About algebraicity of power series in positive characteristic

1. Warm-up: rationality

Let k be a field. Consider

$$\begin{array}{ccc} k[[t]] & \subset & k((t)) \\ | & & | \\ k[t] & \subset & k(t) \end{array}$$

Question: Given $f \in k[[t]]$, how to recognize if $f \in k(t)$?

e.g. $f(t) = t + t^2 + 2t^3 + 3t^4 + 5t^5 + 8t^6 + 13t^7 + \cdots$

(Fibonacci number)

is indeed rational because $f(t) = \dfrac{t}{1-t-t^2}$

More generally, one proves that f is rational iff its sequence of coefficients satisfies a recurrence of the form:

$$a_n = \lambda_1 a_{n-1} + \cdots + \lambda_r a_{n-r} \qquad \begin{array}{l} \forall n \geq r \\ \lambda_i \in k \end{array}$$

Dwork criterion: Let

$$N_{s,m} = \begin{vmatrix} a_s & a_{s+1} & \cdots & a_{s+m} \\ \vdots & & & \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m} \end{vmatrix} \qquad (m+1)\times(m+1)\text{ - matrix}$$

Then f is rational iff $\exists S, m$ s.t. $N_{s,m} = 0$, $\forall s \geq S$

Now we move to algebraicity, ie we wonder if there exist $P \in k[X,Y]$ s.t.

$$P(t, f(t)) = 0, \quad P \neq 0$$

2. Examples: p-Lucas property

Binomial coefficient $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$

Recall that if $n', k' < p$, then

$$\binom{pn+n'}{pk+k'} \equiv \binom{n}{k} \cdot \binom{n'}{k'} \pmod p$$

Proof: Expand $(1+t)^{pn+n'} \equiv (1+t^p)^n \cdot (1+t)^{n'} \pmod p$

and look at the coefficient in $t^{pk+k'}$

Corollary: i) Set $u_n = \binom{2n}{n}$; then $u_{ap+b} \equiv u_a \cdot u_b \pmod p$

(Lucas' property)

ii) For all k, the series

$$f(t) = \sum_{n \geq 0} u_n^k t^n$$

is algebraic

proof: Notice that Lucas' property implies that

$$f(t) = f_p(t)\, f(t)^p \quad \text{with} \quad f_p(t) = \sum_{n=0}^{p-1} u_n^k t^n.$$

Other examples:

* Apery numbers: $u_n = \sum_{k=0}^{n} \binom{n}{k}^2 \cdot \binom{n+k}{k}$

(also Lucas)

* hypergeometric functions

Pochhammer notation $(a)_n = a(a+1)\cdots(a+n-1)$

$$ {}_pF_q\left(\begin{matrix} a_1 & \cdots & a_p \\ b_1 & \cdots & b_q \end{matrix}; t\right) = \sum_{n \geq 0} \frac{(a_1)_n \cdots (a_p)_n}{(b_1)_n \cdots (b_q)_n \cdot n!} t^n$$

e.g. $\exp$, $(1-t)^a$, $\frac{\arcsin(z)}{z}$, ${}_2F_1\left(\begin{matrix} 1/3 & 2/3 \\ & 3/2 \end{matrix}; \frac{27x^2}{4}\right) = \frac{\sqrt[3]{\frac{3x\sqrt{3}+\sqrt{27x^2+4}}{2}} - \sqrt[3]{\frac{2}{3x\sqrt{3}+\sqrt{27x^2+4}}}}{x\sqrt{3}}$

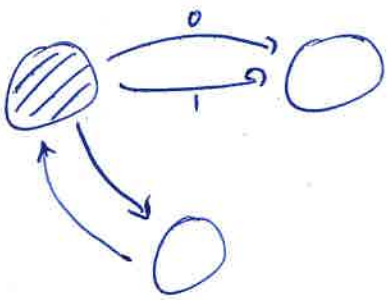
Sometimes hypergeometric functions can be reduced modulo primes, e.g. ${}_3F_2\left(\begin{matrix} 2/9 & 5/9 & 8/9 \\ 2/3 & 1 & \end{matrix}; t\right)$ [works for all $p \neq 3$]
$\quad = f(t)$

One proves that $f(t)$ is p-Lucas (hence algebraic) when $p \equiv 1 \pmod 3$
p^2-Lucas when $p \equiv 2 \pmod 3$

<u>Theorem</u> (Vargas-Montoya):
If an hypergeometric function $f(t)$ can be reduced mod p for almost all p (we say that f is globally bounded), then
$f(t) \bmod p$ is algebraic for almost all p.
with annihilating polynomial of the form $a_0 x + a_1 x^p + \dots + a_n x^{p^n} = 0$
(n indep. from p)

3. Christol's theorem

Here $k = \mathbb{F}_p$.
An automaton is something like



states
+ transitions

$\rightsquigarrow$ p-automatic sequences

<u>Theorem</u> (Christol): $f(t) = \sum_{n \geq 0} a_n t^n$ is algebraic iff the sequence (a_n) is p-automatic.

Reformulation without automaticity.
Now k is any perfect field of characteristic $p > 0$

Section operator:

$$S_r : k[[t]] \longrightarrow k[[t]]$$
$$\sum_{n\geq 0} a_n t^n \longmapsto \sum_{n\geq 0} a_{pn+r}^{1/p} t^n$$

<u>Theorem:</u> $f(t)$ is algebraic
iff $\exists$ finite dimensional k-vector space $W \subset k[[t]]$
with $f(t) \in W$ and f stable by S_r, $r = 0, \dots, p-1$

Link with automaton: $\{\text{states}\} = W$ [here $k = \mathbb{F}_p$]

Christol's proof: if $P(x,y)$ annihilates $f(t)$, with $P(0,0)=0$, $\frac{\partial P}{\partial y}(0,0) \neq 0$ then

$$f(t) = \mathrm{Diag}\left(\frac{y^2 \cdot \frac{\partial P}{\partial y}(xy, y)}{P(xy,y)} \right) \quad \text{[Furstenberg's theorem]}$$

and one takes $W = \left\{ \mathrm{Diag}\left(\frac{Q(x,y)}{P(xy,y)} \right) \text{ with } \deg Q \leq \deg P \right\}$

In fact, a small variation (however not obvious to prove) works without the regularity assumption:

Theorem (Bostan, C, Christol, Dumas)

$$W = \left\{ \frac{Q(t, f(t))}{\frac{\partial P}{\partial y}(t, f(t))} \text{ with } \deg Q \leq \deg P \right\} \text{ always works.}$$

Benefits: . W very explicit, . gives sharp bounds on the alg degree
. extends verbatim to multivariate series
(joint work with Adamczewski, Bostan)

4. Back to diagonals

With a similar argument, one can prove the following.

Theorem: (ABC) Let $f(x_1,\dots,x_n) \in k[[x_1,\dots,x_n]]$ be algebraic of degree d and height $h_1,\dots,h_n$.

Then $\mathrm{Diag}(f)$ is algebraic as well, annihilated by a polynomial of the form:

$$a_0 f + a_1 f^p + \dots + a_N f^{p^N} \quad \text{with } a_i \in k(t)$$

and $N \leq (h_1+1)\cdots(h_n+1)(d+1)$

[+ explicit method for finding an annihilating polynomial]

The theorem implies that $\mathrm{Gal}(f(t)) \subset GL_N(\mathbb{F}_p)$.

If we start with a diagonal $f(t)$ of an algebraic series in characteristic zero, and assume that $f_p(t) := f(t) \bmod p$ is defined for almost all p, then it is algebraic with Galois group $\subset GL_N(\mathbb{F}_p)$ for N independant from p.

Can we say something about the variation of this Galois group. Looks difficult in general but something happens in some cases, e.g: (joint with F. Fürnsinn)

$$(1) \quad {}_3F_2\left(\begin{matrix} 2/9 & 5/9 & 8/9 \\ & 2/3 & 1 \end{matrix}; t\right) = \mathrm{Diag}\left(\frac{\sqrt[3]{1-x_1-x_2}}{1-x_1-x_2-x_3}\right)$$

one expects: $\mathrm{Gal} \simeq \mathbb{F}_p^\times$ if $p \equiv 1 \pmod 3$

$\simeq \mathbb{F}_{p^2}^\times$ if $p \equiv 2 \pmod 3$

Uniformized by the field $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$

(2) ${}_2F_1\left(\begin{matrix} 2/7 & 3/7 \\ & 1 \end{matrix} ; t\right)$; $k_{\mathfrak{p}}$ = residue field at $\mathfrak{p}$ of $K = \mathbb{Q}(\zeta_7)$

one expects: if $p \equiv 1, 2, 4 \pmod 7$, then $\mathrm{Gal} \simeq k_{\mathfrak{p}}^{\times}$

$p \equiv 3, 5 \pmod 7$, then $\mathrm{Gal} \subset k_{\mathfrak{p}}^{\times}$ order $7 \cdot (p^2 - 1)$

$p \equiv 6 \pmod 7$, then $\mathrm{Gal} \subset k_{\mathfrak{p}}^{\times}$ order $7 (p-1)$

uniformized by the group $(K \cap \mathbb{R})^{\times} \cdot \mu_7(K)$