

前置：効率的記号的・代数的計算のための「近似」の利用

横山 和弘

立教大学・理学部数学科

## ■ Goals:

代数的数が関係する効率的計算のために代数的数の近似を利用する

- ⇒ そのままでは計算できないものを計算可能にする
- ⇒ 記号的・代数的計算の効率化を実現する
- ⇒ 計算結果の正当性を保証する

頭に浮かぶ計算例:

代数構造の分解: 多項式の因数分解、代数拡大体の計算、  
分解体の計算、ガロア群の計算

頭に浮かぶ計算技法:

基本計算: 線形方程式への帰着、補間法  
精度の向上: 中国人剰余定理、Hensel 構成

## 近似値による計算

⇒ 正しい答えに非常に近いと期待される

+

計算効率が良い

⇒ 近似でない記号的・代数的表現への変換を経て  
正しい答(の候補)

## 正しい答えを与える精度の評価 (theoretical bound)

⇒ 一般的には難しい (終結式の評価等の限られた技法  
実際の精度に比べ非常に大きくなる)

そこで、暫定的な精度 (heuristic) を適用する

## 正当性の検証の問題

効率的な正当性の判定テスト(検証)

候補の構成の計算量 より判定テストの計算量が多くなることもある

## ■ 代数構造の分解計算について

### 多項式イデアルの計算が基本

多項式の GCD、因数分解、代数拡大体上の多項式の因数分解



多項式イデアルの Gröbner 基底、根基イデアル計算、素分解、準素分解

### 特殊な形としてのガロア群計算、分解体計算

Point: 極大イデアルの零点が群の作用を通じて全て把握できる。

ひとつの零点の近似があれば、すべての零点の近似が求まる



頭に浮かぶ計算技法の格好の例:

基本計算: 線形方程式への帰着、補間法

精度の向上: 中国人剰余定理、Hensel 構成

## ■ 中心課題

候補の構成計算での問題: 近似の精度

効率と正確さのトレードオフ:

精度を高くする  $\Leftrightarrow$  計算量の増大

理論的に正当性を保証する精度  $\Leftarrow$  非常に巨大/計算不能

正当性計算での問題: 記号・代数的計算でのコスト

中間膨張: 計算途中での式(項)や係数の膨張

ユークリッド互除法、グレブナー基底計算、多項式因数分解における試し割り

新たな視点: 「複数の近似」を利用した正当性の検証

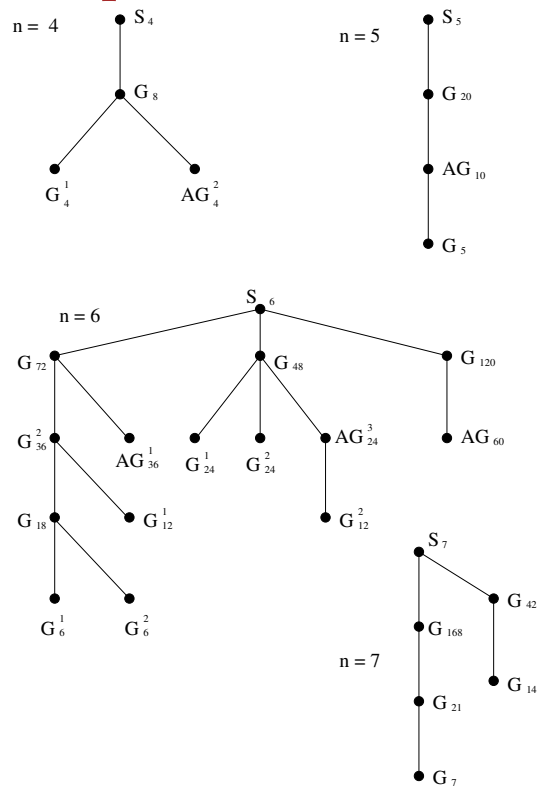
各代数的数に対する複数の近似の「対応」をどう処理するか?

## ■ 効果を検討する問題

### 多項式の高ア群とその分解体計算

### Descending Method (Stauduhar, 1973)

### Directed Graph of All Transitive Subgroups of $S_n$



## Descending Method

→ **Lagrange Relative Resolvent**

constructed from the given polynomial and a specified subgroup



Finding **Rational Roots** of Relative Resolvents using **Root Approximation**

**Existence** of a Rational Simple Root



**Inclusion** of the Galois group in Specified Subgroup

**[N] Numerical Root Approximation**

Huge Precision is required for Correctness of Computation

**[S] p-adic Root Approximation (or Root Approximation in Some Extension Field over  $\mathbb{Q}_p$ )**

## ■ Introduction to Computation of Galois Group and Splitting Field

### ■ Goal

Determine the Galois group of an irreducible integral polynomial  $f(x)$ , and Compute the splitting field of  $f$

### ■ Approach

**Galois Group:** Stauduhar's Approach (Descending Method)  
numeric/symbolic and deterministic algorithm



**Splitting Field:** Gröbner basis of the maximal ideal (the splitting field of  $f$ ) by using the data used in the computation of the Galois group.

## ■ Outline of Computation

Expression  $R$  of roots of  $f$ .



### **Galois Group:**

Find integral roots of resolvents by  $R$ .



### **Splitting Field:**

- Determine the shape of the Gröbner basis  $GB$  by the action of the Galois group on the roots.
- Compute  $GB$  by solving of the system of linear equations derived form  $R$ .  
**techniques:** Solvig the system and Lifting (Hensel)  
Interpolation and Chinese remainder theorem)
- **Check the correctness by ideal inclusion computation.**

### **Ideal Inclusion:**

For the candidate  $GB'$  of the Gröbner basis of the prime ideal  $\mathcal{M}$  corresponding to the splitting field,

$GB'$  is the correct one if

$Id(GB')$  contains the *ideal*  $\mathcal{M}_0$  of the relations between the roots of  $f$ .

## ■ Related Topics

- Change of Ordering (Basis Conversion)
- Generalized Shape Lemma (Univariate Rational Representation)
- Ideal Quotient

## Common Properties

- (1) All are reduced to problems on solving of systems of linear equations or interpolation if all zeros are known.
- (2) Each system is derived from the *guess of the shape* of the results.
- (3) The correctness can be easily checked by ideal inclusion.

## ■ Splitting Field and Ring

$f = x^n + f_{n-1}x^{n-1} + \cdots + f_1x + f_0$ : an irreducible (integral) polynomial

$\alpha_1, \alpha_2, \dots, \alpha_n$ : all roots of  $f$ ,  $X = \{x_1, \dots, x_n\}$

- The **splitting ideal**  $\mathcal{M}$  associated with the assignment of roots  $\alpha_1, \dots, \alpha_n$ :  
the Kernel of the ring homomorphism

$$\phi : g(x_1, \dots, x_n) \rightarrow g(\alpha_1, \dots, \alpha_n)$$

- The **splitting field**  $K_f$  corresponding to  $\mathcal{M}$ :

$$K_f := \mathbf{Q}[X]/\mathcal{M}$$

- The **Galois group**  $G_f$  corresponding to  $\mathcal{M}$ :

$$G_f := \text{Stab}_{S_n}(\mathcal{M}) \subset S_n \text{ acting on } X$$

- The **universal splitting ideal**  $\mathcal{M}_0$ :

$$\text{Id}(s_1(X) + f_{n-1}, s_2(X) - f_{n-2}, \dots, s_n(X) + (-1)^{n-1}f_0)$$

$s_i$  the  $i$ -th fund. symmetric function

- The **universal splitting ring**  $\mathcal{A}_0$ :

$$\mathbf{Q}[X]/\mathcal{M}_0$$

## ■ Lagrange Resolvent

- For a pair  $(H, L)$  of subgroups of  $S_n$  with  $H \subset L$ ,  **$L$ -relative  $H$ -invariant  $P$ :**

$$P \in \mathbf{Q}[X] \text{ and } \text{Stab}_L(P) = H$$

- For an  $L$ -relative  $H$ -invariant polynomial  $P$ , **the generic  $L$ -relative resolvent of  $P$ :**

$$\mathcal{L}_P^L(y) = \prod_{\tau \in H \setminus L} (y - P^\tau)$$

**the  $L$ -relative resolvent  $\mathcal{L}_{P,f}^L$  of  $P$  by  $f$ :**

$$\mathcal{L}_{P,f}^L(y) = \phi(\mathcal{L}_{P,f}^L(y)) = \prod_{\tau \in H \setminus L} (y - \phi(P^\tau))$$

- For the case  $L = S_n$ , we call  $\mathcal{L}_{P,f}^{S_n}$  the **absolute resolvent of  $f$  by  $P$**  and denote it simply by  $\mathcal{L}_{P,f}$ .

## ■ Useful Properties

$H, L$ : subgroups of  $S_n$  such that  $G_f \subset L, H \subset L$

$P$ : an  $L$ -relative invariant of  $H$

- If  $\phi(P^\sigma)$  is a simple root belongs to  $\mathbf{Q}$  for some  $\sigma$  in  $H \setminus L$ , then  $G_f (= \text{Stab}(e)) \subset H^\sigma$ . Moreover, when  $\text{char } \mathbf{Q} = 0$ ,

$$\mathcal{M} = (\cap_{\sigma \in G_f \setminus L} \mathcal{M}^\sigma) + \text{Id}(P^\sigma - \phi(P^\sigma)).$$

- There exists an  $L$ -relative invariant  $P'$  of  $H$  such that  $\mathcal{L}_{P',f}^L$  is square-free.

## ■ Scheme of Stauduhar Method

Applying Procedure repeatedly from  $L = S_n$ , we obtain  $G_f$ .

**Procedure( $L, \phi$ ):** ( $L$  contains  $G_f$ .)

Output:  $L$  as  $G_f$  or  $H$  a maximal subgroup containing  $G_f$ .

(1) Compute  $\mathcal{C}_L$ .

(the list of conjugate classes of maximal subgroups)

(2) For each  $H$  in  $\mathcal{C}_L$ , do:

(2.1) Compute  $H \setminus \setminus L$ .

(2.2) Compute an  $L$ -relative  $H$ -invariant  $P$ .

(2.3) Compute  $A_\sigma = \phi(P^\sigma)$  for every  $\sigma$  in  $H \setminus \setminus L$  and let

$\mathcal{S}_0 = \{\sigma \in H \setminus \setminus L \mid A_\sigma \in \mathbf{Z}\}$ .

(2.4) If  $\mathcal{S}_0 = \emptyset$ , then go to (3).

(2.5) If there is  $\sigma$  in  $\mathcal{S}_0$  such that  $A_\sigma \neq A_{\sigma'}$  for any  $\sigma' \neq \sigma$  in  $\mathcal{S}_0$ , then return  $H^\sigma$ .

Otherwise, go to (2.2).

(3) Return  $L$  as  $G_f = L$ .

## ■ Numeric/Symbolic Stauduhar Method

numerical approximation  $R_{num}$  or  $p$ -adic approximation  $R_p$ . So,  
 $R_{num} = \{\tilde{\alpha}_1, \dots, \tilde{\alpha}_n\}$  and  $R_p = \{\alpha_1^{(k)}, \dots, \alpha_n^{(k)}\}$ .

Let  $\phi_{num}$  and  $\phi_p$  be the map assigning  $x_i \rightarrow \tilde{\alpha}_i^{(k)}$ , and  $x_i \rightarrow \alpha_i^{(k)}$ , respectively.  
 And let  $\varphi$  be either  $\phi_{num}$  or  $\phi_p$ .

**Procedure 1**( $L, \varphi$ ): ( $L$  contains  $G_f$ .)

Output:  $L$  as  $G_f$  or  $H$  a maximal subgroup containing  $G_f$ .

- (1) Compute  $\mathcal{C}_L$ . (the list of conjugate classes of maximal subgroups).
- (2) For each  $H$  in  $\mathcal{C}_L$ , do:
  - (2.1) Compute  $H \setminus \setminus L$ .
  - (2.2) Compute an  $L$ -relative  $H$ -invariant  $P$ .
  - (2.3) Compute  $A_\sigma = \varphi(P^\sigma)$  for every  $\sigma$  in  $H \setminus \setminus L$  and let  
 $\mathcal{S}_0 = \{\sigma \in H \setminus \setminus L \mid A_\sigma \in \mathbf{Z} \text{ and } |A_\sigma| \leq M\}$ .
  - (2.4) If  $\mathcal{S}_0 = \emptyset$ , then go to (3).
  - (2.5) If there is  $\sigma$  in  $\mathcal{S}_0$  such that  $A_\sigma \neq A_{\sigma'}$  for any  $\sigma' \neq \sigma$  in  $\mathcal{S}_0$ , then return  $H^\sigma$ .  
 Otherwise, go to (2.2).
- (3) Return  $L$  as  $G_f = L$ .

## ■ Splitting field over $\mathbf{Q}_p$

- $\pi_p$ : the natural projection from  $\mathbf{Z}_p[X]$  to  $GF(p)[X]$
- $\mathbf{Q}_p[X]/\widetilde{\mathcal{M}}$ : the splitting field of  $f$  over  $\mathbf{Q}_p$
- $\widetilde{\mathcal{G}}$ : the Gröbner basis of  $\widetilde{\mathcal{M}}$  with respect to the lex order  $x_1 < \dots < x_n \Rightarrow \widetilde{\mathcal{G}} \subset \mathbf{Z}_p[X]$
- $GF(p)[X]/\overline{\mathcal{M}}$ : the splitting field of  $\pi_p(f)$  over  $GF(p)$
- $\overline{\mathcal{G}}$ : the Gröbner basis of  $\overline{\mathcal{M}}$  with respect to the order  $<$
- $\mathcal{G}^{(k)}$ :  $k$ -th approximation, i.e.  $\mathcal{G}^{(k)} \equiv \widetilde{\mathcal{G}} \pmod{p^{k+1}}$

⇓

$\mathcal{G}^{(k)}$  is lifted up from  $\overline{\mathcal{G}}$  by Hensel construction.  
 $\overline{\mathcal{G}}$  can be computed by algebraic factoring efficiently.

## ■ Evaluation of $\phi$

- **Sufficient Bound M:**  $2|L : H| < M$ ,  $|\phi(P^\sigma)| < M$  for  $\sigma \in H \setminus L$
- **Sufficient Degree k:**  $p^{k+1} \geq (2M)^{|L:H|}$
- **Approximation:**  $A_\sigma := \text{NormalForm}_{\mathcal{G}^{(k)}}(P^\sigma)$

$$A_\sigma \equiv \tilde{\phi}(P^\sigma) \pmod{p^{k+1}}$$

$\tilde{\phi}$  the ring homomorphism defined by  $\mathbf{Q}_p[X]/\tilde{\mathcal{M}}$

- **Conversion:** From  $A_\sigma$  to  $B_\sigma$  for  $\sigma$  if  $A_\sigma \in \mathbf{Z}$ :  
 $B_\sigma = A_\sigma$  if  $A_\sigma < p^{(k+1)/2}$ , and  $p^{k+1} - A_\sigma$  otherwise.

⇓

If  $B_\sigma \leq M$  and  $B_\sigma \neq B_{\sigma'}$  for any  $\sigma' \neq \sigma$  in  $\mathcal{S}_0$ ,  
then  $B_\sigma = \phi(P^\sigma)$  is a simple integral root of  $\mathcal{L}_{P,f}^L$ ,  
where  $\mathcal{S}_0 = \{\tau \in H \setminus L \mid A_\tau \in \mathbf{Z}, |B_\tau| \leq M\}$ .

## ■ Computation of Splitting Field

Suppose that we have already computed the Galois group  $G_f$  and the  $p$ -adic approximation  $R$  of roots of  $f$  and the map  $\phi_k$ .

We know also the action of  $G_f$  on  $R$ .

- $\phi_k$  corresponds to the splitting ideal  $\tilde{\mathcal{M}}$  of  $f$  in  $\mathbf{Q}_p[X]$ .
- Let  $H = \text{Stab}(\tilde{\mathcal{M}})$ , the Galois group of  $\pi_p(f)$ , where  $\pi_p$  denotes the projection from  $\mathbf{Z}[X]$  to  $GF(p)[X]$ . Then,  $H$  is a subgroup of  $G_f$ .
- For an element  $\sigma$  in  $S_n$ ,  $\phi_k^\sigma$  is the map  $x_i \rightarrow \alpha_{i\sigma}^{(k)}$ .

## ■ Computation of Splitting Field

### Procedure 2( $f, G_f, \varphi$ )

Output: the Gröbner basis  $GB$  of the splitting ideal  $\mathcal{M}$  with respect to the lex order.

- (1) Compute the shape of  $GB$  by the orbit lengths of  $t$ -points stabilizers of  $G_f$ .
- (2) **Compute the image  $\bar{GB}$  by solving of the system of linear equations:**

$$\varphi^\sigma(x_i^{n_i} + \sum c_{j_1, \dots, j_i} x_1^{j_1} \cdots x_i^{j_i}) = 0$$

for  $1 \leq i \leq n$  and  $\sigma$  in the coset  $H \setminus G_f$ .

- (3) Convert  $\bar{GB}$  to a candidate  $GB'$  of the Gröbner basis of  $\mathcal{M}$ .
- (4) **Check if  $Id(GB')$  contains the universal splitting ideal  $\mathcal{M}_0$ .**

If so, return  $GB'$ .

**Otherwise**, lift up the image  $\bar{GB}$  with higher precision

or using other approximation of roots with increased precision and goto (2).

## ■ Basic Property on Denominators of GB

Let  $\text{disc}(f)$  be the discriminant of  $f$ . Then,

$$GB \subset \frac{1}{\text{disc}(f)^N} \mathbf{Z}[X]$$

for some  $N$ .  $N$  is bounded by a function on  $\deg_{x_i}(f_i)$  ( $1 \leq i \leq n$ ), where  $GB = \{f_1, \dots, f_n\}$ .

↓

Moreover, the absolute value of the numerator of each coefficient of  $f_i$  is also bounded by a function on  $|\alpha_i|$ 's and  $\deg_{x_i}(f_i)$ 's.

**Transformation to rational numbers can be efficiently computed based on Euclidean algorithm.**

**Point: Use of Heuristic Bound Much Smaller Than Theoretical One**

## ■ Modular Image Computation

We introduce **indeterminates**  $a_j^{(i)}$  so that

$$g_i = x_i^{d_i} + \sum_{j=1}^{N_i} a_j^{(i)} t_j,$$

where  $N_i = |\mathbf{Q}(\alpha_1, \dots, \alpha_{i-1}) : \mathbf{Q}|$ .

Then, we have the following **system of linear equations**:

$$-V_i = M_i A_i,$$

where  $A_i = (a_j^{(i)})$ ,  $V_i = ((\alpha_i^{n_i})^{\sigma_j})$ , and

$$M_i = \begin{pmatrix} t_1(\alpha(i)^{\sigma_1}) & t_2(\alpha(i)^{\sigma_1}) & \cdots & t_{N_i}(\alpha(i)^{\sigma_1}) \\ t_1(\alpha(i)^{\sigma_2}) & t_2(\alpha(i)^{\sigma_2}) & \cdots & t_{N_i}(\alpha(i)^{\sigma_2}) \\ \vdots & \vdots & & \vdots \\ t_1(\alpha(i)^{\sigma_{N_i}}) & t_2(\alpha(i)^{\sigma_{N_i}}) & \cdots & t_{N_i}(\alpha(i)^{\sigma_{N_i}}) \end{pmatrix}.$$

## ■ Points for Practical Implementation

- **Choice of Prime:**

Efficiency of computations of  $\mathcal{G}^{k+1}$  and  $\text{NormalForm}_{\mathcal{G}^{k+1}}$  depends on the shape of the factorization of  $f$ .

**Random Choice Based on Chebotarev Density Theorem**

- **Modular Image Computation:**

Linear equation solving with Hensel lifting or Interpolation with Chinese remainder theorem

**Effective Choice Based on Complexity Analysis**

- **Conversion of Integers to Rational Numbers:**

We use the technique based on Euclidean algorithm for rational number reconstruction.

$$A \text{ modulo } p^{k+1} \rightarrow \frac{B}{C} \in \mathbb{Q}$$

- **Generation of Invariants:**

To find an invariant  $P$  such that  $\mathcal{L}_{P,f}^L$  is square-free, we generate a certain number of invariants.

**Tschirnhausen transformation**