Ritt's Theorem and refinements.

Alice Medvedev, the City College of New York
joint work with Thomas Scanlon

DART IX
Leeds, UK
August 31, 2018

Ritt's Theorem.

If f_i and g_i are indecomposable polynomials over $\mathbb{C}$ and

$$f_k \circ \ldots \circ f_2 \circ f_1 = g_\ell \circ \ldots \circ g_2 \circ g_1,$$

then $k = \ell$ and the sequence $\vec{g}$ can be obtained from $\vec{f}$ by a finite sequence of *Ritt Swaps*.

Each Ritt swap changes two adjacent factors in one of three ways:

$(x^p, x^q) \rightsquigarrow (x^q, x^p)$ monomials commute;
$(C_p, C_q) \rightsquigarrow (C_q, C_p)$ so do Chebyshev polynomials;
$\big((x^k \cdot u(x)^p), x^p\big) \leftrightsquigarrow \big(x^p, (x^k \cdot u(x^p))\big)$ both give $x^{kp} \cdot u(x^p)^p$;

inserting linear factors as necessary, such as

$$(L \circ x^p \circ M^{-1}, M \circ x^q \circ N) \rightsquigarrow (L \circ x^q, x^p \circ N).$$

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

Ritt's Theorem Example

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

The polynomial $P(x) := x^{14}(x^{98}+1)^2$ has decompositions

$$A := (x(x^7+1)^2, x^7, x^2) \text{ and } B := (x^2, x(x^{14}+1), x^7).$$

B comes from A via two Ritt swaps:

the permutation (12) turns (x^7, x^2) into (x^2, x^7);
then (23) turns $(x(x^7+1)^2, x^2)$ into $(x^2, x(x^{14}+1))$.

So, the permutation $(321) = (23)(12)$ turns A into B.

But $(321) = (12)(23)(12)(23)$ also, but (23) cannot act on A:

$$\left(x(x^7+1)^2\right) \circ x^7 \neq x^7 \circ \text{anything}.$$

Symmetric group not-quite action

Sym_k: generators $t_i := (i\ i+1)$ for $i < k$; and relations $t_i t_i = \mathrm{id}$ and $t_i t_j = t_j t_i$ for $j \neq i \pm 1$ and $t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1}$.

Lemma: The action by Ritt Swaps on decompositions satisfies these, up to linear factors, except the action $(i\ i+1)^2$ might not be defined while id always is.

Fact: For any permutation $\sigma \in \mathrm{Sym}_k$, there is a unique sequence w_σ of t_i that gives σ and encodes an *insert-sort* of the k objects.

Proposition: Suppose that the action $w \star \vec{f}$ of a sequence w of Ritt swaps on a decomposition $\vec{f}$ is defined. Let σ be the permutation corresponding to w. Then $w_\sigma \star \vec{f}$ is defined and equal to $w \star \vec{f}$, up to linear factors.

Symmetric group not-quite action

Sym_k: generators $t_i := (i\ i+1)$ for $i < k$; and relations $t_i t_i = \mathrm{id}$ and $t_i t_j = t_j t_i$ for $j \neq i \pm 1$ and $t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1}$.

Lemma: The action by Ritt Swaps on decompositions satisfies these, up to linear factors, except the action $(i\ i+1)^2$ might not be defined while id always is.

Fact: For any permutation $\sigma \in \mathrm{Sym}_k$, there is a unique sequence w_σ of t_i that gives σ and encodes an *insert-sort* of the k objects.

Proposition: Suppose that the action $w \star \vec{f}$ of a sequence w of Ritt swaps on a decomposition $\vec{f}$ is defined. Let σ be the permutation corresponding to w. Then $w_\sigma \star \vec{f}$ is defined and equal to $w \star \vec{f}$, up to linear factors.

THE HARD PART

Clusters

Theorem. For every polynomial P there is a least r such that $P = L_r \circ P_r \circ \ldots \circ P_2 \circ L_1 \circ P_1 \circ L_0$, where each P_j is a *cluster* and each L_j is linear. The sequence of P_j and L_j is almost unique.

A *cluster* is a (possibly decomposable) Chebyshev polynomial; or one of the form $x^k \cdot u(x^m)^n$ for some $k \geq 1$ and $nm \geq 2$; or an indecomposable polynomial that is not of those forms, even up to linear factors.

Theorem. Ritt swaps within clusters need no auxillary linear factors.

Theorem. Ritt swaps between clusters always involve a quadratic, and change the linear factor so that no more quadratics can pass between the same clusters in the same direction.