Ritt's Theorem and refinements.

Alice Medvedev, University of California, Berkeley
joint work with Thomas Scanlon

AMS Special Session on Dynamical Systems in Algebraic and Arithmetic Geometry at Joint AMS-MAAdness 2012

Decompositions and Ritt's Theorem (char 0).

Slogan: Every polynomial can be written as a composition of indecomposables, uniquely up to permutations and units.

Decompositions and Ritt's Theorem (char 0).

Slogan: Every polynomial can be written as a composition of indecomposables, uniquely up to permutations and units.

- *Unit with respect to composition*: linear.

Decompositions and Ritt's Theorem (char 0).

Slogan: Every polynomial can be written as a composition of indecomposables, uniquely up to permutations and units.

- *Unit with respect to composition*: linear.
- *Indecomposable*: f is not linear, and if $f = g \circ h$, then one of g and h is linear.

Decompositions and Ritt's Theorem (char 0).

Slogan: Every polynomial can be written as a composition of indecomposables, uniquely up to permutations and units.

- *Unit with respect to composition*: linear.
- *Indecomposable*: f is not linear, and if $f = g \circ h$, then one of g and h is linear.
- *Up to units*: $f_3 \circ f_2 \circ f_1 = (f_3 \circ L_2) \circ (L_2^{-1} \circ f_2 \circ L_1) \circ (L_1^{-1} \circ f_1)$.

Decompositions and Ritt's Theorem (char 0).

Slogan: Every polynomial can be written as a composition of indecomposables, uniquely up to permutations and units.

- *Unit with respect to composition*: linear.
- *Indecomposable*: f is not linear, and if $f = g \circ h$, then one of g and h is linear.
- *Up to units*: $f_3 \circ f_2 \circ f_1 = (f_3 \circ L_2) \circ (L_2^{-1} \circ f_2 \circ L_1) \circ (L_1^{-1} \circ f_1)$.
- Some permutations: $(x^k \cdot u(x^m)^{pn}) \circ x^p = x^p \circ (x^k \cdot u(x^{pm})^n)$;

  monomials commute; so do Chebyshevs $C_p \circ C_q = C_q \circ C_p$.

Decompositions and Ritt's Theorem (char 0).

Slogan: Every polynomial can be written as a composition of indecomposables, uniquely up to permutations and units.

- *Up to units*: $f_3 \circ f_2 \circ f_1 = (f_3 \circ L_2) \circ (L_2^{-1} \circ f_2 \circ L_1) \circ (L_1^{-1} \circ f_1)$.
- Basic Ritt Identities: $(x^k \cdot u(x^m)^{pn}) \circ x^p = x^p \circ (x^k \cdot u(x^{pm})^n)$;

  monomials commute; so do Chebyshevs $C_p \circ C_q = C_q \circ C_p$.

Decompositions and Ritt's Theorem (char 0).

Slogan: Every polynomial can be written as a composition of indecomposables, uniquely up to permutations and units.

- *Up to units*: $f_3 \circ f_2 \circ f_1 = (f_3 \circ L_2) \circ (L_2^{-1} \circ f_2 \circ L_1) \circ (L_1^{-1} \circ f_1)$.
- Basic Ritt Identities: $(x^k \cdot u(x^m)^{pn}) \circ x^p = x^p \circ (x^k \cdot u(x^{pm})^n)$;

  monomials commute; so do Chebyshevs $C_p \circ C_q = C_q \circ C_p$.
- If $(L^{-1} \circ f_{i+1} \circ M) \circ (M^{-1} \circ f_i \circ N) = h_{i+1} \circ h_i$ is

  a basic Ritt identity for some linear L, M, N, we say that

  $$(f_k, \ldots f_{i+2}, L \circ h_{i+1}, h_i \circ N^{-1}, f_{i-1} \ldots f_1)$$

  is *obtained from* $(f_k, \ldots f_1)$ *by a Ritt swap at* i.

Decompositions and Ritt's Theorem (char 0).

Slogan: Every polynomial can be written as a composition of indecomposables, uniquely up to permutations and units.

- *Up to units*: $f_3 \circ f_2 \circ f_1 = (f_3 \circ L_2) \circ (L_2^{-1} \circ f_2 \circ L_1) \circ (L_1^{-1} \circ f_1)$.
- Basic Ritt Identities: $(x^k \cdot u(x^m)^{pn}) \circ x^p = x^p \circ (x^k \cdot u(x^{pm})^n)$;

  monomials commute; so do Chebyshevs $C_p \circ C_q = C_q \circ C_p$.
- If $(L^{-1} \circ f_{i+1} \circ M) \circ (M^{-1} \circ f_i \circ N) = h_{i+1} \circ h_i$ is

  a basic Ritt identity for some linear L, M, N, we say that

$$(f_k, \ldots f_{i+2}, L \circ h_{i+1}, h_i \circ N^{-1}, f_{i-1} \ldots f_1)$$

  is *obtained from* $(f_k, \ldots f_1)$ *by a Ritt swap at* i.

Theorem: (Ritt) Given one decomposition of a polynomial, any other can be obtained from it by a sequence of Ritt swaps; up to units.

Examples

Theorem: (Ritt) Given one decomposition of a polynomial, any other can be obtained from it by a sequence of Ritt swaps; up to units.

- $(x^3 - 3x, x^2 - 2, x \cdot (x^2 + 1))$:
  the Ritt swap at 1 needs the middle factor to be x^2, but
  the Ritt swap at 2 (commuting Chebyshevs) needs $x^2 - 2$.

- $(x^5, x \cdot (x^5 + 1))$ is obtained from $(x \cdot (x + 1)^5, x^5)$ by a Ritt Swap ($L = M = N = \mathrm{id}$); but $((32)^6 x^5, \frac{x}{2} \cdot \frac{x^5+1}{32})$ is, too!
  ($L(x) = (32)^6 x$, $M(x) = 32x$, and $N(x) = 2x$).

Lemma: Two decompositions obtained from $(f_k, \ldots f_1)$ by Ritt swaps at the same i are the same up to units.

S_k acts on the set of decompositions?

- Transpositions $(i\ i+1)$ for $i < k$ generate S_k.

S_k acts on the set of decompositions?

- Transpositions $(i\ i+1)$ for $i < k$ generate S_k.
- Let $(i\ i+1)$ act on $(f_k, \ldots f_1)$ by a Ritt swap at i.

S_k acts on the set of decompositions?

- Transpositions $(i\ i+1)$ for $i < k$ generate S_k.
- Let $(i\ i+1)$ act on $(f_k, \ldots f_1)$ by a Ritt swap at i.
- Sometimes (usually) undefined! At best, only up to units.

S_k acts on the set of decompositions?

- Transpositions $(i\ i+1)$ for $i < k$ generate S_k.
- Let $(i\ i+1)$ act on $(f_k, \ldots f_1)$ by a Ritt swap at i.
- Sometimes (usually) undefined! At best, only up to units.
- Relations satisfied by these transpositions in S_k are generated by:

$$(i\ i+1)^2 = \mathrm{id}$$

$$(i\ i+1)(j\ j+1) = (j\ j+1)(i\ i+1) \text{ for } j \neq i \pm 1$$

$$(i\ i+1)(i+1\ i+2)(i\ i+1) = (i+1\ i+2)(i\ i+1)(i+1\ i+2)$$

S_k acts on the set of decompositions?

- Transpositions $(i\ i+1)$ for $i < k$ generate S_k.
- Let $(i\ i+1)$ act on $(f_k, \ldots f_1)$ by a Ritt swap at i.
- Sometimes (usually) undefined! At best, only up to units.
- Relations satisfied by these transpositions in S_k are generated by:

$$(i\ i+1)^2 = \mathrm{id}$$

$$(i\ i+1)(j\ j+1) = (j\ j+1)(i\ i+1) \text{ for } j \neq i \pm 1$$

$$(i\ i+1)(i+1\ i+2)(i\ i+1) = (i+1\ i+2)(i\ i+1)(i+1\ i+2)$$

Lemma: The action satisfies these, except $(i\ i+1)^2$ might not be defined while id always is.

Sorting algorithms and bounds.

How many different decompositions might a polynomial have?
How many Ritt swaps are necessary to get from one to another?

Sorting algorithms and bounds.

How many different decompositions might a polynomial have?
How many Ritt swaps are necessary to get from one to another?

- If $(g_k, \ldots, g_1)$ and $(f_k, \ldots f_1)$ are decompositions of the same polynomial, some sequence S of Ritt swaps turns $\vec{f}$ into $\vec{g}$.

Sorting algorithms and bounds.

How many different decompositions might a polynomial have?
How many Ritt swaps are necessary to get from one to another?

- If $(g_k, \ldots, g_1)$ and $(f_k, \ldots f_1)$ are decompositions of the same polynomial, some sequence S of Ritt swaps turns $\vec{f}$ into $\vec{g}$.
- This sequence S corresponds to a permutation P in S_k.

Sorting algorithms and bounds.

How many different decompositions might a polynomial have?
How many Ritt swaps are necessary to get from one to another?

- If $(g_k, \ldots, g_1)$ and $(f_k, \ldots f_1)$ are decompositions of the same polynomial, some sequence S of Ritt swaps turns $\vec{f}$ into $\vec{g}$.
- This sequence S corresponds to a permutation P in S_k.
- A sorting algorithm (insert-sort, merge-sort) assigns a canonical sequence S' of adjacent transpositions to that permutation.

Sorting algorithms and bounds.

How many different decompositions might a polynomial have?
How many Ritt swaps are necessary to get from one to another?

- If $(g_k, \ldots, g_1)$ and $(f_k, \ldots f_1)$ are decompositions of the same polynomial, some sequence S of Ritt swaps turns $\vec{f}$ into $\vec{g}$.
- This sequence S corresponds to a permutation P in S_k.
- A sorting algorithm (insert-sort, merge-sort) assigns a canonical sequence S' of adjacent transpositions to that permutation.

Theorem The sequence of Ritt swaps corresponding to S' also turns $\vec{f}$ into $\vec{g}$.

Sorting algorithms and bounds.

How many different decompositions might a polynomial have?
How many Ritt swaps are necessary to get from one to another?

- If $(g_k, \ldots, g_1)$ and $(f_k, \ldots f_1)$ are decompositions of the same polynomial, some sequence S of Ritt swaps turns $\vec{f}$ into $\vec{g}$.
- This sequence S corresponds to a permutation P in S_k.
- A sorting algorithm (insert-sort, merge-sort) assigns a canonical sequence S' of adjacent transpositions to that permutation.

Theorem The sequence of Ritt swaps corresponding to S' also turns $\vec{f}$ into $\vec{g}$.

Corollary: A polynomial has at most $k!$ distinct decompositions; up to units.

Sorting algorithms and bounds.

How many different decompositions might a polynomial have?
How many Ritt swaps are necessary to get from one to another?

- If $(g_k, \ldots, g_1)$ and $(f_k, \ldots f_1)$ are decompositions of the same polynomial, some sequence S of Ritt swaps turns $\vec{f}$ into $\vec{g}$.
- This sequence S corresponds to a permutation P in S_k.
- A sorting algorithm (insert-sort, merge-sort) assigns a canonical sequence S' of adjacent transpositions to that permutation.

Theorem The sequence of Ritt swaps corresponding to S' also turns $\vec{f}$ into $\vec{g}$.

Corollary: A polynomial has at most $k!$ distinct decompositions; up to units.

Corollary: It takes at most $\approx \frac{k^2}{2}$ Ritt swaps to get from one decomposition to another.

Behind the scenes: clusters.

For linear A and B, polynomials f and $A \circ F \circ B$ are *linearly related*.

- Every polynomial almost uniquely decomposes into *clusters*, each of which is linearly related to an unswappable indecomposable; to a Chebyshev polynomial; or to a third thing.

Behind the scenes: clusters.

For linear A and B, polynomials f and $A \circ F \circ B$ are *linearly related*.

- Every polynomial almost uniquely decomposes into *clusters*, each of which is linearly related to an unswappable indecomposable; to a Chebyshev polynomial; or to a third thing. Not up to permutations, really uniquely!

Behind the scenes: clusters.

For linear A and B, polynomials f and $A \circ F \circ B$ are *linearly related*.

- Every polynomial almost uniquely decomposes into *clusters*, each of which is linearly related to an unswappable indecomposable; to a Chebyshev polynomial; or to a third thing. Not up to permutations, really uniquely!
- Ritt swaps within clusters are witnessed by identity linear factors.

Behind the scenes: clusters.

For linear A and B, polynomials f and $A \circ F \circ B$ are *linearly related*.

- Every polynomial almost uniquely decomposes into *clusters*, each of which is linearly related to an unswappable indecomposable; to a Chebyshev polynomial; or to a third thing. Not up to permutations, really uniquely!
- Ritt swaps within clusters are witnessed by identity linear factors.
- Ritt swaps between clusters are almost impossible.

Behind the scenes: clusters.

For linear A and B, polynomials f and $A \circ F \circ B$ are *linearly related*.

- Every polynomial almost uniquely decomposes into *clusters*, each of which is linearly related to an unswappable indecomposable; to a Chebyshev polynomial; or to a third thing. Not up to permutations, really uniquely!
- Ritt swaps within clusters are witnessed by identity linear factors.
- Ritt swaps between clusters are almost impossible.
- Factors of degree two can move between clusters, but even this can be controlled.

Behind the scenes: clusters.

For linear A and B, polynomials f and $A \circ F \circ B$ are *linearly related*.

- Every polynomial almost uniquely decomposes into *clusters*, each of which is linearly related to an unswappable indecomposable; to a Chebyshev polynomial; or to $h_m \circ \ldots \circ h_1$ where each h_i is of the form $(x^k \cdot u(x^m)^n)$. Not up to permutations, really uniquely!
- Ritt swaps within clusters are witnessed by identity linear factors.
- Ritt swaps between clusters are almost impossible.
- Factors of degree two can move between clusters, but even this can be controlled.