IMPLICIT FUNCTION THEOREM FOR FORMAL POWER SERIES

Yining Hu
School of Mathematics and Statistics, Huazhong University of Science and Technology, Wuhan, PR China
huyining@protonmail.com

Received: 6/19/17, Accepted: 2/27/18, Published: 3/16/18

Abstract

We generalize a result of Furstenberg about the diagonal of bivariate rational fractions and algebraic series, and give a direct proof of an explicit implicit function theorem for formal power series that is valid for all fields, which implies, in particular, a Lagrange inversion formula and a Flajolet-Soria coefficient extraction formula known for fields of characteristic 0.

1. Main Result

We show that the implicit function theorem for formal power series is a direct consequence of a generalization of Furstenberg's theorem about the diagonal of rational functions and algebraic series.

Theorem 1. *Let K be an arbitrary field. If $P(X,Y) \in K[[X,Y]]$ and $f(X) \in K[[X]]$ are such that $f(0)=0$, $P(X,f(X)) = f(X)$ and $P'_Y(0,0)=0$, then for all $n \in \mathbb{N}$*

$$[X^n]f = \sum_{m\geq 1} [X^n Y^{m-1}](1-P'_Y(X,Y))P^m(X,Y).$$

If the characteristic of K is 0, we also have the following form

$$[X^n]f = \sum_{m\geq 1} \frac{1}{m}[X^n Y^{m-1}]P^m(X,Y).$$

Remark 1. The general case can also be deduced from the 0 characteristic case by regarding the coefficients of $f = \sum_{i=0}^{\infty} f_i X^i$ as indeterminates and the first formula as an identity in $\mathbb{Z}[f_1, f_2, ...]$.

Remark 2. The conditions $P(X, f(X)) = 0$ and $f(0) = 0$ imply that $P(0,0) = 0$. As $P'_Y(0,0)$ is also 0, the sums in both expressions of $[X^n]f$ are finite.

Remark 3. Similar results in characteristic 0 can be found in [6].

Remark 4. When $P(X,Y) = X\phi(Y)$, where $\phi(X) \in K[[X]]$ and $\phi(0) \neq 0$, we obtain the Lagrange inversion formula

$$[X^n]f = [Y^{n-1}](\phi(X)^n - Y\phi'(X)\phi(X)^{n-1}).$$

If the characteristic of K is 0, we also have the following form:

$$[X^n]f = \frac{1}{n}[Y^{n-1}]\phi(Y)^n.$$

For different proofs of the Lagrange inversion formula in characteristic 0, see [4].

Remark 5. When $P(X,Y)$ is a polynomial in X and Y, we obtain the Flajolet-Soria coefficient extraction formula. See [1], [7] for proofs in characteristic 0. See [5] for a proof for arbitrary fields using Furstenberg's Theorem.

2. Proof

When K is a field of 0 characteristic, where $P(X,Y) \in K[[X,Y]]$ and $f(X) \in K[[X]]$ with $f(0) = 0$, the Taylor formula takes the form

$$P(X,Y) = \sum_{n=0}^{\infty} \frac{1}{n!}(Y - f(X))^n P_Y^{(n)}(X, f(X)).$$

However, because of the $n!$ in the denominators, we cannot use it in positive characteristic. To make up for this, we define $P_Y^{[m]}(X,Y)$ as an alternative to the m-th partial derivative of P with respect to Y that "absorbs" the factorial. Once this obstacle is circumvented, the Taylor formula works as expected.

Definition 1. Let $P(X,Y) \in K[[X,Y]]$,

$$P(X,Y) = \sum_{j=0}^{\infty} a_j(X)Y^j,$$

where $a_j(X) \in K[[X]]$. We define

$$P_Y^{[m]}(X,Y) = \sum_{j=m}^{\infty} \binom{j}{m} a_j(X)Y^{j-m}.$$

for $m \in \mathbb{N}$.

Proposition 1. *Let K be an arbitrary field. Let $P(X,Y) \in K[[X,Y]]$ and $f(X) \in K[[X]]$ with $f(0) = 0$. Then*

$$P(X,Y) = \sum_{m=0}^{\infty} (Y - f(X))^m P_Y^{[m]}(X, f(X)). \tag{*}$$

Proof. Let $P(X,Y)=\sum\limits_{j=0}^{\infty} a_j(X)Y^j$ with $a_j(X)\in K[[X]]$ for $j\in\mathbb{N}$. We prove that for all $k\in\mathbb{N}$, the coefficients of Y^k in the left side and the right side of $(*)$ are equal. Indeed, we have

$$\begin{aligned}
&[Y^k]\sum_{m=0}^{\infty}(Y-f(X))^m P_Y^{[m]}(X,f(X))\\
=&\sum_{m=k}^{\infty}\binom{m}{k}(-f(X))^{m-k}\sum_{j=m}^{\infty}\binom{j}{m}a_j(X)f(X)^{j-m}\\
=&\sum_{j=k}^{\infty}a_j(X)f(X)^{j-k}\sum_{m=k}^{j}\binom{j}{m}\binom{m}{k}(-1)^{m-k}\\
=&\sum_{j=k}^{\infty}a_j(X)f(X)^{j-k}\sum_{m=k}^{j}\binom{j}{j-m,m-k,k}(-1)^{m-k}\\
=&a_k(X).
\end{aligned}$$

We have the last equality because $\sum\limits_{m=k}^{j}\binom{j}{j-m,m-k,k}(-1)^{m-k}=1$ if $j=k$ and 0 if $j>k$. This is because we have the multinomial expansion

$$\begin{aligned}
(a+b+c)^j&=\sum_{k\le m\le j}\binom{j}{j-m,m-k,k}a^{j-m}b^{m-k}c^k\\
&=\sum_{k=0}^{j}\sum_{m=k}^{j}\binom{j}{j-m,m-k,k}a^{j-m}b^{m-k}c^k.
\end{aligned}$$

When we take $a=1$, $b=-1$, the identity becomes

$$c^j=\sum_{k=0}^{j}\left(\sum_{m=k}^{j}\binom{j}{j-m,m-k,k}(-1)^{m-k}\right)c^k.$$

Seeing this as a polynomial identity in the variable c gives us the desired result. □

The following corollary is immediate.

Corollary 1. *Let K be an arbitrary field. Let $Q(X,Y)\in K[[X,Y]]$ and $f(X)\in K[[X]]$ be such that $f(0)=0$ and $Q(X,f(X))=0$. Then there exists $R(X,Y)\in K[[X,Y]]$ such that $Q(X,Y)=(Y-f(X))R(X,Y)$.*

Definition 2. For the formal power series in $K((X_1,...,X_m))$

$$P(X_1,X_2,...,X_m)=\sum_{n_i>-\mu} a_{n_1n_2...n_m}X_1^{n_1}X_2^{n_2}...X_m^{n_m}$$

its (principal) diagonal $\mathcal{D}f(t)$ is defined as the element in $K((T))$

$$\mathcal{D}P(T)=\sum a_{nn...n}T^n.$$

In [3], Furstenberg proved the following result about algebraic series and the diagonal of rational fractions.

Proposition 2. (Furstenberg) *Let K be an arbitrary field. Let $Q(X,Y)\in K[X,Y]$ and $f(X)\in K[[X]]$ be such that $f(0)=0$, $Q(X,f(X))=0$ and $Q'_Y(0,0)\neq 0$, then*

$$f(X)=\mathcal{D}\left(Y^2\frac{Q'_Y(XY,Y)}{Q(XY,Y)}\right).$$

Proposition 2 can be used to deduce a coefficient extraction formula for algebraic series with coefficients in an arbitrary field (see Remark 5) and can be used to compute efficiently the n-th term of an algebraic series with coefficients in a field of positive characteristic [2].

The following proposition is a generalization of Proposition 2, where $Q(X,Y)$ can be any formal power series and not just a polynomial. The only difference in the proof is in the first step where we use Corollary 1 to factorize $Q(X,Y)$.

Proposition 3. *Let K be an arbitrary field. Let $Q(X,Y)\in K[[X,Y]]$ and $f(X)\in K[[X]]$ be such that $f(0)=0$, $Q(X,f(X))=0$ and $Q'_Y(0,0)\neq 0$. Then*

$$f(X)=\mathcal{D}\left(Y^2\frac{Q'_Y(XY,Y)}{Q(XY,Y)}\right).$$

Proof. Using Corollary 1 we can write $Q(X,Y)=(Y-f(X))R(X,Y)$ with $R(X,Y)\in K[[X,Y]]$. We have $R(0,0)\neq 0$ because $f(0)=0$ and $Q'_Y(0,0)\neq 0$. Then

$$\frac{1}{Q(X,Y)}Q'_Y(X,Y)=\frac{1}{Y-f(X)}+\frac{R'_Y(X,Y)}{R(X,Y)}.$$

Replacing X by XY and multiplying by Y^2 we get

$$\mathcal{D}\left(Y^2\frac{Q'_Y(XY,Y)}{Q(XY,Y)}\right)=\mathcal{D}\left(\frac{Y^2}{Y-f(XY)}\right)+\mathcal{D}\left(Y^2\frac{R'_Y(XY,Y)}{R(XY,Y)}\right). \qquad (\dagger)$$

For the first term on the right side of (†) we have

$$\begin{aligned}
&\mathcal{D}\left(\frac{Y^2}{Y-f(XY)}\right)\\
=&\mathcal{D}\left(\frac{Y}{1-Y^{-1}f(XY)}\right)\\
=&\mathcal{D}\left(\sum_{n=0}^{\infty}Y^{-n+1}f(XY)^n\right)\\
=&\mathcal{D}\left(f(XY)\right)\\
=&f(X).
\end{aligned}$$

For the second term, as $R(0,0)\neq 0$, $\frac{R'_Y(XY,Y)}{R(XY,Y)}$ is a power series in XY and Y, so when we multiply this by Y^2 there is no diagonal term.

□

Proof of Theorem 1. Let the power series $Q(X,Y)$ be defined as $Q(X,Y)=P(X,Y)-Y$, then $Q'_Y(0,0)=P'_Y(0,0)-1\neq 0$, and $Q(X,f(X))=P(X,f(X))-f(X)=0$. According to Proposition 3,

$$\begin{aligned}
f&=\mathcal{D}\{Y^2Q'_Y(XY,Y)/Q(XY,Y)\}\\
&=\mathcal{D}\{Y^2(P'_Y(XY,Y)-1)/(P(XY,Y)-Y)\}\\
&=\mathcal{D}\{Y(1-P'_Y(XY,Y))/(1-\frac{P(XY,Y)}{Y})\}\\
&=\mathcal{D}\{Y(1-P'_Y(XY,Y))(1+\sum_{m\geq 1}(\frac{P(XY,Y)}{Y})^m)\}.
\end{aligned}$$

We have the last equality due to the fact that $P'_Y(0,0)=0$, $\frac{P(XY,Y)}{Y}$ has no constant term, and therefore $1/(1-\frac{P(XY,Y)}{Y})=1+\sum_{m\geq 1}(\frac{P(XY,Y)}{Y})^m$. As in each term of $Y(1-P'_Y(XY,Y))$ the power of Y is larger than that of X, it cannot contribute to the diagonal. Therefore,

$$\begin{aligned}
f_n&=[X^nY^n]Y(1-P'_Y(XY,Y))(1+\sum_{m\geq 1}(\frac{P(XY,Y)}{Y})^m)\\
&=[X^nY^n]Y(1-P'_Y(XY,Y))(\sum_{m\geq 1}(\frac{P(XY,Y)}{Y})^m)\\
&=\sum_{m\geq 1}[X^nY^{m-1}](1-P'_Y(X,Y))P(X,Y)^m.
\end{aligned}$$

□

References

[1] C. Banderier and M. Drmota, Formulae and asymptotics for coefficients of algebraic functions, *Combin. Probab. Comput.* **24**, (2015), No. 1, 1-53.

[2] A. Bostan, G. Christol, P. Dumas, Fast computation of the nth term of an algebraic series over a finite prime field, *Proceedings ISSAC'16*, pp. 119-126, ACM Press, 2016.

[3] H. Furstenberg, Algebraic functions over finite fields, *J. Algebra* **7**, (1967) 271-277.

[4] I. Gessel, Lagrange inversion, *J. Combin. Theory* Ser. A **144** (2016), 212-249.

[5] Y. Hu, Coefficient extraction formula and Furstenberg's theorems, arXiv:1505.01379.

[6] A. Sokal, A ridiculously simple and explicit implicit function theorem, *Sém. Lothar. Combin.* 61A (2009/11).

[7] M. Soria, Thèse d'habilitation (1990), LRI, Orsay.