^{185}	a^{5}	a^{164}	a^{178}	a^{138}	a^{137}	a^{233}	a^{228}
x^{11}	$\longrightarrow$	a^{168}	a^{128}	a^{146}	a^{129}	a^{129}	a^{207}	a^{54}	a^{160}

$$M_f = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ a^{21} & a^{202} & a^{238} & a^{50} & a^{218} & a^{122} & a^{36} & a^{125} \\ a^{11} & a^{245} & a^{37} & a^{93} & a^{145} & a^{245} & a^{231} & a^{41} \\ a^{185} & a^{5} & a^{164} & a^{178} & a^{138} & a^{137} & a^{233} & a^{228} \\ a^{168} & a^{128} & a^{146} & a^{129} & a^{129} & a^{207} & a^{54} & a^{160} \end{pmatrix}$$

$$M_g = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & a^{51} & a^{34} & a^{153} & 1 & a^{51} & a^{238} & a^{51} \\ a^{204} & 0 & a^{85} & a^{238} & a^{68} & 0 & 1 & a^{204} \\ a^{51} & a^{34} & a^{85} & a^{238} & a^{85} & a^{187} & a^{34} & a^{221} \\ a^{119} & a^{51} & a^{204} & a^{34} & a^{136} & 1 & a^{136} & a^{17} \end{pmatrix}$$

$$R_f = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & a^{85} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & a^{85} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & a^{170} \end{pmatrix}$$

$$R_g = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & a^{85} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & a^{85} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & a^{170} \end{pmatrix}$$

Module structure over S

- $S = \mathbb{F}^\sigma[x]$
- a primitive element of $\mathbb{F}$
- $\{1, a, \ldots, a^{\mu-1}\}$ is a basis of $\mathbb{F}$ over $\mathbb{F}^\sigma$
- S–module structure is given by left multiplication by x

Function 6 Matrix of R/Rf as S-module

```
1: function MatrixConstructionS(f)
2:     n = deg(f)
3:     B_3 = {a^i x^j : 0 ≤ i < μ, 0 ≤ j < n}
4:     Let M be a matrix with no rows and nμ columns.
5:     for 0 ≤ j < n do
6:         for 0 ≤ i < μ do
7:             r =remainder of the left division of x a^i x^j = σ(a^i) x^{1+j} by f
8:             Add to M a new row with the coefficients of r with respect to B_3
9:     return M
```

Similarity test using S

Algorithm 7 Similarity over a finite field using S

Input: $f, g \in R = \mathbb{F}[x; \sigma]$

Output: `True` if they are similar or `False` otherwise.

1: **if** $\deg(f) \neq \deg(g)$ **then**
2: **return** `False`
3: Decompose $f = cf'x^r$ and $g = dg'x^s$ (f', g' monic, x-torsionfree)
4: **if** $r \neq s$ **then**
5: **return** `False`
6: Let $R_{f'}$ = rational form of MatrixConstructionS(f')
7: Let $R_{g'}$ = rational form of MatrixConstructionS(g')
8: **if** $R_{f'} \neq R_{g'}$ **then**
9: **return** `False`
10: **return** `True`

Are similar?

- $\mathbb{F}_4[x;\tau]$, hence $\mu = 2$
- $f = x^6 + (a+1)\,x^5 + x^3 + ax^2 + ax + 1$
- $g = x^6 + (a+1)\,x^5 + (a+1)\,x^3 + ax^2 + (a+1)\,x + a$

Matrix construction for f $(\sigma(a) = a + 1)$

xa^ix^j		Corresponding row											
x	$\longrightarrow$	0	0	1	0	0	0	0	0	0	0	0	0
$\sigma(a)x$	$\longrightarrow$	0	0	1	1	0	0	0	0	0	0	0	0
x^2	$\longrightarrow$	0	0	0	0	1	0	0	0	0	0	0	0
$\sigma(a)x^2$	$\longrightarrow$	0	0	0	0	1	1	0	0	0	0	0	0
x^3	$\longrightarrow$	0	0	0	0	0	0	1	0	0	0	0	0
$\sigma(a)x^3$	$\longrightarrow$	0	0	0	0	0	0	1	1	0	0	0	0
x^4	$\longrightarrow$	0	0	0	0	0	0	0	0	1	0	0	0
$\sigma(a)x^4$	$\longrightarrow$	0	0	0	0	0	0	0	0	1	1	0	0
x^5	$\longrightarrow$	0	0	0	0	0	0	0	0	0	0	1	0
$\sigma(a)x^5$	$\longrightarrow$	0	0	0	0	0	0	0	0	0	0	1	1
x^6	$\longrightarrow$	1	0	0	1	0	1	1	0	0	0	1	1
$\sigma(a)x^6$	$\longrightarrow$	1	1	1	0	1	0	1	1	0	0	0	1

$$M_f = \begin{pmatrix}
 & & 1 & & & & & & & & \\
 & & 1 & 1 & & & & & & & \\
 & & & & 1 & & & & & & \\
 & & & & 1 & 1 & & & & & \\
 & & & & & & 1 & & & & \\
 & & & & & & 1 & 1 & & & \\
 & & & & & & & & 1 & & \\
 & & & & & & & & 1 & 1 & \\
 & & & & & & & & & & 1 \\
 & & & & & & & & & & 1 & 1 \\
1 & & & 1 & & 1 & 1 & & & & 1 & 1 \\
1 & 1 & 1 & & 1 & & 1 & 1 & & & & 1
\end{pmatrix}$$

$$M_g = \begin{pmatrix}
 & & 1 & & & & & & & & \\
 & & 1 & 1 & & & & & & & \\
 & & & & 1 & & & & & & \\
 & & & & 1 & 1 & & & & & \\
 & & & & & & 1 & & & & \\
 & & & & & & 1 & 1 & & & \\
 & & & & & & & & 1 & & \\
 & & & & & & & & 1 & 1 & \\
 & & & & & & & & & & 1 \\
 & 1 & 1 & 1 & & 1 & 1 & 1 & & & 1 & 1 \\
1 & & & 1 & 1 & & & 1 & & & & 1
\end{pmatrix}$$

$$R_f = \begin{pmatrix} & & & & & & & & & & & & 1 \\ 1 & & & & & & & & & & & & \\ & 1 & & & & & & & & & & & \\ & & 1 & & & & & & & & & & \\ & & & 1 & & & & & & & & & \\ & & & & 1 & & & & & & & & \\ & & & & & 1 & & & & & & & \\ & & & & & & 1 & & & & & & \\ & & & & & & & 1 & & & & & \\ & & & & & & & & 1 & & & & \\ & & & & & & & & & 1 & & 1 & \\ & & & & & & & & & & 1 & & \end{pmatrix}$$

$$R_g = \begin{pmatrix} & & & & & & & & & & & & 1 \\ 1 & & & & & & & & & & & & \\ & 1 & & & & & & & & & & & 1 \\ & & 1 & & & & & & & & & & \\ & & & 1 & & & & & & & & & 1 \\ & & & & 1 & & & & & & & & \\ & & & & & 1 & & & & & & & \\ & & & & & & 1 & & & & & & \\ & & & & & & & 1 & & & & & 1 \\ & & & & & & & & 1 & & & & \\ & & & & & & & & & 1 & & 1 & \\ & & & & & & & & & & 1 & & \end{pmatrix}.$$

Comparison

Parameters

- $\mu = [\mathbb{F} : \mathbb{F}^\sigma]$
- Matrix multiplication $\in \mathcal{O}(n^\omega)$

Theoretical efficiency

Comm. Algebra	Time[a]	Space[b]	Space (sparse)
$C = \mathbb{F}^\sigma[x^\mu]$	$\mathcal{O}(\mu^\omega n^\omega \log n \log\log n)$	$\mathcal{O}(\mu^2 n^2)$	$--$
$T = \mathbb{F}[x^\mu]$	$\mathcal{O}(\mu n^\omega \log n \log\log n)$	$\mathcal{O}(\mu n^2)$	$\mathcal{O}(\mu^2 n)$
$S = \mathbb{F}^\sigma[x]$	$\mathcal{O}(\mu^\omega n^\omega \log n \log\log n)$	$\mathcal{O}(\mu^2 n^2)$	$\mathcal{O}(\mu n)$

[a] Operations over $\mathbb{F}^\sigma$
[b] Elements in $\mathbb{F}^\sigma$

Isormorphic modules

Problem

Let $R = D[x;\sigma]$, A and B finitely generated left R-modules.
How to decide if $A \cong B$? (efficiently, if possible)

Isormorphic modules

Problem

Let $R = D[x;\sigma]$, A and B finitely generated left R-modules.
How to decide if $A \cong B$? (efficiently, if possible)

Considerations

Given a finitely generated left R-module A

- $R^m \longrightarrow A$ surjective, for some m
- hence, $A \cong R^m/L$ for some m

Problem

Decide if $R^m/L_1 \cong R^n/L_2$

Reduction to cyclic modules

Jacobson (1943)

Let $A = R^m/L$ a left R-module,

1. Find $h_1, h_2, \ldots, h_t$ generators of L
2. Construct $M \in \mathcal{M}_{t\times m}(R)$, rows are coordinates of h_i
3. Diagonalize matrix M, i.e. find Q, P regular with $PMQ = D$
   - Check if M_{00} divides (by the left) all elements in its row and column
   $$\begin{pmatrix} M_{00} & \rightarrow \\ \downarrow & M' \end{pmatrix}$$
   - If not, divide, put remainder at position $(0,0)$ and repeat
   $$\left(\begin{array}{c|c} b_1 & 0 \\ \hline 0 & M' \end{array}\right)$$
   - Repeat with matrix M'
   - Return diagonal elements of $D = \mathrm{diag}\{b_1, b_2, \ldots, b_r, 0, \ldots, 0\}$
4. Drop those b_i with zero degree
5. $A = R^{m-r} \oplus \dfrac{R}{Rb_1} \oplus \cdots \oplus \dfrac{R}{Rb_e}$ (**Rough decomposition**)

Reduction to the center

Theorem

Let A, B finitely generated R-modules with rough decomposition

$$A = R^s \oplus \frac{R}{Rb_1} \oplus \cdots \oplus \frac{R}{Rb_e} \text{ and } B = R^t \oplus \frac{R}{Rf_1} \oplus \cdots \oplus \frac{R}{Rf_d}$$

Hence, the following are equivalent

- $A \cong B$
- $s = t$ *and* $\frac{R}{Rb_1} \oplus \cdots \oplus \frac{R}{Rb_e} \cong \frac{R}{Rf_1} \oplus \cdots \oplus \frac{R}{Rf_d}$ *as C-modules*

Algorithm 8 Isomorphism of finitely generated modules

Input: $A = R^n/L_1$ and $B = R^m/L_2$ finitely generated left R–modules

Output: `True` if they are isomorphic; `False` otherwise.

1: Find rough decomposition $A = R^s \oplus \dfrac{R}{Rb_1} \oplus \cdots \oplus \dfrac{R}{Rb_e}$

2: Find rough decomposition $B = R^t \oplus \dfrac{R}{Rf_1} \oplus \cdots \oplus \dfrac{R}{Rf_d}$

3: **if** $t \neq s$ **then**

4: **return** `False`

5: Compute the matrices M_{b_i} =MatrixConstruction(b_i)

6: Compute the matrices M_{f_i} =MatrixConstruction(f_i)

7: Create block matrices

$$M_A = \left(\begin{array}{c|c|c} M_{b_1} & & 0 \\ \hline & \ddots & \\ \hline 0 & & M_{b_e} \end{array}\right) \text{ and } M_B = \left(\begin{array}{c|c|c} M_{g_1} & & 0 \\ \hline & \ddots & \\ \hline 0 & & M_{g_d} \end{array}\right)$$

8: **if** the rational canonical form of M_A and M_B are different **then**

9: **return** `False`

10: **return** `True`

Example

$\mathbb{F}_{2^8}[x;\tau^2]$, a primitive element, $\mu = 4$

- Matrix for A

$$\begin{pmatrix} 1 & 0 & 0 & x+a^3 \\ 0 & x+a^{11} & x^2+a^{116}x+a^{12} & 0 \\ 0 & 0 & x^5+a^7x^4+a^{170}x+a^{177} & 0 \\ x+a^{78} & 0 & 0 & x^2+a^{42}x+a^7+a^{81} \end{pmatrix}$$

- Matrix for B

$$\begin{pmatrix} x+a^2 & x^2+a^{247}x+a^5+a^{69} & x^2+a^{196}x+a^{225} \\ x^2+a^{206}x+a^{36} & x^5+a^{25}x^4+x^3+a^{253}x^2+a^{149}x+a^{122} & x^3+a^{52}x^2+a^{56}x+a^4 \end{pmatrix}$$

$\mathbb{F}_{2^8}[x;\tau^2]$, a primitive element, $\mu = 4$

- Diagonal matrix for A

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x + a^{11} & 0 & 0 \\ 0 & 0 & x^5 + a^7 x^4 + a^{170} x + a^{177} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

- Diagonal matrix for B

$$\begin{pmatrix} x + a^2 & 0 & 0 \\ 0 & x^5 + a^{25} x^4 + a^{170} x + a^{195} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$\mathbb{F}_{2^8}[x;\tau^2]$, a primitive element, $\mu = 4$

- Rough decomposition for A

$$A \cong R \oplus \frac{R}{R(x + a^{11})} \oplus \frac{R}{R(x^5 + a^7 x^4 + a^{170} x + a^1 77)}$$

- Rough decomposition for B

$$B \cong R \oplus \frac{R}{R(x + a^2)} \oplus \frac{R}{R(x^5 + a^{25} x^4 + a^{170} x + a^{195})}$$

$\mathbb{F}_{2^8}[x;\tau^2]$, a primitive element, $\mu = 4$

- Matrix of the diagonal polynomials for A

$$M_A = \left(\begin{array}{c|ccccc} a^{170} & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & a^{177} & a^{170} & 0 & 0 & a^{7} \\ 0 & a^{205} & 0 & a^{170} & 0 & a^{35} \\ 0 & a^{62} & 0 & 0 & a^{170} & a^{147} \\ 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

- Matrix of the diagonal polynomials for B

$$M_B = \left(\begin{array}{c|ccccc} a^{170} & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & a^{195} & a^{170} & 0 & 0 & a^{25} \\ 0 & a^{40} & 0 & a^{170} & 0 & a^{125} \\ 0 & a^{185} & 0 & 0 & a^{170} & a^{15} \\ 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

$\mathbb{F}_{2^8}[x;\tau^2]$, a primitive element, $\mu = 4$

- Rational form of M_A

$$R_A = \left(\begin{array}{c|c|c|c|cc} a^{170} & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & a^{170} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & a^{170} & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & a^{170} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right)$$

- Rational form of M_B

$$R_B = \left(\begin{array}{c|c|c|c|cc} a^{170} & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & a^{170} & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & a^{170} & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & a^{170} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right)$$