Testing Algebraic Independence over Finite Fields

Nitin Saxena (IIT Kanpur, India)

(Joint work with Johannes Mittmann, Peter Scheiblechner)

**all pictures are works of others.

2013

Contents

Algebraic independence

- We call polynomials $f_1,\ldots,f_m \in F[x_1,\ldots,x_n]$ algebraically dependent if there is an $A \in F[y_1,\ldots,y_m]$ such that $A(f_1,\ldots,f_m)=0$.
- A is called an annihilating polynomial.
  - Eg. polynomials x_1, x_2^2, $x_1^2+x_2$:
  - They annihilate $A := (y_3 - y_1^2)^2 - y_2$.
- This concept defines the transcendence degree of a set of polynomials.
  - $\mathrm{trdeg}\{f_1,\ldots,f_m\}$ = the maximal number of alg.independent polynomials there.

Alg. independence – Applications

- trdeg generalizes linear-algebra to higher-degree.
- So, it has several known applications in algebraic complexity.
  - [Kalorkoti '85] showed a formula lower bound for *determinant*.
  - It provides a notion of entropy for *polynomial maps* $G: F_p^n \to F_p^n$.
  - [Dvir Gabizon Wigderson '07] used this to construct explicit *extractors*, *condensers* and *dispersers.*
  - [Beecken-Mitmann-S '11, Agrawal-Saha-Saptharishi-S '12] have shown various *identity testing* algorithms.
  - [Forsman '92] gives applications in *control theory*.

Alg. independence – Geometry?

- trdeg is a concept in the center of *commutative algebra*.
- Does it have a *geometric* meaning?
  - Eg. $\mathrm{trdeg}\{x_1, x_1x_2\} = 2$.
  - $\dim F[x_1, x_2] / \langle x_1, x_1x_2\rangle = 1$.
  - $\dim F[x_1, x_1x_2] = 2$.

Krull dimension

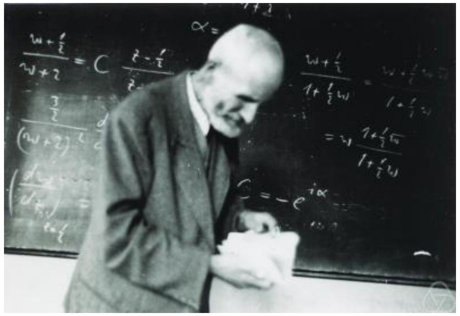
Krull 1899-1971

- trdeg equals the dim of the subset $\{ (f_1(\alpha),\ldots,f_m(\alpha)) \mid \alpha \in F^n \}$, in the m-affine space.

F is alg.closed

Alg. Independence – Bounds

- Given *explicit* polynomials $f_1,\ldots,f_m \in F[x_1,\ldots,x_n]$ of degrees at most d.
- [Perron 1927] The annihilating polynomial degree is at most d^{trdeg}.



Perron 1880-1975

- Thus, using linear-algebra we can produce the annihilating polynomial in PSPACE !

Log of size of system of eqns.

- [Kayal '09] showed that computing the annihilating polynomial is #P hard (*per coefficient*).
- Annihilating polynomial route is hard!

Contents

Jacobian criterion

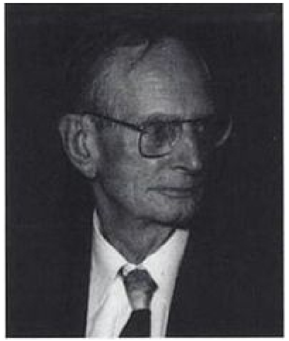
- **Definition:** The $m \times n$ matrix $(\partial_j f_i)_{i,j}$ is called the Jacobian $J_x(f_1,\ldots,f_m)$.
- **Theorem** [Jacobi 1841, BMS'11]: If $char(F)=0$ or $>d^r$ then $rk\, J_x(f_1,\ldots,f_m) = trdeg\{f_1,\ldots,f_m\} =: r$.

  Efficiently computable !
- A *modern* proof is via the de Rham complex.
- Let A be an R-algebra then the de Rham complex is:
  - $\Omega^\bullet_{A/R} : 0 \to A \to \Omega^1_{A/R} \to \Omega^2_{A/R} \to \cdots \to \Omega^i_{A/R} \to \Omega^{i+1}_{A/R} \to \cdots$
  - Each is an R-module.
  - $\Omega^1_{A/R}$ has elements da $(a \in A)$ satisfying $d(ab) = a.db+b.da$.

Kähler differentials module

Leibniz rule

Jacobi 1804-51



de Rham 1903-90

Jacobian criterion – Proof

- Let A be an R-algebra. The de Rham complex is:
  - $\Omega^{\bullet}_{A/R} : 0 \to A=\Omega^0_{A/R} \to \Omega^1_{A/R} \to \Omega^2_{A/R} \to\cdots\to \Omega^i_{A/R} \to \Omega^{i+1}_{A/R} \to\cdots$

- $\Omega^i_{A/R}$ is defined as the i-fold wedge-product $\Lambda^i\, \Omega^1_{A/R}$.
  - Like i-th tensor-product, with extra conditions: $da\wedge db = - db\wedge da$.

- The maps $d: \Omega^i_{A/R} \to \Omega^{i+1}_{A/R}$ in de Rham complex are derivatives.
  - Defined via $d: a.da_1\wedge\cdots\wedge da_i \mapsto da\wedge da_1\wedge\cdots\wedge da_i$.

- Eg. when R is the field F, and A the n-variate polynomial ring:
  - For any polynomial $f\in A$, $df = (\partial_1 f)dx_1 +\ldots+ (\partial_n f)dx_n$.
  - $\Omega^{\bullet}_{A/R}$ is zero beyond $i=n$.
  - $\Omega^n_{A/R}$ is a 1-dim A-module generated by $dx_1\wedge\cdots\wedge dx_n$.

Jacobian criterion – Proof contd.

- Let A be an R-algebra. The de Rham complex is:
  - $\Omega^\bullet_{A/R} : 0 \to A = \Omega^0_{A/R} \to \Omega^1_{A/R} \to \Omega^2_{A/R} \to \cdots \to \Omega^i_{A/R} \to \Omega^{i+1}_{A/R} \to \cdots$
- It is particularly well-behaved as we change
  - R to another R-algebra R'. $\Omega^\bullet_{A/R'} \cong R' \otimes_R \Omega^\bullet_{A/R}$
  - A to a localization B. $\Omega^\bullet_{B/R} \cong B \otimes_A \Omega^\bullet_{A/R}$
  - Field A to a separable algebraic extn. B. $\Omega^\bullet_{B/R} \cong B \otimes_A \Omega^\bullet_{A/R}$
- These neatly prove the Jacobian criterion.
  - *Pf. sketch*: Let $r:=\mathrm{trdeg}\{f_1,\ldots,f_m\}$ & $R:=F$. Wlog let $B:=F(x_1,\ldots,x_n)$ be algebraic over $A:=F(f_1,\ldots,f_r,x_{r+1},\ldots,x_n)$.
  - If $\mathrm{char}(F)=0$ then B/A is a separable algebraic field extension.
  - Thus, $J(f):=df_1\wedge\cdots\wedge df_r$ which is nonzero in $\Omega^r_{A/R}$, remains nonzero in $\Omega^r_{B/R}$.

Is exactly Jacobian matrix condition!

Contents

- Algebraic independence
- Jacobian criterion
- *p-adic Jacobian*
- Witt-Jacobian criterion
- Proof – de Rham-Witt complex
- At the end...

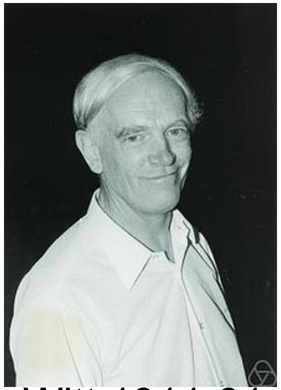
p-adic Jacobian

- Why does the Jacobian *fail*?
  - Eg. $B:=F_p(x) \supset A:=F_p(x^p) \supset R:=F_p$.
  - Here, dx^p is nonzero in $\Omega^1_{A/R}$, but vanishes in $\Omega^1_{B/R}$.
  - Because, B/A is an inseparable algebraic field extension.
- A natural way, to avoid this problem, is to change the characteristic!
  - Instead of F_p move to the p-adic integers – Z_p.
  - Recall, a p-adic integer corresponds to a *formal* series $[a_0] + [a_1]p + [a_2]p^2 + \cdots$, where $a_0, a_1, \ldots \in F_p$.
  - In particular, Z_p has characteristic zero and $Z_p/pZ_p \cong F_p$.

p-adic Jacobian – Witt ring

- We now fix $k=F_p$, for a prime p.

- Construction of p-adic integers was significantly generalized by Witt (1936).
  - For any k-algebra A, there is a $\mathbb{Z}_p$-algebra $W(A)$.



Witt 1911-91

- $W(A)$ is the Witt ring of A.
  - Its elements are $a = [a_0] + [a_1]p + [a_2]p^2 + \cdots$, where $a_0, a_1, \ldots \in A$.
  - The ring morphism $F\colon a \mapsto [a_0^p] + [a_1^p]p + [a_2^p]p^2 + \cdots$. (Frobenius)
  - The additive morphism $V\colon a \mapsto pF^{-1}$. (Verschiebung)

- Thus, any $a \in W(A)$ has the form $a = [a_0] + V[a_1] + V^2[a_2] + \cdots$, where $a_0, a_1, \ldots \in A$. (a is a Witt vector)

p-adic Jacobian – Filtration

- The nice action of V defines a filtration on $W(A)$.
  - $VW(A), V^2W(A), V^3W(A), \ldots$ are ideals of $W(A)$.
  - Further, $W(A) \supset VW(A) \supset V^2W(A) \supset V^3W(A) \supset \cdots$.
- So, the projection of $W(A)$ to the first ℓ coordinates is $W_\ell(A) := W(A) / V^\ell W(A)$.
  - $W_\ell(A)$ is called Witt vectors of A of length ℓ.
  - $W_1(A) = A$.
  - V induces a map $W_\ell(A) \rightarrow W_{\ell+1}(A)$.
- When $A := k[\mathbf{x}]$, $W_\ell(A)$ is explicitly realizable in $C := W(k)[\mathbf{x}\text{^}\{p^{-\infty}\}] := \cup_{i\geq 0} W(k)[\mathbf{x}\text{^}\{p^{-i}\}]$.
  - *Idea:* To realize $F^{-1}, \ldots, F^{-\ell}$ we need $x_1^{1/p}, \ldots, x_1^{1/(p\text{^}\ell)}$.

Frobenius is *not surjective* on the polynomial ring

Realize for finite ℓ, not the Witt vectors of *infinite* length

p-adic Jacobian – Degeneracy

- Fix $k=F_p$ and $A = k[\mathbf{x}]$. Let $\mathbf{f} := \{f_1,\ldots,f_n\} \subset A$.
- Consider their lift $\mathbf{f}' := \{ f_1' ,\ldots, f_n'\} \subset W(k)[\mathbf{x}]$.
  - Whereby, the coefficients have been lifted from $k \twoheadleftarrow W(k)$.
- Consider the p-adic Jacobian polynomial,
  - $J'(\mathbf{f}) := (x_1\cdots x_n)\bullet\det(\partial_j f_i')_{i,j}$.
  - What could be a possible criterion for the alg.independence of $\mathbf{f}$?
- Degeneracy: J' is degenerate if for every $\boldsymbol{\alpha}$, $v_p(\mathrm{coef}(\mathbf{x}^{\boldsymbol{\alpha}})(J')) > v_p(\boldsymbol{\alpha})$.
- Theorem 1: $\mathbf{f}$ are alg.dependent $\Rightarrow$ $J'(\mathbf{f})$ is degenerate.
  - Converse is false ☹
  - Eg. $J'(x_1^p, x_2^p) = p^2 x_1^p x_2^p$.

New notion of *zeroness*

v_p is the p-adic valuation

Contents

- Algebraic independence
- Jacobian criterion
- p-adic Jacobian
- *Witt-Jacobian criterion*
- Proof – de Rham-Witt complex
- At the end...

Witt-Jacobian criterion

- The *correct* version of p-adic Jacobian is Witt-Jacobian, for $\ell \geq 0$,
  - $WJP_{\ell+1}(\mathbf{f}) := (f_1'\cdots f_n')^\wedge\{p^\ell - 1\} \bullet J'(\mathbf{f})$
    $= (f_1'\cdots f_n')^\wedge\{p^\ell - 1\} \bullet (x_1\cdots x_n) \bullet \det(\partial_j f_i')_{i,j}$.
- The Witt-Jacobian criterion is (fix $\ell \geq \log_p \deg(\mathbf{f})$) –

  Theorem 2: $\mathbf{f}$ are alg.dependent ⇔ $WJP_{\ell+1}(\mathbf{f})$ is degenerate.
- Efficiency issues:
  - Degeneracy testing requires computing coefficients of a compactly given polynomial. So, doable in $NP^{\#P} \subseteq PSPACE$.
  - But, is also #P-hard !
- Conjecture: Alg.dependence testing has an efficient algorithm.

Contents

- Algebraic independence
- Jacobian criterion
- p-adic Jacobian
- Witt-Jacobian criterion
- *Proof – de Rham-Witt complex*
- At the end...

Proof – de Rham-Witt Complex

Illusie 1940-

- We prove the Witt-Jacobian criterion using the de Rham-Witt pro-complex of A.

- Essentially, we would like to work with the de Rham complex of the $W_\ell(k)$-algebra $W_\ell(A)$, i.e. $\Omega^\bullet_{W\_\ell(A)\,/\,W\_\ell(k)}$.

- But, we can do better: We can remember the V-filtration of $W_\ell(A)$.
  - This gives us *quotient-modules*, $W_\ell\Omega^\bullet_A$.
- We get the following pro-complex $W_\bullet\Omega^\bullet_A$ (with action of V & derivation d).

- $$\begin{tikzcd}
W_1\Omega^\bullet_A : & 0 \arrow[r] & W_1\Omega^0_A \arrow[r] & W_1\Omega^1_A \arrow[r] & \cdots \arrow[r] & W_1\Omega^i_A \arrow[r] & W_1\Omega^{i+1}_A \arrow[r] & \cdots \\
W_2\Omega^\bullet_A : \arrow[u, leftarrow] \arrow[d] & 0 \arrow[r] & W_2\Omega^0_A \arrow[u, leftarrow] \arrow[r] \arrow[d] & W_2\Omega^1_A \arrow[u, leftarrow] \arrow[r] \arrow[d] & \cdots \arrow[r] & W_2\Omega^i_A \arrow[u, leftarrow] \arrow[r] \arrow[d] & W_2\Omega^{i+1}_A \arrow[u, leftarrow] \arrow[r] \arrow[d] & \cdots \\
{} & & {} & {} & & {} & {} &
\end{tikzcd}$$

Proof – de Rham-Witt Complex

- All that's left is:
  - Show that the pro-complex $W_\bullet\Omega^\bullet_A$ changes in a *natural* way as we vary A.
  - Consider the differential $WJ(\mathbf{f}) := d[f_1] \wedge \cdots \wedge d[f_n]$ in $W_l\Omega^n_A$, for a suitable $l \geq 0$.
  - Show that: $WJ(\mathbf{f})$ vanishes iff $\mathbf{f}$ are alg.dependent.
  - The *explicit form* of $WJ(\mathbf{f})$ using $C = W(k)[\mathbf{x}^\wedge\{p^{-\infty}\}]$ proves the Witt-Jacobian criterion.

Contents

- Algebraic independence
- Jacobian criterion
- p-adic Jacobian
- Witt-Jacobian criterion
- Proof – de Rham-Witt complex
- *At the end...*

At the end …

- We proved the first *nontrivial* criterion for alg.independence over $k=F_p$.
  - Explicitization of the functorial properties of the de Rham-Witt pro-complex of $A=k[\mathbf{x}]$.

- It is not efficient enough. We expect a better criterion to exist.
  - Is there a more *geometric* approach?
  - Is *p-adic analysis* of use?

- Study WJP for really small primes, eg. $p=2$ $(=m=n)$?

Thank you!