Functional Decomposition using Principal Subfields

L. Allem, J. Capaverde, M. van Hoeij and Jonas Szutkoski

ISSAC'17, Kaiserslautern

The problem

Let $f \in K(t)$. We want to find **complete decompositions** of f. That is, we want to find indecomposable rational functions $g_1, \ldots, g_m$ such that

$$f = g_1 \circ \cdots \circ g_m.$$

The problem

Let $f \in K(t)$. We want to find **complete decompositions** of f. That is, we want to find indecomposable rational functions $g_1, \ldots, g_m$ such that

$$f = g_1 \circ \cdots \circ g_m.$$

Consider the extension $K(t)/K(f(t))$ and let L be a subfield of this extension. By Lüroth's Theorem, there exists a rational function $h(t)$ such that $L = K(h(t))$ and hence, $f = g \circ h$, for some $g \in K(t)$. The converse also holds.

The problem

Let $f \in K(t)$. We want to find **complete decompositions** of f. That is, we want to find indecomposable rational functions $g_1, \ldots, g_m$ such that

$$f = g_1 \circ \cdots \circ g_m.$$

Consider the extension $K(t)/K(f(t))$ and let L be a subfield of this extension. By Lüroth's Theorem, there exists a rational function $h(t)$ such that $L = K(h(t))$ and hence, $f = g \circ h$, for some $g \in K(t)$. The converse also holds. Thus

decompositions of $f \longleftrightarrow$ **subfields** of $K(t)/K(f(t))$.

complete decomp. of $f \longleftrightarrow$ **max. chains** of subfields.

Principal Subfields

Let $K(t)/K(f(t))$. Then t is a primitive element with minpoly

$$\Phi_f := f_n(x) - f(t)f_d(x) \in K(f(t))[x].$$

Let $F_1, \ldots, F_r$ be the irreducible factors of Φ_f over $K(t)$.

Principal Subfields

Let $K(t)/K(f(t))$. Then t is a primitive element with minpoly

$$\Phi_f := f_n(x) - f(t)f_d(x) \in K(f(t))[x].$$

Let $F_1, \ldots, F_r$ be the irreducible factors of Φ_f over $K(t)$.

Definition: For each factor F_i, let $L_i := \{g(t) \in K(t) : F_i \mid \Phi_g\}$.

We may assume $F_1 = x - t$. Hence, $L_1 = K(t)$. The subfields $L_1, \ldots, L_r$ are called **principal subfields**.

Principal Subfields

Let $K(t)/K(f(t))$. Then t is a primitive element with minpoly

$$\Phi_f := f_n(x) - f(t)f_d(x) \in K(f(t))[x].$$

Let $F_1, \ldots, F_r$ be the irreducible factors of Φ_f over $K(t)$.

Definition: For each factor F_i, let $L_i := \{g(t) \in K(t) : F_i \mid \Phi_g\}$.

We may assume $F_1 = x - t$. Hence, $L_1 = K(t)$. The subfields $L_1, \ldots, L_r$ are called **principal subfields**.

Theorem [van Hoeij et al., 2013]

For every subfield L of $K(t)/K(f(t))$, there exists a subset $I \subseteq \{1, \ldots, r\}$ such that $L = \bigcap_{i \in I} L_i$.

Principal Subfields

Finding all subfields of $K(t)/K(f(t))$:

1. Factor $\Phi_f \in K(f(t))[x]$ over $K(t)$.

Finding all subfields of $K(t)/K(f(t))$:

1. Factor $\Phi_f \in K(f(t))[x]$ over $K(t)$.
2. For each irreducible factor F_i, define the principal subfield L_i.

Principal Subfields

Finding all subfields of $K(t)/K(f(t))$:

1. Factor $\Phi_f \in K(f(t))[x]$ over $K(t)$.
2. For each irreducible factor F_i, define the principal subfield L_i.
3. Compute the intersection of all subsets of $\{L_1, \ldots, L_r\}$.

Principal Subfields

Finding all subfields of $K(t)/K(f(t))$:

1. Factor $\Phi_f \in K(f(t))[x]$ over $K(t)$.
2. For each irreducible factor F_i, define the principal subfield L_i.
3. Compute the intersection of all subsets of $\{L_1, \ldots, L_r\}$.

Number of intersections: $\leq r \cdot m$ (m is the number of subfields).

Finding all subfields of $K(t)/K(f(t))$:

1. Factor $\Phi_f \in K(f(t))[x]$ over $K(t)$.
2. For each irreducible factor F_i, define the principal subfield L_i.
3. Compute the intersection of all subsets of $\{L_1, \ldots, L_r\}$.

Number of intersections: $\leq r \cdot m$ (m is the number of subfields).

$\rightsquigarrow$ To reduce the cost of each intersection, we use partitions. For each L, we associate a unique partition P_L of $\{1, \ldots, r\}$.

Finding all subfields of $K(t)/K(f(t))$:

1. Factor $\Phi_f \in K(f(t))[x]$ over $K(t)$.
2. For each irreducible factor F_i, define the principal subfield L_i.
3. Compute the intersection of all subsets of $\{L_1, \ldots, L_r\}$.

Number of intersections: $\leq r \cdot m$ (m is the number of subfields).

$\rightsquigarrow$ To reduce the cost of each intersection, we use partitions. For each L, we associate a unique partition P_L of $\{1, \ldots, r\}$.

$$\begin{array}{ccc}
K(t) & \Phi_f = F_1 \cdot F_2 \cdot F_3 \cdot F_4 \cdot F_5 & \longrightarrow \{\{1\},\{2\},\{3\},\{4\},\{5\}\} \\
\downarrow & \downarrow & \\
L & \Phi_f = (F_1 F_2 F_3) \cdot (F_4 F_5) & \longrightarrow P_L = \{\{1,2,3\},\{4,5\}\} \\
\downarrow & \downarrow & \\
K(f(t)) & \Phi_f = (F_1 F_2 F_3 F_4 F_5) & \longrightarrow \{\{1,2,3,4,5\}\}
\end{array}$$

Reducing the cost of each intersection

Theorem [Szutkoski & van Hoeij, 2016]

Let L and L' be subfields with partitions P_L and $P_{L'}$, resp. Then

$$P_{L \cap L'} = P_L \vee P_{L'}.$$

Reducing the cost of each intersection

Theorem [Szutkoski & van Hoeij, 2016]

Let L and L' be subfields with partitions P_L and $P_{L'}$, resp. Then

$$P_{L\cap L'} = P_L \vee P_{L'}.$$

L_i, L_j

Reducing the cost of each intersection

Theorem [Szutkoski & van Hoeij, 2016]

Let L and L' be subfields with partitions P_L and $P_{L'}$, resp. Then

$$P_{L \cap L'} = P_L \vee P_{L'}.$$

$$L_i, L_j$$

$$\downarrow$$

$$L_i \cap L_j$$

Reducing the cost of each intersection

Theorem [Szutkoski & van Hoeij, 2016]

Let L and L' be subfields with partitions P_L and $P_{L'}$, resp. Then

$$P_{L \cap L'} = P_L \vee P_{L'}.$$

$$L_i, L_j \xrightarrow{(1)} P_{L_i}, P_{L_j}$$

Reducing the cost of each intersection

Theorem [Szutkoski & van Hoeij, 2016]

Let L and L' be subfields with partitions P_L and $P_{L'}$, resp. Then

$$P_{L \cap L'} = P_L \vee P_{L'}.$$

$$\begin{array}{ccc} L_i, L_j & \xrightarrow{(1)} & P_{L_i}, P_{L_j} \\ & & \downarrow \\ & & P_{L_i} \vee P_{L_j} \end{array}$$

Reducing the cost of each intersection

Theorem [Szutkoski & van Hoeij, 2016]

Let L and L' be subfields with partitions P_L and $P_{L'}$, resp. Then

$$P_{L \cap L'} = P_L \vee P_{L'}.$$

$$\begin{array}{ccc} L_i, L_j & \xrightarrow{(1)} & P_{L_i}, P_{L_j} \\ & & \downarrow \\ L_i \cap L_j & \xleftarrow[(2)]{} & P_{L_i} \vee P_{L_j} \end{array}$$

Reducing the cost of each intersection

Theorem [Szutkoski & van Hoeij, 2016]

Let L and L' be subfields with partitions P_L and $P_{L'}$, resp. Then

$$P_{L \cap L'} = P_L \vee P_{L'}.$$

$$\begin{array}{ccc} L_i, L_j & \xrightarrow{(1)} & P_{L_i}, P_{L_j} \\ & & \downarrow \\ L_i \cap L_j & \xleftarrow[(2)]{} & P_{L_i} \vee P_{L_j} \end{array}$$

- $\rightsquigarrow$ $P \vee Q =$ the finest partition refined by both P and Q.
- $\rightsquigarrow$ $\mathcal{O}(r \log r)$ CPU operations [Freese, 1997].

(1): How to find the partitions

Let $F_1(x,t), \ldots, F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1, \ldots, e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^{r} F_j^{e_j} \in L_i[x]$.

(1): How to find the partitions

Let $F_1(x,t),\ldots,F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1,\ldots,e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^{r} F_j^{e_j} \in L_i[x]$.

$\Phi_f = (F_1 F_2 F_3) \cdot (F_4 F_5) \leftrightarrow (1,1,1,0,0),(0,0,0,1,1) \leftrightarrow P_L$

(1): How to find the partitions

Let $F_1(x,t),\ldots,F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1,\ldots,e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^r F_j^{e_j} \in L_i[x]$.

$\Phi_f = (F_1 F_2 F_3) \cdot (F_4 F_5) \leftrightarrow (1,1,1,0,0),(0,0,0,1,1) \leftrightarrow P_L$

- Use Logarithmic derivative: if $g = \prod F_j^{e_j}$, then $\frac{g'}{g} = \sum e_j \frac{F_j'}{F_j}$.

(1): How to find the partitions

Let $F_1(x,t), \dots, F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1, \dots, e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^{r} F_j^{e_j} \in L_i[x]$.

$\Phi_f = (F_1 F_2 F_3) \cdot (F_4 F_5) \leftrightarrow (1,1,1,0,0), (0,0,0,1,1) \leftrightarrow P_L$

- Use Logarithmic derivative: if $g = \prod F_j^{e_j}$, then $\frac{g'}{g} = \sum e_j \frac{F_j'}{F_j}$.

Theorem

If $g'(c)/g(c) \in L_i$, for $2n$ points $c \in K(f(t))$, then $g \in L_i[x]$.

(1): How to find the partitions

Let $F_1(x,t),\ldots,F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1,\ldots,e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^{r} F_j^{e_j} \in L_i[x]$.

$\Phi_f = (F_1 F_2 F_3) \cdot (F_4 F_5) \leftrightarrow (1,1,1,0,0),(0,0,0,1,1) \leftrightarrow P_L$

- Use Logarithmic derivative: if $g = \prod F_j^{e_j}$, then $\frac{g'}{g} = \sum e_j \frac{F_j'}{F_j}$.

Theorem

If $g'(c)/g(c) \in L_i$, for $2n$ points $c \in K(f(t))$, then $g \in L_i[x]$.

- $g'(c)/g(c) =: e(t) \in L_i$

(1): How to find the partitions

Let $F_1(x,t),\ldots,F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1,\ldots,e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^r F_j^{e_j} \in L_i[x]$.

$\Phi_f = (F_1F_2F_3)\cdot(F_4F_5) \leftrightarrow (1,1,1,0,0),(0,0,0,1,1) \leftrightarrow P_L$

- Use Logarithmic derivative: if $g = \prod F_j^{e_j}$, then $\frac{g'}{g} = \sum e_j \frac{F_j'}{F_j}$.

Theorem

If $g'(c)/g(c) \in L_i$, for $2n$ points $c \in K(f(t))$, then $g \in L_i[x]$.

- $g'(c)/g(c) =: e(t) \in L_i \Leftrightarrow F_i \mid e_n(x) - e(t)e_d(x)$

Let $F_1(x,t),\ldots,F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1,\ldots,e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^{r} F_j^{e_j} \in L_i[x]$.

$$\Phi_f = (F_1F_2F_3)\cdot(F_4F_5) \leftrightarrow (1,1,1,0,0),(0,0,0,1,1) \leftrightarrow P_L$$

- Use Logarithmic derivative: if $g = \prod F_j^{e_j}$, then $\frac{g'}{g} = \sum e_j \frac{F_j'}{F_j}$.

Theorem

If $g'(c)/g(c) \in L_i$, for $2n$ points $c \in K(f(t))$, then $g \in L_i[x]$.

- $g'(c)/g(c) =: e(t) \in L_i \Leftrightarrow F_i \mid e_n(x) - e(t)e_d(x) \to \mathcal{S}_{i,c}$.

(1): How to find the partitions

Let $F_1(x,t), \ldots, F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1, \ldots, e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^r F_j^{e_j} \in L_i[x]$.

$\Phi_f = (F_1 F_2 F_3) \cdot (F_4 F_5) \leftrightarrow (1,1,1,0,0), (0,0,0,1,1) \leftrightarrow P_L$

- Use Logarithmic derivative: if $g = \prod F_j^{e_j}$, then $\frac{g'}{g} = \sum e_j \frac{F_j'}{F_j}$.

Theorem

If $g'(c)/g(c) \in L_i$, for $2n$ points $c \in K(f(t))$, then $g \in L_i[x]$.

- $g'(c)/g(c) =: e(t) \in L_i \Leftrightarrow F_i \mid e_n(x) - e(t)e_d(x) \to \mathcal{S}_{i,c}$.
- Solving $\mathcal{S}_i := \cup \mathcal{S}_{i,c}$, for $2n$ points c, gives the partition P_i.

(1): How to find the partitions

Let $F_1(x,t),\ldots,F_r(x,t)$ the irreducible factors of Φ_f over $K(t)$.

- $P_i \Leftrightarrow (e_1,\ldots,e_r) \in \{0,1\}^r$ such that $\prod_{j=1}^r F_j^{e_j} \in L_i[x]$.

$\Phi_f = (F_1 F_2 F_3) \cdot (F_4 F_5) \leftrightarrow (1,1,1,0,0),(0,0,0,1,1) \leftrightarrow P_L$

- Use Logarithmic derivative: if $g = \prod F_j^{e_j}$, then $\frac{g'}{g} = \sum e_j \frac{F_j'}{F_j}$.

Theorem

If $g'(c)/g(c) \in L_i$, for $2n$ points $c \in K(f(t))$, then $g \in L_i[x]$.

- $g'(c)/g(c) =: e(t) \in L_i \Leftrightarrow F_i \mid e_n(x) - e(t)e_d(x) \to \mathcal{S}_{i,c}$.
- Solving $\mathcal{S}_i := \cup \mathcal{S}_{i,c}$, for $2n$ points c, gives the partition P_i.

Takes too long. Find probabilistic version.

(1): How to find the partitions

Idea 1: Start with only 1 evaluation point (use more if needed).
Idea 2: Compute the remainder modulo prime ideals. Let $O \subset K(t)$ be a ring with max. ideal P. Then O is a **good** ring if:

- $F_i(x, t) \in O[x]$.
- The image of $f(t)$ in O/P is not zero.
- The image of Φ_f in $(O/P)[x]$ is separable.

If P is not the place at infinity, then $O/P \cong K[x]/\langle q(x) \rangle \cong K[\alpha]$.

(1): How to find the partitions

Idea 1: Start with only 1 evaluation point (use more if needed).
Idea 2: Compute the remainder modulo prime ideals. Let $O \subset K(t)$ be a ring with max. ideal P. Then O is a **good** ring if:

- $F_i(x, t) \in O[x]$.
- The image of $f(t)$ in O/P is not zero.
- The image of Φ_f in $(O/P)[x]$ is separable.

If P is not the place at infinity, then $O/P \cong K[x]/\langle q(x) \rangle \cong K[\alpha]$.

$$F_i(x, t) \mid e_n(x) - e(t)e_d(x) \rightarrow \mathcal{S}_{i,c} \qquad\qquad K(t)[x]$$

(1): How to find the partitions

Idea 1: Start with only 1 evaluation point (use more if needed).
Idea 2: Compute the remainder modulo prime ideals. Let $O \subset K(t)$ be a ring with max. ideal P. Then O is a **good** ring if:

- $F_i(x,t) \in O[x]$.
- The image of $f(t)$ in O/P is not zero.
- The image of Φ_f in $(O/P)[x]$ is separable.

If P is not the place at infinity, then $O/P \cong K[x]/\langle q(x)\rangle \cong K[\alpha]$.

$$\begin{array}{ccc} F_i(x,t) \mid e_n(x) - e(t)e_d(x) \to \mathcal{S}_{i,c} & \quad & K(t)[x] \\ \downarrow & & \downarrow \\ F_i(x,\alpha) \mid e_n(x) - e(\alpha)e_d(x) \to \tilde{\mathcal{S}}_{i,c} & & K[\alpha][x] \end{array}$$

(1): How to find the partitions

Idea 1: Start with only 1 evaluation point (use more if needed).
Idea 2: Compute the remainder modulo prime ideals. Let $O \subset K(t)$ be a ring with max. ideal P. Then O is a **good** ring if:

- $F_i(x,t) \in O[x]$.
- The image of $f(t)$ in O/P is not zero.
- The image of Φ_f in $(O/P)[x]$ is separable.

If P is not the place at infinity, then $O/P \cong K[x]/\langle q(x)\rangle \cong K[\alpha]$.

$$
\begin{array}{ccc}
F_i(x,t) \mid e_n(x) - e(t)e_d(x) \to \mathcal{S}_{i,c} & & K(t)[x] \\
\downarrow & & \downarrow \\
F_i(x,\alpha) \mid e_n(x) - e(\alpha)e_d(x) \to \tilde{\mathcal{S}}_{i,c} & & K[\alpha][x] \\
\downarrow \text{char K} = 0 & & \downarrow \\
(F_i(x,\alpha) \mid e_n(x) - e(\alpha)e_d(x)) \bmod p \to \tilde{\mathcal{S}}_{i,c} & & \mathbb{F}_p[\alpha][x]
\end{array}
$$

(1): How to find the partitions

Idea 1: Start with only 1 evaluation point (use more if needed).
Idea 2: Compute the remainder modulo prime ideals. Let $O \subset K(t)$ be a ring with max. ideal P. Then O is a **good** ring if:

- $F_i(x,t) \in O[x]$.
- The image of $f(t)$ in O/P is not zero.
- The image of Φ_f in $(O/P)[x]$ is separable.

If P is not the place at infinity, then $O/P \cong K[x]/\langle q(x)\rangle \cong K[\alpha]$.

$$\begin{array}{ccc}
F_i(x,t) \mid e_n(x) - e(t)e_d(x) \to \mathcal{S}_{i,c} & & K(t)[x] \\
\downarrow & & \downarrow \\
F_i(x,\alpha) \mid e_n(x) - e(\alpha)e_d(x) \to \tilde{\mathcal{S}}_{i,c} & & K[\alpha][x] \\
\downarrow \text{char K} = 0 & & \downarrow \\
(F_i(x,\alpha) \mid e_n(x) - e(\alpha)e_d(x)) \bmod p \to \tilde{\mathcal{S}}_{i,c} & & \mathbb{F}_p[\alpha][x]
\end{array}$$

Obs. It suffices to take $q(x)$ irreducible with $\deg(q) \in \mathcal{O}(\log n)$.

(1): How to find the partitions

However, every solution of $\mathcal{S}_i$ is also a solution of $\tilde{\mathcal{S}}_{i,c}$, but the converse is not always true.

(1): How to find the partitions

However, every solution of $\mathcal{S}_i$ is also a solution of $\tilde{\mathcal{S}}_{i,c}$, but the converse is not always true.

- **!** Basis of solutions of $\tilde{\mathcal{S}}_{i,c}$ might not correspond to a partition.
  - $\rightsquigarrow$ Choose distinct c' and solve $\tilde{\mathcal{S}}_{i,c} \cup \tilde{\mathcal{S}}_{i,c'}$ and so on.
- **!** $\tilde{P}_i$ might be a proper refinement of P_i ($|P_i| \leq |\tilde{P}_i|$).
  - $\rightsquigarrow$ We need a check that verifies whether $\tilde{P}_i = P_i$.

(1): How to find the partitions

However, every solution of $\mathcal{S}_i$ is also a solution of $\tilde{\mathcal{S}}_{i,c}$, but the converse is not always true.

- ! Basis of solutions of $\tilde{\mathcal{S}}_{i,c}$ might not correspond to a partition.
  - $\rightsquigarrow$ Choose distinct c' and solve $\tilde{\mathcal{S}}_{i,c} \cup \tilde{\mathcal{S}}_{i,c'}$ and so on.
- ! $\tilde{P}_i$ might be a proper refinement of P_i ($|P_i| \leq |\tilde{P}_i|$).
  - $\rightsquigarrow$ We need a check that verifies whether $\tilde{P}_i = P_i$.

Theorem

Let $\tilde{P}_i = \{P^{(1)}, \ldots, P^{(s)}\}$ and $G_j := \prod_{l \in P^{(j)}} F_l(x,t)$. If $G_j \in L_i[x]$, for $j = 1, \ldots, s$, then $\tilde{P}_i = P_i$.

This can also be verified modulo prime ideals.

(1): Alternatively...

Use a method from Landau & Miller (1985) to compute P_i.

- Involves gcd /resultant computations over extension of $K(t)$.
  - ⇝ We can simplify computations by reducing mod prime ideals.
  - ⇝ This yields a partition $\hat{P}_i$ such that P_i refines $\hat{P}_i$ ($|P_i| \geq |\hat{P}_i|$).

Need different check to show that $\hat{P}_i = P_i$ or...

(1): Alternatively...

Use a method from Landau & Miller (1985) to compute P_i.

- Involves gcd /resultant computations over extension of $K(t)$.
  - $\rightsquigarrow$ We can simplify computations by reducing mod prime ideals.
  - $\rightsquigarrow$ This yields a partition $\hat{P}_i$ such that P_i refines $\hat{P}_i$ ($|P_i| \geq |\hat{P}_i|$).

Need different check to show that $\hat{P}_i = P_i$ or... use both methods (without any check). This gives partitions

$$\tilde{P}_i \text{ refines } P_i \text{ refines } \hat{P}_i.$$

In particular, $|\hat{P}_i| \leq |P_i| \leq |\tilde{P}_i|$. Hence, if $|\tilde{P}_i| = |\hat{P}_i|$, then we have $\tilde{P}_i = P_i = \hat{P}_i$ (i.e., a provable result).

(2): Back to Subfields

- After we compute the partitions $P_1, \ldots, P_r$, we can compute the partitions of all subfields by computing the join of all combinations of these partitions (number of joins $\leq rm$).
- Given a partition P_L of $\{1, \ldots, r\}$, we want to find the subfield L it represents.

(2): Back to Subfields

- After we compute the partitions $P_1, \dots, P_r$, we can compute the partitions of all subfields by computing the join of all combinations of these partitions (number of joins $\leq rm$).
- Given a partition P_L of $\{1, \dots, r\}$, we want to find the subfield L it represents.

Theorem

Let $P_L^{(1)}$ be the part of P_L that contains 1. Then any non-constant coefficient $h(t)$ of $\prod_{j \in P_L^{(1)}} F_j$ is such that $L = K(h(t))$.

(2): Back to Subfields

- After we compute the partitions $P_1, \ldots, P_r$, we can compute the partitions of all subfields by computing the join of all combinations of these partitions (number of joins $\leq rm$).
- Given a partition P_L of $\{1, \ldots, r\}$, we want to find the subfield L it represents.

Theorem

Let $P_L^{(1)}$ be the part of P_L that contains 1. Then any non-constant coefficient $h(t)$ of $\prod_{j \in P_L^{(1)}} F_j$ is such that $L = K(h(t))$.

Finally, given $f, h \in K(t)$, find $g \in K(t)$ such that $f = g \circ h$.

The polynomial case

Theorem [Blankertz, 2014]

All **minimal decompositions** of $f \in \mathbb{F}_q[t]$ can be found in $\tilde{O}(n^6)$.

- $\rightsquigarrow$ $g \circ h$ is a minimal dec. $\Leftrightarrow$ $K(h(t))$ is a maximal subfield.
- $\rightsquigarrow$ $K(h(t))$ must be a principal subfield.
- $\rightsquigarrow$ Use $P_1, \ldots, P_r$ to find minimal decompositions.
- $\rightsquigarrow$ Compute at most r generators and at most r left components.

Total cost: Cost(Factoring $f(x) - f(t)$)$+\tilde{\mathcal{O}}(rn^2)$ field operations.

The polynomial case

Theorem [Blankertz, 2014]

All **minimal decompositions** of $f \in \mathbb{F}_q[t]$ can be found in $\tilde{O}(n^6)$.

- $\rightsquigarrow$ $g \circ h$ is a minimal dec. $\Leftrightarrow$ $K(h(t))$ is a maximal subfield.
- $\rightsquigarrow$ $K(h(t))$ must be a principal subfield.
- $\rightsquigarrow$ Use $P_1, \dots, P_r$ to find minimal decompositions.
- $\rightsquigarrow$ Compute at most r generators and at most r left components.

Total cost: $\tilde{\mathcal{O}}(n^{\omega+1}) + \tilde{\mathcal{O}}(rn^2)$ field operations, $2 < \omega \leq 3$.

The polynomial case

Theorem [Blankertz, 2014]

All **minimal decompositions** of $f \in \mathbb{F}_q[t]$ can be found in $\tilde{O}(n^6)$.

- $\rightsquigarrow$ $g \circ h$ is a minimal dec. $\Leftrightarrow$ $K(h(t))$ is a maximal subfield.
- $\rightsquigarrow$ $K(h(t))$ must be a principal subfield.
- $\rightsquigarrow$ Use $P_1, \ldots, P_r$ to find minimal decompositions.
- $\rightsquigarrow$ Compute at most r generators and at most r left components.

Total cost: $\tilde{\mathcal{O}}(n^4)$ field operations.

Some timings

K	n	r	$\#dec$	$d_q, \#c$	Decompose	Ayad & Fleischmann 08'
$\mathbb{F}_{11}$	12	7	3	3,1	0.01s	0.03s
$\mathbb{Q}$	24	8	6	1,4	0.02s	0.09s
$\mathbb{Q}$	144	10	6	1,4	1.82s	101.08s
$\mathbb{F}_{11}$	24	10	8	3,1	0.02s	0.20s
$\mathbb{F}_3$	18	12	12	4,1	0.05s	0.81s
$\mathbb{F}_{11}$	24	14	12	4,1	0.07s	10.57s
$\mathbb{F}_3$	60	17	5	5,1	0.18s	981.43s
$\mathbb{Q}$	60	17	5	1,8	0.77s	4,338.47s
$\mathbb{F}_{17}$	96	26	44	2,4	0.42s	$> 12h$
$\mathbb{F}_{11}$	60	60	111	3,5	1.91s	n.a.
$\mathbb{F}_{11}$	120	61	111	3,5	2.36s	n.a.
$\mathbb{F}_{13}$	169	91	14	3,7	3.41s	n.a.
$\mathbb{F}_5$	120	120	587	5,4	18.59s	n.a.
$\mathbb{F}_7$	168	168	680	4,9	50.53s	n.a.

Some timings

K	n	r	$\#dec$	$d_q, \#c$	Decompose	Ayad & Fleischmann 08'
$\mathbb{F}_{11}$	12	7	3	3,1	0.01s	0.03s
$\mathbb{Q}$	24	8	6	1,4	0.02s	0.09s
$\mathbb{Q}$	144	10	6	1,4	1.82s	101.08s
$\mathbb{F}_{11}$	24	10	8	3,1	0.02s	0.20s
$\mathbb{F}_3$	18	12	12	4,1	0.05s	0.81s
$\mathbb{F}_{11}$	24	14	12	4,1	0.07s	10.57s
$\mathbb{F}_3$	60	17	5	5,1	0.18s	981.43s
$\mathbb{Q}$	60	17	5	1,8	0.77s	4,338.47s
$\mathbb{F}_{17}$	96	26	44	2,4	0.42s	$> 12h$
$\mathbb{F}_{11}$	60	60	111	3,5	1.91s	n.a.
$\mathbb{F}_{11}$	120	61	111	3,5	2.36s	n.a.
$\mathbb{F}_{13}$	169	91	14	3,7	3.41s	n.a.
$\mathbb{F}_5$	120	120	587	5,4	18.59s	n.a.
$\mathbb{F}_7$	168	168	680	4,9	50.53s	n.a.

Thank you for your attention!