CS 829
Polynomial systems: geometry and algorithms
Lecture 7: Putting the pieces together
Éric Schost
eschost@uwo.ca
Main algorithm

Let $F_1, \ldots, F_n$ be in $\mathbb{K}[X_1, \ldots, X_n]$, such that

- for $i = 1, \ldots, n$, $V_i = V(F_1, \ldots, F_i)$ is equidimensional of dimension $n - i$;
- for $i = 1, \ldots, n - 1$, the Jacobian determinant of $F_1, \ldots, F_{i-1}$ has maximal rank on $V_i$ (except maybe on a subvariety of lower dimension).
Main algorithm

Let $F_1, \ldots, F_n$ be in $\mathbb{K}[X_1, \ldots, X_n]$, such that

- for $i = 1, \ldots, n$, $V_i = V(F_1, \ldots, F_i)$ is equidimensional of dimension $n - i$;
- for $i = 1, \ldots, n - 1$, the Jacobian determinant of $F_1, \ldots, F_{i-1}$ has maximal rank on $V_i$ (except maybe on a subvariety of lower dimension).

We will solve the system equation after equation.

- **Preliminary:** apply a generic linear change of coordinates
- **Incremental step:** supposing we have solved $X_1 = x_1, \ldots, X_{n-i} = x_{n-i}, F_1 = \ldots, F_i = 0$ we deduce a solution of $X_1 = x_1, \ldots, X_{n-i-1} = x_{n-i-1}, F_1 = \ldots, F_{i+1} = 0$. 
Initial change of variable

We replace $X_1, \ldots, X_n$ by $Y_1, \ldots, Y_n$ through the change of variables

$$\begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix} = A \begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix},$$

for a random invertible matrix $A$. 
Initial change of variable

We replace $X_1, \ldots, X_n$ by $Y_1, \ldots, Y_n$ through the change of variables

$$
\begin{bmatrix}
X_1 \\
\vdots \\
X_n
\end{bmatrix}
= A
\begin{bmatrix}
Y_1 \\
\vdots \\
Y_n
\end{bmatrix},
$$

for a random invertible matrix $A$.

In the new coordinates:

- the equations become $F_i^A(Y_1, \ldots, Y_n)$;
- a point $\alpha$, after change of variable, is written $\alpha^A$.

The matrix $A$ should be “generic enough”, to ensure several nice geometric properties.
Making the appropriate Jacobian non-zero

Let $J^A$ be the Jacobian determinant of $F_1^A, \ldots, F_i^A$ w.r.t. $Y_{n-i+1}, \ldots, Y_n$.

**Theorem.** For a generic $A$, $J^A$ is identically zero on no component of $V_i$. 
Making the appropriate Jacobian non-zero

Let $J^A$ be the Jacobian determinant of $F_1^A, \ldots, F_i^A$ w.r.t. $Y_{n-i+1}, \ldots, Y_n$.

Theorem. For a generic $A$, $J^A$ is identically zero on no component of $V_i$.

Proof. The Jacobian determinant $J^A$ equals

$$J^A = \det \left( \text{Jac}(F_1, \ldots, F_i) \begin{bmatrix} A_{1,n-i+1} & \cdots & A_{1,n} \\ \vdots & & \vdots \\ A_{n,n-i+1} & \cdots & A_{n,n} \end{bmatrix} \right).$$

Let $(V_{i,j})_{j \leq d_i}$ be the irreducible components of $V_i$. For $j \leq d_i$, there exists a minor $D_{i,j}$ of $\text{Jac}(F_1, \ldots, F_i)$ and a witness point $\alpha_{i,j}$ of $V_{i,j}$ such that

$$\det(D_{i,j})(\alpha_{i,j}) \neq 0.$$

Let $\Delta(A) = \prod_j J^A(\alpha_{i,j}^A)$.

Exercise: $\Delta \neq 0$ and if $\Delta(A) \neq 0$, then OK.
Consequences

Consequence (Jacobian criterion).

When this is the case, for generic $y_1, \ldots, y_i$, the system

$$\{ F_1^A = \cdots = F_i^A = 0, Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i} \}$$

has dimension 0.

In other words, the system $\{ F_1^A = \cdots = F_i^A = 0 \}$ has dimension 0 in $\mathbb{K}(Y_1, \ldots, Y_{n-i})[Y_{n-i+1}, \ldots, Y_n]$. 
Consequences

Consequence (Jacobian criterion). When this is the case, for generic $y_1, \ldots, y_i$, the system

$$\{ Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i}, F_1^A = \cdots = F_i^A = 0 \}$$

has dimension 0. In other words, the system $\{ F_1^A = \cdots = F_i^A = 0 \}$ has dimension 0 in $\mathbb{K}(Y_1, \ldots, Y_{n-i})[Y_{n-i+1}, \ldots, Y_n]$.

Better, all components of $V_i$ have a dense projection on the $Y_1, \ldots, Y_{n-i}$-space.

**Theorem.** For a generic choice of $A$:

- the former system has $\delta_i = \deg(V_i)$ solutions for generic $y$ (and exactly that number when counting multiplicities);
- $Y_{n-i+1}$ is a separating element for that system.

**Proof (not quite easy):** use the definition of degree for point 1. and the Chow form for point 2.
There exist $Q_i, P_{i,n-i+2}, \ldots, P_{i,n}$ in $\mathbb{K}(Y_1, \ldots, Y_{n-i})[Y_{n-i+1}]$ such that
\[
Q_i(Y_{n-i+1}) = 0, \quad Y_{n-i+2} = P_{i,n-i+2}(Y_{n-i+1}), \ldots, \quad Y_n = P_{i,n}(Y_{n-i+1})
\]
describes the solutions of $\{F_{1}^{\mathbf{A}} = \cdots = F_{i}^{\mathbf{A}} = 0\}$ over $\mathbb{K}(Y_1, \ldots, Y_{n-i})$. 
Consequences, continued

There exist $Q_i, P_{i,n-i+2}, \ldots, P_{i,n}$ in $\mathbb{K}(Y_1, \ldots, Y_{n-i})[Y_{n-i+1}]$ such that

$$Q_i(Y_{n-i+1}) = 0, \ Y_{n-i+2} = P_{i,n-i+2}(Y_{n-i+1}), \ldots, \ Y_n = P_{i,n}(Y_{n-i+1})$$

describes the solutions of $\{F_1^A = \cdots = F_i^A = 0\}$ over $\mathbb{K}(Y_1, \ldots, Y_{n-i})$.

Further properties.

- (difficult) $\gcd(Q_i, Q'_i) = 1$,
- for all $j \leq i$, $F_j^A(Y_1, \ldots, Y_{n-i}, Y_{n-1+i}, P_{i,n-1+2}, \ldots, P_{i,n}) = 0 \mod Q_i$,
- the determinant of

$$
\begin{vmatrix}
\frac{\partial F_1^A}{\partial Y_{n-i+1}}(\cdots) & \cdots & \frac{\partial F_1^A}{\partial Y_n}(\cdots) \\
\vdots & \ddots & \vdots \\
\frac{\partial F_i^A}{\partial Y_{n-i+1}}(\cdots) & \cdots & \frac{\partial F_i^A}{\partial Y_n}(\cdots)
\end{vmatrix}
$$

is invertible modulo $Q_i$.  

Degree bounds

Instead of $P_{i,j}$, one can use $S_{i,j}$ such that

$$P_{i,j} = \frac{S_{i,j}}{Q_i'} \mod Q_i \text{ or } S_{i,j} = P_{i,j} Q_i' \mod Q_i.$$
Degree bounds

Instead of $P_{i,j}$, one can use $S_{i,j}$ such that

$$P_{i,j} = \frac{S_{i,j}}{Q'_i} \mod Q_i \quad \text{or} \quad S_{i,j} = P_{i,j} Q'_i \mod Q_i.$$

**Theorem.**

- $Q_i$ is polynomial in $Y_1, \ldots, Y_{n-i}$ and has total degree $\delta_i$.
- The $P_{i,j}$ have degree less than $\delta_i$ in $Y_{n-i+1}$.
- The $S_{i,j}$ are polynomial in $Y_1, \ldots, Y_{n-i}$ and have total degree at most $\delta_i$.
- All denominators in the $P_{i,j}$ divide the discriminant of $Q_i$ and have degree at most $\delta_i^2$. All numerators have degree at most $\delta_i^2$.

**Proof.** Similar the the proof of the height bound from Lecture 2.
Specialization properties

**Theorem** Let $\Gamma_i(Y_1, \ldots, Y_{n-i})$ be the discriminant of $Q_i$ w.r.t. $Y_{n-i+1}$. Then:

- $\Gamma_i \neq 0$,
- if $\Gamma_i(y_1, \ldots, y_{n-i}) \neq 0$, $Q_i(y_1, \ldots, y_{n-i}, Y_{n-i+1})$ remains squarefree, and

\[
Q_i(y_1, \ldots, y_{n-i}, Y_{n-i+1}), \quad Y_{n-i+2} = P_{i,n-i+2}(y_1, \ldots, y_{n-i}, Y_{n-i+1}),
\]

\[
\ldots \quad Y_n = P_{i,n}(y_1, \ldots, y_{n-i}, Y_{n-i+1})
\]

is a univariate representation of the system

\[
\{ F_1^A = \cdots = F_i^A = 0, Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i} \}\]
Specialization properties

**Theorem**  Let $\Gamma_i(Y_1, \ldots, Y_{n-i})$ be the discriminant of $Q_i$ w.r.t. $Y_{n-i+1}$. Then:

- $\Gamma_i \neq 0$,
- if $\Gamma_i(y_1, \ldots, y_{n-i}) \neq 0$, $Q_i(y_1, \ldots, y_{n-i}, Y_{n-i+1})$ remains squarefree, and

\[ Q_i(y_1, \ldots, y_{n-i}, Y_{n-i+1}), \quad Y_{n-i+2} = \frac{S_{i,n-i+2}(y_1, \ldots, y_{n-i}, Y_{n-i+1})}{Q'_i(y_1, \ldots, y_{n-i}, Y_{n-i+1})}, \]
\[ \ldots \quad Y_n = \frac{S_{i,n}(y_1, \ldots, y_{n-i}, Y_{n-i+1})}{Q'_i(y_1, \ldots, y_{n-i}, Y_{n-i+1})} \]

is a univariate representation of the system

\[ \{ F_1^A = \cdots = F_i^A = 0, Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i} \}. \]
Specialization properties

**Theorem** Let \( \Gamma_i(Y_1, \ldots, Y_{n-i}) \) be the discriminant of \( Q_i \) w.r.t. \( Y_{n-i+1} \). Then:

- \( \Gamma_i \neq 0 \),
- if \( \Gamma_i(y_1, \ldots, y_{n-i}) \neq 0 \), \( Q_i(y_1, \ldots, y_{n-i}, Y_{n-i+1}) \) remains squarefree, and

\[
Q_i(y_1, \ldots, y_{n-i}, Y_{n-i+1}), \quad Y_{n-i+2} = \frac{S_i,n-i+2(y_1, \ldots, y_{n-i}, Y_{n-i+1})}{Q_i'(y_1, \ldots, y_{n-i}, Y_{n-i+1})}, \quad \ldots \quad Y_n = \frac{S_i,n(y_1, \ldots, y_{n-i}, Y_{n-i+1})}{Q_i'(y_1, \ldots, y_{n-i}, Y_{n-i+1})}
\]

is a univariate representation of the system

\[
\{ F_1^A = \cdots = F_i^A = 0, Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i} \}.
\]

**Proof.** Easy: this univariate representation gives solutions to the system.

Harder: there are no other solutions.

**Remark.** \( \Gamma_i \) has degree \( \leq \delta_i^2 \leq d^{2n} \).
Specialization properties

Theorem  There exists a non-zero polynomial $\Gamma'_i(Y_1, \ldots, Y_{n-i})$ of degree $\leq nd^{m+1}$ such that if $\Gamma'_i(y_1, \ldots, y_{n-i}) \neq 0$, the Jacobian determinant $J^A$ of

$$F_1^A, \ldots, F_i^A$$

w.r.t. $Y_{n-i+1}, \ldots, Y_n$ vanishes on none of the solutions of the system

$$\{F_1^A = \cdots = F_i^A = 0, Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i}\}.$$
Specialization properties

**Theorem** There exists a non-zero polynomial \( \Gamma'_i(Y_1, \ldots, Y_{n-i}) \) of degree \( \leq nd^{n+1} \) such that if \( \Gamma'_i(y_1, \ldots, y_{n-i}) \neq 0 \), the Jacobian determinant \( J^A \) of

\[
F^A_1, \ldots, F^A_i
\]

w.r.t. \( Y_{n-i+1}, \ldots, Y_n \) vanishes on none of the solutions of the system

\[
\{F^A_1 = \cdots = F^A_i = 0, Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i}\}.
\]

**Proof.** The intersection

\[
V \cap V(J^A)
\]

has dimension less than \( n - i \) and degree at most \( nd\delta_i \leq nd^{n+1} \). The same holds for its projection on the \( Y_1, \ldots, Y_{n-i} \)-space.

**Remark:** I think that \( \Gamma_i \neq 0 \implies \Gamma'_i \neq 0 \). Proof welcome!
Inductive step
Inductive step

**Input:** a univariate description

\[ Q_i(y_1, \ldots, y_{n-i}, Y_{n-i+1}), \quad Y_{n-i+2} = P_{i,n-i+2}(y_1, \ldots, y_{n-i}, Y_{n-i+1}), \]

\[ \ldots \quad Y_n = P_{i,n}(y_1, \ldots, y_{n-i}, Y_{n-i+1}) \]

of the system \( \{ F_1^A = \cdots = F_i^A = 0, Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i} \} \).
Inductive step

Input: a univariate description

\[ Q_i(y_1, \ldots, y_{n-i}, Y_{n-i+1}), \quad Y_{n-i+2} = P_{i,n-i+2}(y_1, \ldots, y_{n-i}, Y_{n-i+1}), \]

\[ \ldots \quad Y_n = P_{i,n}(y_1, \ldots, y_{n-i}, Y_{n-i+1}) \]

of the system \( \{F_1^A = \cdots = F_i^A = 0, Y_1 = y_1, \ldots, Y_{n-i} = y_{n-i}\} \).

Output: a univariate description

\[ Q_{i+1}(y_1, \ldots, y_{n-i-1}, Y_{n-i}), \quad Y_{n-i+1} = P_{i+1,n-i+1}(y_1, \ldots, y_{n-i-1}, Y_{n-i}), \]

\[ \ldots \quad Y_n = P_{i+1,n}(y_1, \ldots, y_{n-i-1}, Y_{n-i}) \]

of the system \( \{F_1^A = \cdots = F_{i+1}^A = 0, Y_1 = y_1, \ldots, Y_{n-i-1} = y_{n-i-1}\} \).
Step 1: lifting

Let $\gamma(Y_{n-i}) = \Gamma \Gamma'(y_1, \ldots, y_{n-i-1}, Y_{n-i})$ and suppose that $\gamma(y_{n-i}) \neq 0$.

- We can apply the lifting algorithm modulo the powers of $<Y_{n-i} - y_{n-i}>$.
- The polynomials $P_{i,j}$ do not have coefficients in $\mathbb{K}[Y_{n-i}]$, but the $S_{i,j}$ do.
- We stop the lifting after reaching degree $\delta_i$ and deduce the $S_{i,j}$. 
Step 1: lifting

Let $\gamma(Y_{n-i}) = \Gamma\Gamma'(y_1, \ldots, y_{n-i-1}, Y_{n-i})$ and suppose that $\gamma(y_{n-i}) \neq 0$.

- We can apply the lifting algorithm modulo the powers of $\langle Y_{n-i} - y_{n-i} \rangle$.
- The polynomials $P_{i,j}$ do not have coefficients in $\mathbb{K}[Y_{n-i}]$, but the $S_{i,j}$ do.
- We stop the lifting after reaching degree $\delta_i$ and deduce the $S_{i,j}$.

Hence, the total cost is

$$O(n^4M(\delta_i) + (n^3 + nL)M(\delta_i)^2)$$

to obtain the parametrization

$$Q_i(y_1, \ldots, Y_{n-i}, Y_{n-i+1}), \quad Y_{n-i+2} = \frac{S_{i,n-i+2}(y_1, \ldots, Y_{n-i}, Y_{n-i+1})}{Q_i'(y_1, \ldots, Y_{n-i}, Y_{n-i+1})},$$

$$\ldots \quad Y_n = \frac{S_{i,n}(y_1, \ldots, Y_{n-i}, Y_{n-i+1})}{Q_i'(y_1, \ldots, Y_{n-i}, Y_{n-i+1})}.$$
Avoiding degenerate points

The solutions of

\[ F_1^A = \cdots = F_i^A = F_{i+1}^A = 0, \Gamma_i \Gamma_i' \neq 0 \]

are the solutions of

\[ Q_i = 0, \quad Y_{n-i+2} = P_{i,n-i+2}, \quad \cdots, \quad Y_n = P_{i,n}, \quad F_{i+1}^A = 0, \Gamma_i \Gamma_i' \neq 0. \]
Avoiding degenerate points

The solutions of

\[ F_1^A = \cdots = F_i^A = F_{i+1}^A = 0, \; \Gamma_i \Gamma'_i \neq 0 \]

are the solutions of

\[ Q_i = 0, \; Y_{n-i+2} = P_{i,n-i+2}, \; \ldots, \; Y_n = P_{i,n}, \; F_{i+1}^A = 0, \; \Gamma_i \Gamma'_i \neq 0. \]

Theorem (not easy). Let

\[ W_i = V(F_1^A, \ldots, F_{i+1}^A, \Gamma_i \Gamma'_i). \]

For a generic matrix \( A \), the projection of \( W_i \) on the \( Y_1, \ldots, Y_{n-i-1} \)-space is contained in \( V(\Lambda_i) \), for some non-zero \( \Lambda_i \) of degree at most \( n^{O(1)} d^{3n} \).

Corollary for a random choice of \( y_1, \ldots, y_{n-i-1} \), we can forget about the constraint \( \Gamma_i \Gamma'_i \neq 0 \). In other words, we can assume that all denominators are non-zero.
Step 2: intersection

Let

\[ F(Y_1, \ldots, Y_{n-i}, Y_{n-i+1}) = F^A_{i+1}(Y_1, \ldots, Y_{n-i+1}, P_{i,n-i+2}, \ldots, P_{i,n}). \]

This is a rational function.
Step 2: intersection

Let

$$F(Y_1, \ldots, Y_{n-i}, Y_{n-i+1}) = F_{i+1}^A(Y_1, \ldots, Y_{n-i+1}, P_{i,n-i+2}, \ldots, P_{i,n}).$$

This is a rational function.

Proposition (not easy). The polynomial $Q_{i+1}$ is given by

$$Q_{i+1} = \text{res}_{Y_{n-i+1}}(F, Q_i).$$

In particular, this resultant

- is in $\mathbb{K}[Y_1, \ldots, Y_{n-i}]$, of degree at most $\delta_{i+1} \leq d\delta_i$,
- has no multiple factor.
Step 2: intersection

Let

\[ F(Y_1, \ldots, Y_{n-i}, Y_{n-i+1}) = F_{i+1}^A(Y_1, \ldots, Y_{n-i+1}, P_i, n-i+2, \ldots, P_{i,n}). \]

This is a rational function.

Proposition (not easy). The polynomial \( Q_{i+1} \) is given by

\[ Q_{i+1} = \text{res}_{Y_{n-i+1}}(F, Q_i). \]

In particular, this resultant

- is in \( \mathbb{K}[Y_1, \ldots, Y_{n-i}] \), of degree at most \( \delta_{i+1} \leq d\delta_i \),
- has no multiple factor.

If \( y_1, \ldots, y_{n-i-1} \) does not cancel \( \Gamma_{i+1} \), then the specialization

\[ Q_{i+1}(y_1, \ldots, y_{n-i-1}, Y_{n-i}) \]

has no multiple factor.
Complexity of the intersection

Preliminaries. We do not compute the

\[ P_{i,j}(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}), \]

which have degrees \( \delta_i^2, \delta_i \). Since the resultant \( Q_{i+1} \) has degree \( \leq d\delta_i \) in \( Y_{n-i} \), it is enough to compute

\[ P_{i,j}(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}) \mod \langle Y_{n-i} - y_{n-i} \rangle^{d\delta_i+1}. \]
Complexity of the intersection

Preliminaries. We do not compute the

\[ P_{i,j}(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}), \]

which have degrees \( \delta_i^2, \delta_i \). Since the resultant \( Q_{i+1} \) has degree \( \leq d\delta_i \) in \( Y_{n-i} \), it is enough to compute

\[ P_{i,j}(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}) \mod (Y_{n-i} - y_{n-i})^{d\delta_i+1}. \]

- Using the extended Euclidean algorithm with coefficients modulo \( Y_{n-i}^{d\delta_i+1} \), the cost is
  \[ O(M(\delta_i)M(d\delta_i) \log(\delta_i)). \]

- This requires that \( (y_1, \ldots, y_{n-i}) \) cancels no leading term in the Euclidean algorithm: need to avoid a hypersurface of degree \( \simeq d^{4n+O(1)}. \)
Complexity of the intersection

Substitution: we use the given straight-line program to evaluate

\[ F(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}, P_{i,n-i+2}, \ldots, P_{i,n}) \mod \langle Q_i, Y_{n-i} - y_{n-i} \rangle^{d\delta_i+1}. \]

Cost: \( O(LM(d\delta_i)M(\delta_i)) \).
Complexity of the intersection

Substitution: we use the given straight-line program to evaluate

\[ F(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}, P_{i,n-i+2}, \ldots, P_{i,n}) \mod \langle Q_i, Y_{n-i} - y_{n-i} \rangle^{d\delta_i+1}. \]

Cost: \( O(LM(d\delta_i)M(\delta_i)) \).

Resultant: we compute the resultant of

\[ F(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}, P_{i,n-i+2}, \ldots, P_{i,n}) \mod \langle Q_i, Y_{n-i} - y_{n-i} \rangle^{d\delta_i+1} \]

and \( Q_i(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}) \). This gives \( Q_{i+1}(y_1, \ldots, y_{n-i-1}, Y_{n-i}) \). We get the parametrization \( S_{i+1,n-i+1}(y_1, \ldots, y_{n-i-1}, Y_{n-i}) \) using the \( \lambda \)-resultant.
Complexity of the intersection

Substitution: we use the given straight-line program to evaluate

\[ F(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}, P_{i,n-i+2}, \ldots, P_{i,n}) \mod \langle Q_i, Y_{n-i} - y_{n-i} \rangle^{d\delta_i+1}. \]

Cost: \( O(LM(d\delta_i)M(\delta_i)) \).

Resultant: we compute the resultant of

\[ F(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}, P_{i,n-i+2}, \ldots, P_{i,n}) \mod \langle Q_i, Y_{n-i} - y_{n-i} \rangle^{d\delta_i+1} \]

and \( Q_i(y_1, \ldots, y_{n-i-1}, Y_{n-i}, Y_{n-i+1}) \). This gives \( Q_{i+1}(y_1, \ldots, y_{n-i-1}, Y_{n-i}) \). We get the parametrization \( S_{i+1,n-i+1}(y_1, \ldots, y_{n-i-1}, Y_{n-i}) \) using the \( \lambda \)-resultant.

Cost: using evaluation / interpolation, \( O(\delta_i M(d\delta_i) \log(d\delta_i)) \).

Remark: the evaluation / interpolation points should not cancel any leading term in the Euclidean remainder sequence.
Summary

The cost of the inductive step is (after simplifying a bit)

\[ O((n^4 + nL)M(\delta_i)M(d\delta_i) \log(d\delta_i)). \]

Hence, the total cost is

\[ O((n^4 + nL)M(\Delta)M(d\Delta) \log(d\Delta)), \]

where \( \Delta = \max \delta_i \).
Summary

The cost of the inductive step is (after simplifying a bit)

\[ O((n^4 + nL)M(\delta_i)M(d\delta_i)\log(d\delta_i)). \]

Hence, the total cost is

\[ O((n^4 + nL)M(\Delta)M(d\Delta)\log(d\Delta)), \]

where \( \Delta = \max \delta_i \).

There are several genericity conditions to be fulfilled:

- the change of variable should be generic enough;
- the points \( y_1, \ldots, y_{n-i} \) should avoid a degeneracy hypersurface;
- additional lucky sample points are needed for the resultant computations.

One can quantify these conditions. If all values are chosen in a finite subset \( S \) of \( \mathbb{K} \), the probability of failure is \( \sim \frac{d^{4n}}{|S|} \).
Bertini’s theorem
Bertini’s theorem

Theorem Suppose that $V(G_1, \ldots, G_s)$ has dimension 0, over a field of characteristic $>(d + 1)^s$. Then a generic linear combination

$$F_i = \lambda_{i,1}G_1 + \cdots + \lambda_{i,s}G_s$$

satisfies the conditions:

- $V_i = V(F_1, \ldots, F_i)$ has dimension $n - i$ for all $i$
- the Jacobian of $F_1, \ldots, F_i$ has maximal rank on $V_i$ for $i < n$. 
Bertini’s theorem

**Theorem** Suppose that $V(G_1, \ldots, G_s)$ has dimension 0, over a field of characteristic $>(d+1)^s$. Then a generic linear combination

$$F_i = \lambda_{i,1}G_1 + \cdots + \lambda_{i,s}G_s$$

satisfies the conditions:

- $V_i = V(F_1, \ldots, F_i)$ has dimension $n - i$ for all $i$
- the Jacobian of $F_1, \ldots, F_i$ has maximal rank on $V_i$ for $i < n$.

**Bonus** If $s = n$ and the Jacobian determinant of $G$ vanishes on none of the solutions, then this is still the case for $F$ (generically).
Modular methods
Modular methods

Let $F_1, \ldots, F_n$ be in $\mathbb{Q}[X_1, \ldots, X_n]$ that satisfy the following conditions (over $\mathbb{Q}$). For all $i$:

- $V_i = V(F_1, \ldots, F_i)$ has dimension $n - i$,
- the Jacobian determinant of $F_1, \ldots, F_i$ has maximal rank on each component of $V_i$.

We will compute the target univariate representation by modular methods:

- do all computations modulo a prime $p$,
- lift the result over $\mathbb{Q}$,
- and use a probabilistic test to stop the lifting.
Good specialization of the system

Theorem. There exists a non-zero integer $A$ such that if $A \mod p \neq 0$, the following holds:

- the Jacobian determinant of $(F \mod p)$ vanishes on no solution of $(F \mod p)$,
- (Jacobian criterion) thus $(F \mod p)$ has dimension zero,
- and the number of solutions of $(F \mod p)$ is $\leq$ the number of solutions of $F$.

Furthermore, one can take $\text{height}(A) \lesssim nhd^n$. 
Good specialization of the system

Theorem. There exists a non-zero integer $A$ such that if $A \mod p \neq 0$, the following holds:

- the Jacobian determinant of $(F \mod p)$ vanishes on no solution of $(F \mod p)$,
- (Jacobian criterion) thus $(F \mod p)$ has dimension zero,
- and the number of solutions of $(F \mod p)$ is $\leq$ the number of solutions of $F$.

Furthermore, one can take $\text{height}(A) \lesssim nhd^n$.

Proof: effective Nullstellensatz. Since the Jacobian is non-zero on all solutions, there exists a non-zero integer $A$ such that

$$A = G_0J + \sum G_iF_i,$$

with all $G_i$ in $\mathbb{Z}[X_1, \ldots, X_n]$. Bounds on the size of $A$ are a difficult theorem.
Good specialization, continued

**Theorem.** There exists a non-zero integer $A'$ such that if $A' \mod p \neq 0$, the following holds:

- The discriminant of $Q$ and all denominators in either $P_1, \ldots, P_n$ or $Q_1, \ldots, Q_n$ are non-zero modulo $p$.

Furthermore, one can take $\text{height}(A') \lesssim nhd^{2n}$.

**Proof:** bounds of the coefficients in Lecture 2.
Good specialization, continued

**Theorem.** There exists a non-zero integer $A'$ such that if $A' \mod p \neq 0$, the following holds:

- The discriminant of $Q$ and all denominators in either $P_1, \ldots, P_n$ or $Q_1, \ldots, Q_n$ are non-zero modulo $p$.

Furthermore, one can take $\text{height}(A') \lesssim nhd^{2n}$.

**Proof:** bounds of the coefficients in Lecture 2.

**Corollary.** When $AA' \mod p \neq 0$, $(Q, P_1, \ldots, P_n \mod p)$ are a univariate representation of the system $(F \mod p)$.

**Proof.** Easy: this describes solutions of the system mod $p$. Harder: this describes all solutions of the system mod $p$. 
Lifting strategy

When \( AA' \mod p \neq 0 \), one can lift \((Q, P_1, \ldots, P_n) \mod p\), to compute either

\[ Q, P_1, \ldots, P_n \mod p^{2^\ell} \quad \text{or rather} \quad Q, S_1, \ldots, S_n \mod p^{2^\ell} \]

for any \( \ell \).
Lifting strategy

When $AA' \mod p \neq 0$, one can lift $(Q, P_1, \ldots, P_n) \mod p$, to compute either

$$Q, P_1, \ldots, P_n \mod p^{2^\ell}$$

or rather

$$Q, S_1, \ldots, S_n \mod p^{2^\ell}$$

for any $\ell$.

However, contrary to what happened before, we do not know what exactly is the height in the output. Two solutions:

- lift until we reach the upper-bound $nhd^m$ on the $S_i$, and deduce the $P_i$ (if needed),

- or use a probabilistic stop criterion:
  - at each lifting step, try a rational reconstruction, to get $(Q^*, P_1^*, \ldots, P_n^*)$ with coefficients in $\mathbb{Q}$,
  - test $(Q^*, P_1^*, \ldots, P_n^*)$ modulo another prime $p'$. 
Lifting and rational reconstruction
Rational reconstruction

Compare the two problems:

- Given $A/B \mod X^\alpha$, with $B(0) \neq 0$, reconstruct $A/B \in \mathbb{K}(X)$.
- Given $a/b \mod p^\alpha$, with $b \mod p \neq 0$, reconstruct $a/b \in \mathbb{Q}$.
Rational reconstruction

Compare the two problems:

- Given $A/B \mod X^\alpha$, with $B(0) \neq 0$, reconstruct $A/B \in \mathbb{K}(X)$.
- Given $a/b \mod p^\alpha$, with $b \mod p \neq 0$, reconstruct $a/b \in \mathbb{Q}$.

Assuming a bound $d$ on the degrees of $A, B$, the first problem can be translated as a linear system in the coefficients of $A$ and $B$. Dimension count suggests to take $\alpha \simeq 2d$.

Suppose a bound $h$ is given on the height of $a, b$. The second problem has no linear algebra interpretation, but counting digits suggests to take $\alpha \simeq 2h/\log(p)$. 
Rational reconstruction

Let $M_Z$ be such that one can multiply integers of size $\ell$ in $M_Z(\ell)$ word operations.

**Theorem.** Suppose that $a/b = c \mod p^\alpha$, with $\log(|a|), \log(|b|) \leq h$, and that $\alpha > 2h/\log(p)$. From $c$, one can compute $a/b$ in $O(M_Z(h) \log(h))$ word operations.

**Remarks**

- The condition means that $\text{height}(p^\alpha) > 2h$.
- The complexity is quasi-optimal.
Rational reconstruction

Let \( M_\mathbb{Z} \) be such that one can multiply integers of size \( \ell \) in \( M_\mathbb{Z}(\ell) \) word operations.

**Theorem.** Suppose that \( a/b = c \mod p^\alpha \), with \( \log(|a|), \log(|b|) \leq h \), and that \( \alpha > 2h/\log(p) \). From \( c \), one can compute \( a/b \) in \( O(M_\mathbb{Z}(h) \log(h)) \) word operations.

**Remarks**

- The condition means that \( \text{height}(p^\alpha) > 2h \).
- The complexity is quasi-optimal.

**Sketch of proof.** Apply the extended GCD algorithm to \( c \) and \( p^\alpha \). One gets a series of Bézout equalities

\[ u_i c + v_i p^\alpha = r_i, \]

so that \( c = r_i/u_i \mod p^\alpha \) (assuming \( u_i \) is a unit).

The \( r_i \) decrease, the \( u_i \) increase, and the sum of their height is always \( \simeq 2h \).

Somewhere in the middle, there are \( u_{i_0} \) and \( r_{i_0} \) of height \( \simeq h \).
Complexity

Recall that:

- the $P_i$ have height $\lesssim nhd^{2n}$,
- the $S_i = P_iQ' \mod Q$ have height $\lesssim nhd^n$.

Hence, at each lifting step, we convert the $P_i \mod p^{2\ell}$ to $S_i \mod p^{2\ell}$ and do rational reconstruction on the latter.
Complexity

Recall that:

- the $P_i$ have height $\lesssim nhd^{2n}$,
- the $S_i = P_i Q'$ mod $Q$ have height $\lesssim nhd^n$.

Hence, at each lifting step, we convert the $P_i$ mod $p^{2^\ell}$ to $S_i$ mod $p^{2^\ell}$ and do rational reconstruction on the latter.

Let $\ell' = 2^\ell \log(p)$. Then, the output size of the $\ell$th lifting step is $n\delta\ell'$ words.

Cost: $O((n^3 + nL)M(\delta)M_\mathbb{Z}(\ell')) + nM(\delta)M_\mathbb{Z}(\ell') + n\delta M_\mathbb{Z}(\ell') \log(\ell'))$.

- $\delta = \deg(Q)$.

- first term: lifting,
- second term: conversion to $S_i$,
- third term: rational reconstruction.
Stop criterion
Stop criterion

Pick a new prime $p'$ and define a procedure $\text{test}(Q^*, S^*_1, \ldots, S^*_n)$, for a candidate resolution with coefficients in $\mathbb{Q}$.

- If $p'$ cancels a denominator or the discriminant of $Q^*$, return $\text{false}$.
- Let $(q^*, p^*_1, \ldots, p^*_n) = (Q^*, S^*_1, \ldots, S^*_n \mod p')$.
- If not all $F_i$ are reduced to zero modulo $(q^*, p^*_1, \ldots, p^*_n)$ and $p'$, return $\text{false}$.
- If the Jacobian determinant is invertible modulo $(q^*, p^*_1, \ldots, p^*_n)$ and $p'$, return $\text{true}$, else return $\text{false}$.
Stop criterion

Pick a new prime \( p' \) and define a procedure \( \text{test}(Q^*, S_1^*, \ldots, S_n^*) \), for a candidate resolution with coefficients in \( \mathbb{Q} \).

- If \( p' \) cancels a denominator or the discriminant of \( Q^* \), return \text{false}.
- Let \((q^*, p_1^*, \ldots, p_n^*) = (Q^*, S_1^*, \ldots, S_n^* \mod p')\).
- If not all \( F_i \) are reduced to zero modulo \((q^*, p_1^*, \ldots, p_n^*)\) and \( p' \), return \text{false}.
- If the Jacobian determinant is invertible modulo \((q^*, p_1^*, \ldots, p_n^*)\) and \( p' \), return \text{true}, else return \text{false}.

\textbf{Theorem.} If \( AA' \mod p' \neq 0 \), then \( \text{test}(Q^*, S_1^*, \ldots, S_n^*) \) outputs \text{true} if and only if

\[ (Q^*, S_1^*, \ldots, S_n^*) = (Q, S_1, \ldots, S_n) \mod p'. \]

\textbf{Proof:} easy consequence of the definitions of \( A, A' \).

\textbf{Cost:} similar to that of the first lifting step.
Possible failures

Let $p, p'$ be such that $AA' \mod p \neq 0$ and $AA' \mod p' \neq 0$.

- If we let the lifting process run, it will eventually correctly reconstruct $Q, P_1, \ldots, P_n$, and test will then output true.
- The possibility of failure is that we stop too early.
Possible failures

Let $p, p'$ be such that $AA' \mod p \neq 0$ and $AA' \mod p' \neq 0$.

- If we let the lifting process run, it will eventually correctly reconstruct $Q, P_1, \ldots, P_n$, and test will then output true.

- The possibility of failure is that we stop too early.

Suppose that at step $\ell$ we have reconstructed $(Q^*, S_1^*, \ldots, S_n^*)$ with rational coefficients. The risk is that

$$(Q^*, S_1^*, \ldots, S_n^*) = (Q, S_1, \ldots, S_n) \mod p',$$

whereas they are actually different over $\mathbb{Q}$.

The coefficients $(Q^*, S_1^*, \ldots, S_n^*)$ of have height $2^\ell$; those of $(Q, S_1, \ldots, S_n)$ have height $\simeq nhd^n$.

Hence, there exists an integer $B_\ell$ of height $\simeq 2^\ell + nhd^n$ such that, if $B_\ell \mod p' \neq 0$, the reductions mod $p'$ differ, and we do not stop at step $\ell$. 
Possible failures

Let $\ell_{\text{max}}$ be the number of lifting steps to do before we can reconstruct $Q, P_1, \ldots, P_n$. Using the bounds on the output size, we get

$$\ell_{\text{max}} \leq \log(nhd^n).$$

Hence, there is a non-zero integer $M(p) = A A' B_1 \cdots B_{\ell_{\text{max}}}$ such that if

- $p$ does not divide $A A'$,
- $p'$ does not divide $M(p)$,

the whole lifting process works correctly.

The height of $M(p)$ is $\simeq nhd^{2n} \log(nhd^n)$ (rough upper bound).
Counting probabilities
Probabilistic arguments

Compare the two statements:

• There exists a non-zero polynomial \( P(E_1, \ldots, E_r) \) of degree \( \leq \cdots \) such that if \( P(e_1, \ldots, e_r) \neq 0 \), algorithm \( X \) succeeds.

  Remark: \( P(e_1, \ldots, e_r) = P \mod \langle E_1 - e_1, \ldots, E_r - e_r \rangle \).

• There exists a non-zero integer \( M \) of height \( \leq \cdots \) such that if \( (M \mod p) \neq 0 \), algorithm \( Y \) succeeds.
Probabilistic arguments

Compare the two statements:

• There exists a non-zero polynomial $P(E_1, \ldots, E_r)$ of degree $\leq \cdots$ such that if $P(e_1, \ldots, e_r) \neq 0$, algorithm $X$ succeeds.
  
  **Remark:** $P(e_1, \ldots, e_r) = P \mod \langle E_1 - e_1, \ldots, E_r - e_r \rangle$.

• There exists a non-zero integer $M$ of height $\leq \cdots$ such that if $(M \mod p) \neq 0$, algorithm $Y$ succeeds.

In both cases, we expect that for a random choice of $e_1, \ldots, e_r$ (resp. of $p$), we should have a large probability of success.

• In the first case, this is controlled by Zippel-Schwartz’ result.

• In the second, we are going to use number theory.
Let $B$ be an integer (which will control the probability of failure). We will pick our primes in $\Gamma = [B, \ldots, 2B]$.

**Theorem.** The cardinality of $\Gamma$ is at least $\frac{B}{2 \log(B)}$.

**Proof:** hard.

**Proposition.** There are at most $\frac{\log(M)}{\log(B)}$ primes in $\Gamma$ that divide $M$.

**Proof:** The product of these primes divides $M$. 

Arithmetic Zippel-Schwartz
Arithmetic Zippel-Schwartz

Let $B$ be an integer (which will control the probability of failure). We will pick our primes in $\Gamma = [B, \ldots, 2B]$.

**Theorem.** The cardinality of $\Gamma$ is at least $\frac{B}{2 \log(B)}$.

**Proof:** hard.

**Proposition.** There are at most $\frac{\log(M)}{\log(B)}$ primes in $\Gamma$ that divide $M$.

**Proof:** The product of these primes divides $M$.

**Corollary.** Suppose you can pick primes at random in $\Gamma$. Then the probability of finding one that divides $M$ is at most $\frac{2 \log(M)}{B}$.

**Corollary.** Choosing $B \simeq 4 \log(M) = 4 \text{height}(M)$ gives $\simeq 50\%$ probability of success.

Our situation is slightly more involved (we have $p$ and $p'$). However, similar bounds $B \simeq nhd^{2n} \log(nhd^{2n})$ give $\simeq 50\%$ probability of success.
Overall complexity

1. Solving the system mod $p$.

The resolution mod $p$ is probabilistic. Hence, we have new constraint $p \gtrsim d^{4n}$ to get a probability of success of order 50%. Complexity:

$$O((n^4 + nL)M(\Delta)M(d\Delta)\log(d\Delta)M_\mathbb{Z}(n \log(d) + \log(h) + \cdots))$$

word operations, where $\Delta = \max \delta_i$.

- **blue term**: number of operations mod $p$,
- **red term**: cost of computations mod $p$. 
Overall complexity

2. Lifting over $\mathbb{Q}$.

We have seen that $p, p' \gtrsim nhd^{2n}$ is enough to get 50% probability of success. Complexity:

$$O((n^4 + nL)M(\delta)M_\mathbb{Z}(H) \log(H))$$

word operations (a little bit oversimplified), where $H$ is the height of the polynomials $S_1, \ldots, S_n$ and $\delta = \delta_n = \text{deg}(Q)$. 
Overall complexity

2. Lifting over \( \mathbb{Q} \).

We have seen that \( p, p' \gtrsim nhd^{2n} \) is enough to get 50% probability of success. Complexity:

\[
O((n^4 + nL)M(\delta)M_{\mathbb{Z}}(H) \log(H))
\]

word operations (a little bit oversimplified), where \( H \) is the height of the polynomials \( S_1, \ldots, S_n \) and \( \delta = \delta_n = \deg(Q) \).

3. Worst case.

Putting things at worst, all \( \delta_i \) are \( \leq d^i \), \( H \) is \( \leq nhd^n \), so we get a cost of

\[
O(Lhd^{2n+1})
\]

up to logarithmic factors.
Extras
Lifting fibers

In the previous algorithms, we used a description of the positive-dimensional varieties

\[ V_i = \{F_1 = \cdots = F_i = 0\} \]

by means of zero-dimensional ones

\[ F_1 = \cdots = F_i = 0, \ Y_1 = y_1, \ldots, \ Y_{n-i} = y_{n-i} \quad (\ast) \]

Using Newton iteration, one can recover a (generic) description of \( V_i \) from the solutions of (\ast), assuming the Jacobian determinant of \( F_1, \ldots, F_i \) vanishes nowhere on them.

- A system such as (\ast), together with a univariate representation for it, is called a \textit{lifting fiber} for \( F_1, \ldots, F_i \).
- Lifting fibers can be used to describe positive-dimensional varieties.
The most general version (Lecerf)

• Let $F_1, \ldots, F_s$ be polynomials over a field $\mathbb{K}$ of large enough characteristic.

• Let $V = V(F_1, \ldots, F_s)$ and write its equidimensional decomposition

$$ V = V_0 \cup V_1 \cup \cdots \cup V_r. $$

One can compute a family of lifting fibers $L F_0, \ldots, L F_r$ for $V_0, \ldots, V_r$ by an algorithm that extends the previous one.

Difficult points: one needs to handle

• splittings (when intersections are not proper)

• multiple components (some Jacobian determinants are added to the system).

The cost is polynomial in $L, s$ and some algebraic degree (that counts multiplicities).