Number Theoretic Algorithms

다항식의 해 구하기

September 23, 2019

1 다양한 체에서 다항식의 해 구하기

체 F 위의 다항식 P가 주어져 있을 때, $P(x) = 0$을 만족하는 $x \in F$를 찾는 것을 다항식의 해를 구한다고 하고, x를 다항식 P의 해라고 합니다. Ψ에서와 Φ에서의 곱셈을 identify할 수 있기 때문에, 해를 구하는 것은 다항식을 인수분해하는 것과 큰 관련이 있습니다.

일반적인 체에서 closed form으로 다항식의 해를 구하는 것은 **불가능합니다**.[1] 우리는 다음 세 가지의 매우 특수한 경우를 볼 것입니다:

- $F = \mathbb{Q}$.
- $F = \mathbb{R}$ 혹은 $F = \mathbb{C}$.
- $F = \mathbb{Z}_{p^k}$.

첫 번째 경우는 근이 유리수여야 한다는 사실을 이용하여, 순수하게 정수론적으로 문제를 해결할 수 있습니다. 신기한 것은 이 체 위에서도 일반적인 인수분해를 할 수 있습니다.[2] 이 경우는 characteristic이 0인 경우에도 해를 정확하게 기술하거나 인수분해를 완전히 하는 방법이 있다는 것을 제외하면, 특별히 우리의 관심사는 아닙니다.

두 번째 경우는 완비순서체의 확장입니다. 실수체에는 순서가 정해져 있기 때문에, 체 확장에서 각 성분별로 근사하여 해를 구하는 방법을 생각해 볼 수 있습니다. 우리는 이미 $F = \mathbb{R}$에서 해를 이런 식으로 근사하는 방법을 알고 있습니다. 이를 확장하여, $F = \mathbb{C}$에서 해를 근사하는 방법을 알아봅니다.

세 번째 경우는 유한 체이기 때문에, 가능한 해를 모두 넣어 보는 방법으로 naïve $\mathcal{O}(np^k)$, 혹은 $k = 1$인 경우 지난 자료의 polynomial evaluation을 사용하여 $\mathcal{O}(p \log^2 n)$ for $n := \deg P$ 시간에 해를 알아낼 수 있습니다. 우리는 p^k가 아주 크고 n이 대략 100 정도로 아주 작아, n에 대한 선형/제곱 시간은 괜찮고 p^k에 대한 선형 시간으로는 상당히 오래 걸리는 경우에 대해 시간을 줄이는 방법을 알아봅니다.

[1] 학부 대수학 시간에 alternating group A_5와 5차방정식의 해의 표현 불가능성을 배우게 됩니다.

[2] naïve한 방법은 이미 알고 계실지도 모르겠습니다. 효율적인 방법은 지나치게 복잡해서 다루지 않겠습니다.

2 $F = \mathbb{Q}$

$\mathbb{Q}$ 위에서 정의된 다항식 P는 정수계수 다항식으로 바꿀 수 있습니다. 다음 정리는 rational root theorem으로 잘 알려진 결과입니다.

Theorem 1 (Rational Root Theorem)**.** *정수계수 다항식 $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$에 대해, 만일 $x = p/q$가 P의 해라면, $p|a_0$이고 $q|a_n$이다.*

Proof. 일반성을 잃지 않고 $\gcd(p, q) = 1$이라 합니다.

$$\begin{aligned} q^n P(p/q) &= \sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i q^n \\ &= \sum_{i=0}^{n} a_i p^i q^{n-i} \end{aligned}$$

이고, $a_0 q^n = -p \cdot \sum_{i=1}^{n} a_i p^{i-1} q^{n-i}$와 $a_n p^n = -q \cdot \sum_{i=0}^{n-1} a_i p^i q^{n-1-i}$를 얻습니다. $\gcd(p, q) = 1$로부터 정리를 곧바로 얻습니다. □

이로부터 가능한 모든 해를 추정하는 방법으로 문제를 풀 수 있습니다. $F = \mathbb{Q}$인 경우 이를 더 빠르게 만드는 것은 우리의 관심사가 아닙니다. 원소의 개수가 무한히 많은 체에서도 다항식의 해를 찾을 수 있는 방법이 있다는 것을 제외하면 특별히 우리의 관심사도 아닙니다.

3 $F = \mathbb{R}$

우리는 이미 실수체인 경우 Newton's method가 매우 빠르게 수렴한다는 것을 알고 있습니다. 그러나, 지금은 Newton's method를 정수 연산으로 수정하지 않고 실수를 다루기 때문에 numerical stability에 대한 걱정이 생깁니다. 이 "걱정"을 해결해 보도록 합시다.

Newton's method의 식은 다음과 같습니다:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

3주차 자료에서 오차의 한계도 계산했습니다. 그러니 지금 우리의 관심사는 오차의 한계가 아니라 $\frac{f(x_n)}{f'(x_n)}$이 얼마나 커질 것인가입니다. 특히, $f'(x_n) = 0$이면 큰 문제가 생깁니다. $f(\alpha) = 0$이라고 두고, $x_n \to \alpha$라 하면,

$$\begin{aligned} f(x) &= (x - \alpha)g(x) \\ f'(x) &= g(x) + (x - \alpha)g'(x) \\ f'(\alpha) &= g(\alpha) = 0 \end{aligned}$$

이 말은 f가 α라는 근을 두 개 가지고 있다는 의미입니다.

다행히도, characteristic 0의 체 위에서 정의된 다항식의 경우, 중근을 제거하는 것이 대단히 쉽습니다. $f/\gcd(f, f')$를 계산하면 해집합이 그대로이면서 중근은 모두 제거되어 있는

다항식을 얻을 수 있습니다. 이제 우리의 관심사는 $f'(\alpha) \approx 0$이지만 $f'(\alpha) \neq 0$인 경우로 좁혀졌습니다.

만일 $f'(\alpha) = c \approx 0$이고 $c \neq 0$이면,

$$\frac{f(x_n)}{f'(x_n)} = \frac{f(x_n)}{k \cdot \frac{f(x_n)-f(\alpha)}{x_n-\alpha}} = \frac{1}{k} \cdot (x_n - \alpha) \quad \text{where} \quad k \approx 1$$

이므로, 중근만 제거해도 Newton's method를 이용하여 평범하게 계산할 수 **있다**는 결론이 나옵니다.[3]

실수체 위의 다항식 $P(x)$의 irreducible factor는 항상 일차 혹은 이차인데, 이 증명을 위해서는 복소수 해 $c \in \mathbb{C}$의 도움이 필요합니다. c가 P의 해라면 $\bar{c}$도 그러하며, $(x-c)(x-\bar{c}) = x^2 - (c+\bar{c})x + c\bar{c}$의 계수는 모두 실수입니다. 그러나, 증명에 복소수 해가 필요했듯이, quadratic irreducible factor들의 곱으로 이루어진 다항식 Q가 주어졌을 때 복소수의 도움 없이 이를 인수분해하는 것은 쉽지 않습니다.

4 $F = \mathbb{C}$

복소수 체인 경우 다항식 f를

$$f(x) = \sum_{k=0}^{n} r_k e^{i\theta_k} x^k \quad \text{then} \quad f(r,\theta) = \sum_{k=0}^{n} r_k r^k \cdot e^{i(\theta_k+\theta)}$$

와 같이 이변수 함수로 바꾸어 문제를 풀 수 있습니다. 이때 Newton's method의 식은

$$X_{n+1} = X_n - (f'(X_n))^{-1} \cdot (f(X_n))$$

과 같이 바뀌며, f'은 f의 Jacobian matrix입니다. Newton's method라는 이름에서 추정할 수 있듯이 이 방법 역시 quadratic convergence를 자랑하는 iterative method입니다.

또, 복소수 전체 영역으로 확장한 경우에는 상당히 아름다운 정리들이 많이 알려져 있습니다. 실수체의 경우와 마찬가지로 영점 주변에서 $1/f'$이 폭발적으로 커질 수 없다든지, 경계에서의 크기 비교를 통해 내부의 영점 개수를 알 수 있다든지(Rouché)[4] 하는 결과들이 알려져 있어서, numerical stability를 지키기 위해 이 사실들을 적절히 섞어서 사용할 수 있습니다.

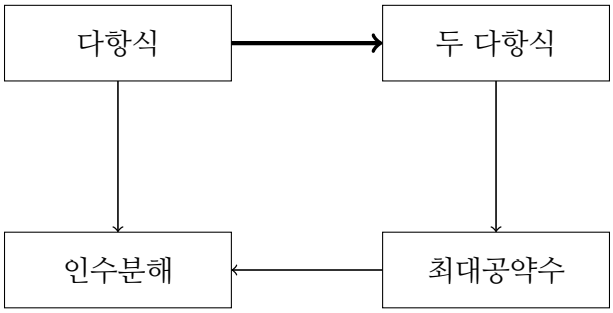
5 $F = \mathbb{Z}_{p^k}$

체 F 위에서 정의된 다항식 P의 가능한 해는 $|F|$개밖에 없으므로, 더 이상 근사를 생각하지 않고 해를 정확히 구하는 데 치중합니다.

[3] 우리의 마지막 관심사는 underflow입니다. 우리는 수의 길이에 대한 (거의) 선형으로 빠르게 계산할 수 있는 방법을 알기에, 이 문제는 일단 넘어갑니다. precision과 관련한 문제를 다루게 된다면, 그때 얘기하겠습니다.

[4] 이 결과는 실로 놀라운데, 계수만 보고 원점을 중심으로 하는 원 안에 영점이 몇 개 있는지 알 수 있기 때문입니다!

기본적으로 가능한 일차식 factor를 모두 구해 인수분해하는 것을 목표로 합니다. 소인수분해 때와 기본적인 아이디어는 같습니다.



그때와 화살표 방향이 약간 달라진 것을 알아채셔야 합니다. 물론 인수분해를 할 수 있다면 최대공약수를 구할 수 있는 것은 당연하지만, 우리의 관점은 그게 아닙니다. 지금 우리가 못하는 것을 굵은 화살표로 표시했습니다. 우리는 주어진 다항식과 해집합이 적당히 다른, 다른 다항식 하나를 찾지 못합니다.

numerical analysis를 할 것은 아니지만, 중근은 역시 골칫거리이므로 주어진 다항식 P에 대해 중근을 제거하려는 노력을 해 봅시다. 우리는 F의 모든 원소를 **한 번씩** 해로 갖는 다항식 $x^{|F|}-x$를 알고 있기에, 주어진 다항식 P와 $x^{|F|}-x$의 polynomial gcd를 구하는 방법으로 모든 중근을 제거할 수 있습니다. 이 과정 중에서 이차 이상의 factor도 P에서 제거됩니다.

만일 p가 홀수라면, 즉 $p>2$라면, 이 다항식의 일부 factor를 가져올 수 있습니다: $p^k-1=2m$인 자연수 m이 존재하므로,

$$x^{|F|}-x=x(x^{p^k-1}-1)=x(x^m-1)(x^m+1).$$

가장 왼쪽 식이 일차식으로 완전히 인수분해되기 때문에, 가장 오른쪽 식의 각 factor도 일차식으로 완전히 인수분해되며, 임의의 $d\in F$에 대해 x 대신 $(x+d)$를 대입하는 방법으로 가능한 factor를 무수히 많이 늘릴 수 있습니다.

다른 다항식으로 $Q(x)=x^m-1$을 골랐다고 합시다. P와 Q의 polynomial gcd를 어떻게 빠르게 계산할까요? 이는 quadratic gcd의 idea의 도움이 약간 필요한데, $x^m \mod P(x)$를 repeated squaring을 이용해 $\mathcal{O}(nk\log p\log n)$ 시간에 계산할 수 있습니다. 따라서 $(Q(x)=x^m-1) \mod P(x)$도 빠른 시간에 계산 가능하며, $\gcd(P,Q)=\gcd(P,Q \mod P)$임을 이용하여 여기서부터 subquadratic gcd를 이용하면 됩니다.

d를 임의로 고르면 50퍼센트의 확률로 인수가 나뉠 것을 예측할 수 있는데, 실제로도 그렇다는 것은 (polynomial) factor ring을 이용하여 증명하므로 여기서는 증명하지 않겠습니다. 따라서, 평균 시간복잡도가 $\mathcal{O}(nk\log p\log n+n\log^3 n)$입니다.

5.1 $p = 2$

$p = 2$라면 위와 같은 방법으로 나누는 것은 불가능한데, 그것은 $2m$이 더 이상 짝수가 아니기 때문입니다. 다음 식을 활용합니다.

$$x^{2^k} + x = (x + x^2 + x^4 + \cdots + x^{2^{k-1}})^2 + (x + x^2 + x^4 + \cdots + x^{2^{k-1}})$$

증명은 F의 characteristic이 2이므로 $(\sum a_i)^2 = \sum a_i^2$을 이용하면 쉽게 할 수 있습니다. 중요한 것은 이 식을 도대체 어떻게 얻었냐인데, 이는 각 다항식을 characteristic polynomial로 가지는 행렬과 깊은 연관이 있습니다.

아무튼 $p = 2$인 경우에 $(x^{2^k} + x)$가 $(x + x^2 + x^4 + \cdots + x^{2^{k-1}})$으로 나누어떨어지므로, 쓸만해 보이는 식을 얻었습니다. 중요한 것은 이를 어떻게 빠르게 계산하는가인데, 각각 제곱해서 더하는 것으로도 시간 $\mathcal{O}(nk \log p \log n)$이 얻어집니다. 따라서, 비슷한 방법을 이용해 평균 시간복잡도 $\mathcal{O}(nk \log p \log n + n \log^3 n)$을 달성할 수 있습니다.

6 문제

1. (Rouché) 복소해석학에서 Rouché 정리는 다음과 같이 기술됩니다.

   > 폐곡선 $C \subseteq \mathbb{C}$ 위의 모든 점 $z \in C$에 대해 $|f(z)| > |g(z)|$이면, C 내부에서 $f(z) + g(z)$와 $f(z)$의 영점의 개수는 같다.

   이 정리가 의미하는 바를 대략적으로 쓰면, 경계에서 대세에 영향을 주지 않는 함수를 더해도 영점의 개수에 영향을 주지 못한다는 의미입니다.

   (a) $\mathbb{C}$ 위에서 정의된 다항식 $z^8 + z^4 + z^3 + 1$의 해의 크기를 추정하세요. 즉, P의 임의의 해 z에 대해 $A \leq |z| \leq B$인 상수 A, B를 근사하세요.

   (b) $\mathbb{C}$ 위에서 정의된 임의의 다항식 $P(z) = a_n z^n + \cdots + a_0$에 대해 $a_n \neq 0 \neq a_0$이고 $C > 0$인 상수 C에 대해 $|a_i| \leq C \ \forall i$이면, P의 해 z_0에 대해 $|z_0| \geq \frac{a_0}{C+1}$임을 보이세요. 이 식이 의미하는 바는 계수의 크기가 적당히 작으면 해 자체가 작아질 일이 없다는 뜻입니다.

   (c) 대수학의 기본정리를 증명하세요. 증명 과정 중에 해가 모두 포함되는 원의 크기가 다항식의 차수에 영향을 받는 것을 알 수 있습니다. 이는 다항식의 **일반적인 성질**입니다. 즉, 안쪽에 해가 많을수록 바깥쪽에서 증가 폭이 큽니다.

2. (de Moivre's formula)

   (a) 정수 n에 대해 다음을 증명하세요.

   $$(\cos x + i \sin x)^n = \cos nx + i \sin nx$$

Hint.[5] 오일러는 일반적인 형태인 $e^{ix} = \cos x + i \sin x$를 증명했습니다. 이 식이 의미하는 바는 e^x의 자연스러운 복소 방향 확장이 있다면(좌변), 그 확장은 우변이 되어야 한다는 뜻입니다. 이 **notation**을 쓸 경우 사뭇 자명해 보이는 식 $(e^{ix})^n = e^{inx}$를 얻습니다.

(b) $\mathbb{C}$ 위에서 정의된 다항식 P에 대해 $P(r, \theta)$를 위와 같이 정의하지 않고, 표준적인 확장 $a+bi$를 이용할 경우 Newton's method를 적용하기 까다로움을 보이세요. 여기서 "까다롭다"란, 항 별로 변수가 분리된 형태가 아니어서 미분한 결과를 얻기가 힘들다는 의미입니다.

$a + bi$를 이용하는 경우 오차 분석이 어렵다는 단점이 있습니다. $P(r, \theta)$를 미리 계산해 두면, 계수만으로 절대 오차가 어느 정도가 될지 알 수 있어서 해를 정확하게 구하거나, 그러지 못하는 경우 그러지 못한다는 사실을 알 수 있습니다.

3. (Quadratic Convergence of Multivariate Newton's Method) 다변수 Newton's method에서의 error bound를 보이세요. 다변수에서의 Taylor 정리를 이용하여 증명할 수 있습니다.

4. 왜 유한 체에서는 중근을 제거할 때 $f/\gcd(f, f')$을 이용하지 않았을까요? "미분"을 7주차에서 정의한 사상 $D : F[x] \to F[x]$를 이용하여 $f' := Df$로 정의합니다.

   (a) characteristic이 p인 유한 체 F에서 정의된 다항식 $P(x) = x^p(x-1)$에 대해 $\gcd(P, P') = x^p$임을 보이세요. 따라서 $P/\gcd(P, P')$로는 중복 factor가 완전히 없어지는 경우가 있습니다.

   (b) $P/\gcd(P, P')$으로 중복 factor가 완전히 없어진다면, 그 factor f에 대해 어떤 g가 존재하여 $f = g^p$임을 보이세요.[6]

   (c) (b)에서 $f = g^p$임이 보장될 때, g를 빠르게 구하는 방법을 찾으세요. Hint: F의 characteristic이 p이므로... 따라서 f를 완전히 인수분해할 수 있는 방법을 찾는다면, $f/\gcd(f, f')$은 유용합니다.

5. (키파컵 G번 풀이)

   (a) 식에 최대 $\lceil \log_2(N+1) \rceil$개의 항밖에 없으므로, 위에서부터 $\lceil \log_2(N+1) \rceil + 1$개의 항 중 하나는 0입니다. 이를 통해 가능한 c의 값을 해로 가지는 방정식을 구하세요.

   (b) 이 방정식을 풀고, 가능한 c에 대해 다항식을 모두 구성하는 방법으로 키파컵 G번을 푸세요.

[5] $n = 0$부터 시작하여 양의 방향으로 수학적 귀납법. 음수의 경우 절댓값을 이용합니다.
[6] 화살표 뒤집기.