Dynamic Newton-Puiseux Theorem

Bassel Mannaa & Thierry Coquand

University of Gothenburg

Nov 30, 2011
Given \( P(X, Y) = 0 \) we want to express \( Y \) as a function in \( X \).

e.g. given \( Y^3 - XY + 1 = 0 \) then

\[
Y = -1 + 1/3X - 1/81X^3 + 1/243X^4 + \ldots
\]

Newton (1736) gave an algebraic solution and Puiseux (1850) found an analytic solution.
Abhyankar:
Newton theorem was revived by Puiseux in 1850. So it acquired the name ”Puiseux expansion” which is a misnomer. What’s more is that Puiseux proof which is based on Cauchy’s integral theorems, applies only to convergent power series with complex coefficients. On the other hand, Newton’s proof, being algorithmic, applies equally well to power series, whether they converge or not. Moreover, and that is the main point, Newton’s algorithmic proof leads to numerous other existence theorems while Puiseux’s existential proof does not do so.
Preliminaries

Binomial Theorem

For \( n \) rational,

\[
(1 + X)^n = 1 + nX + \cdots + \frac{n(n-1)\ldots(n-i+1)}{i!}X^i + \cdots
\]

We get a possibly infinite series (power series).

- We can find the solutions to \( Y^n - (1 + X)^m = 0 \)
Preliminaries

- We obtain solutions of
  \[ F(X, Y) = Y^n - (a + X)^m = Y^n - a^m(1 + X/a)^m = 0 \]
  by solving \( F(0, Y) = Y^n - a^m \).

  If \( a \in \mathbb{Q} \) and \( L \) is the splitting field of \( Y^n - a^m \) then the roots
  of \( F(X, Y) \) lie in \( L[[X]] \).

- Let \( F(X, Y) = Y^4 - X^2 + X = 0 \). Then
  \[ Y = X^{1/4}(1 + X)^{1/4} = X^{1/4}(1 + 1/4X - 3/32X^2 + ...) \]
  We obtain a factorization of \( F \) over \( \mathbb{Q}(i)[[X^{1/4}]] \).
Newton-Puiseux Theorem

Theorem (Newton-Puiseux Theorem)

Let $K$ be a field with $\text{char}(K) = 0$. Given $F \in K[X][Y]$, there exist a finite extension $L \supseteq K$ and $m \in \mathbb{Z}^+$ such that $F$ factors linearly over $L[[X^{1/m}]]$, i.e. $F = \prod_{i=0}^{n} (Y - \eta_i)$, $\eta_i \in L[[X^{1/m}]]$.

- Abhyankar (1990) gave a proof using Hensel’s lemma.
Newton-Puiseux Theorem

Newton-Puiseux theorem is used for instance to compute the parametrization of branches algebraic curves. e.g. the curve

\[ Y^3 + X^3 - 3XY \]

\[(t, 1/3t^2 + ...), (t^2, \sqrt{3}t - 1/6t^4 + ...), (t, -\sqrt{3}t - 1/6t^4 + ...)\]
The theorem should correspond to an algorithm generating the different factors.

How to specify such an algorithm? How to specify computation with algebraic numbers?
Dynamic evaluation of algebraic numbers

To obtain field extension we need a method of factorization of polynomials over the field.

- No general algorithm for factorization of polynomial over all explicitly given fields (van der Waerden).
- Fröhlich and Shepherdson constructed a particular extension $K_0$ of the rationals for which no factorization method of polynomials in $K_0[X]$ exist.
- Factorization is computationally expensive.
Dynamic evaluation (Duval et al.): We formally add the root of a polynomial without deciding if it is irreducible or not. The result is an algebra over the base field rather than a field extension. We proceed lazily and discover factors of the polynomial when testing if an element is zero or unit.

Let \( p \in K[X] \) be square-free, \( a \in K[X]/(p) \).

\( a \) is 0 in \( K[X]/(\gcd(p, a)) \) and 1 in \( K[X]/(p/\gcd(p, a)) \).
Dynamic evaluation of algebraic numbers

We can always extend the algebra with new algebraic elements and refine it to resolve anomalies.

\[
\begin{array}{c}
\mathbb{Q} \\
\mid
\mathbb{Q} \langle \alpha^2 - 2 \rangle \quad \alpha \\
\mid \\
\mathbb{Q} \langle \alpha^2 - 2, \beta^2 - 2 \rangle \quad \beta \\
\end{array}
\]

\[
\begin{array}{c}
\mathbb{Q} \langle \alpha^2 - 2, \beta - \alpha \rangle \quad \text{yes} \\
\mathbb{Q} \langle \alpha^2 - 2, \beta + \alpha \rangle \quad \text{no}
\end{array}
\]

root of $X^2 - 2$? 

root of $X^2 - 2$? 

$\alpha = \beta$?
Triangular separable algebra

Definition (Triangular separable algebra)

A triangular separable algebra over a field $K$ is an algebra

$K[a_1, a_2, ..., a_n], p_1(X), p_2(a_1, X), ..., p_n(a_1, ..., a_{n-1}, X)$

Where $p_i$ is a separable polynomial in $K[a_1, ..., a_{i-1}][X]$ and $a_i$ is a root of $p_i$.

- For example, $\mathbb{Q}[a, b], a^2 - 2 = 0, b^2 - ab + 2 = 0$
Triangular separable algebra

Triangular separable algebras are (von Neumann) regular, i.e.
\[ \forall a \in R \ \exists! b \in R \ a^2 b = a \land b^2 a = b. \]

The ring of polynomials over a regular ring behave much like the ring of polynomials over a field.
A cover of a triangular separable algebra is the set of leaves of a tree of extensions and refinements of the algebra. e.g. the set \( \{ A, B \} \) is a cover of \( R \).

\[
\begin{align*}
R & \\
\quad \mid & \\
R\langle \alpha^4 - 5\alpha^2 + 6 \rangle & \\
\quad \mid & \\
B = R\langle \alpha^2 - 2 \rangle & \quad R\langle \alpha^2 - 3 \rangle \\
\quad \mid & \\
A = R\langle \alpha^2 - 3, \beta^2 + \alpha + 1 \rangle
\end{align*}
\]
For *sheaf models* over a space the existential quantifier is interpreted by a covering by open subsets. In our setting the *existence* of a finite algebraic extension of the base field $K$ becomes a cover of $K$. 
Dynamic Newton-Puiseux Theorem

Theorem (Dynamic Newton-Puiseux Theorem)

Let $K$ be a field of characteristic 0 and $F \in K[X][Y]$ a monic polynomial of degree $n$ separable in $Y$, i.e.

$\exists P, Q \in K(X)[Y] \quad PF + QF_Y = 1$. Then there exists a cover $C$ of $K$ and $m \in \mathbb{Z}^+$ such that for all $R \in C$, $F$ factors linearly over $R[[X^{1/m}]]$, i.e. $F = \prod_{i=1}^{n} (Y - \eta_i)$, $\eta_i \in R[[X^{1/m}]]$. 

Let \( R_1 = \langle K[a_1, \ldots, a_n], p_1, \ldots, p_n \rangle \) and \( R_2 = \langle K[b_1, \ldots, b_m], q_1, \ldots, q_n \rangle \) be two algebras in the resulting cover. Then,

- \( R_2 \) splits \( R_1 \) and \( R_1 \) splits \( R_2 \). Meaning, each of \( p_1, \ldots, p_n \) splits over \( R_2 \) and vice-a-versa.

- If \( P_1 \in \text{Spec}(R_1) \) and \( P_2 \in \text{Spec}(R_2) \) then \( R_1/P_1 \cong R_2/P_2 \).

Let \( R \) be an algebra in the resulting cover

- \( R \) splits itself.

- If \( P \in \text{Spec}(R) \) then \( L = R/P \) is normal.
\[ Y^5 - 7 \, Y^4 + 13 \, Y^3 + 5 \, Y^2 - 30 \, Y + 18 + X \, Y \]

State: \( a - \frac{8}{5} = 0, b^2 + \frac{3}{14} = 0, c^3 - \frac{7}{3}c + \frac{34}{27} = 0, d^2 + \frac{3}{4}c^2 - \frac{7}{3} = 0 \)

Result: 
\[ (Y-3-bX^{1/2}-\frac{43}{392}X+ \ldots) \]
\[ (Y-3+bX^{1/2}-\frac{43}{392}X+ \ldots) \]
\[ (Y-c-\frac{1}{3}+(\frac{129}{196}c^2+\frac{30}{49}c-\frac{559}{588})X+ \ldots) \]
\[ (Y-d+\frac{1}{2}c-\frac{1}{3}+(-\frac{29}{196}cd+\frac{30}{49}d-\frac{29}{392}c^2-\frac{5}{49}c+\frac{86}{147})X+ \ldots) \]
\[ (Y+d+\frac{1}{2}c-\frac{1}{3}+(\frac{129}{196}cd-\frac{30}{49}d-\frac{29}{392}c^2-\frac{5}{49}c+\frac{86}{147})X+ \ldots) \]

State: \( a^3+\frac{16}{5}a^2+\frac{27}{25}a-\frac{2}{125} = 0, b-\frac{1}{4}a-\frac{8}{5} = 0, c^2+\frac{3}{14} = 0, d^2+\frac{3}{4}a^2+\frac{8}{5}a-\frac{37}{25} = 0 \)

Result: 
\[ (Y-a-\frac{7}{5}+(\frac{129}{196}a^2+\frac{494}{245}a+\frac{2211}{4900})X+ \ldots) \]
\[ (Y-3-cX^{1/2}-\frac{43}{392}X+\frac{7621}{65856}cX^{3/2}+ \ldots) \]
\[ (Y-3+cX^{1/2}-\frac{43}{392}X-\frac{7621}{65856}cX^{3/2}+ \ldots) \]
\[ (Y-d+\frac{1}{2}a+\frac{1}{5}+(-\frac{29}{196}ad-\frac{22}{245}d-\frac{29}{392}a^2-\frac{247}{245}a-\frac{42}{1225})X+ \ldots) \]
\[ (Y+d+\frac{1}{2}a+\frac{1}{5}+(\frac{129}{196}ad+\frac{22}{245}d-\frac{29}{392}a^2-\frac{247}{245}a-\frac{42}{1225})X+ \ldots) \]
State: \(a^3 + \frac{16}{5}a^2 + \frac{27}{25}a - \frac{2}{125} = 0\), \(b^2 + \frac{1}{2}ab + \frac{16}{5}b + \frac{13}{16}a^2 + \frac{12}{5}a + \frac{27}{25} = 0\), \(c - \frac{1}{3}b - \frac{1}{4}a - \frac{8}{5} = 0\), \(d^2 + \frac{3}{14} = 0\)

Result: 

\[\begin{align*}
(Y - a - \frac{7}{5} + (129/196a^2 + 494/245a + 2211/4900)X + \ldots) \\
(Y - b + \frac{1}{4}a - \frac{7}{5} + (-29/196ab - 22/245b - 387/784a^2 - 33/490a - 318/1225)X + \ldots) \\
(Y - 3 - dX^{1/2} - 43/392X + 7621/65856dX^{3/2} + \ldots) \\
(Y - 3 + dX^{1/2} - 43/392X - 7621/65856dX^{3/2} + \ldots) \\
(Y + b + \frac{3}{4}a + \frac{9}{5} + (129/196ab + 22/245b - 29/784a^2 + 33/490a + 34/1225)X + \ldots)
\end{align*}\]