

# From essential to canonical dimension: An overview

(Bielefeld, February 2005)

## §1 Tschirnhaus transformations

Let  $k$  be a field,  $K/k$  be any field extension.

Two polynomials  $f, g \in K[X]$  are said to be Tschirnhaus equivalent

if there is  $K$ -algebra isomorphism  $K[X]/\langle f \rangle \xrightarrow{\varphi} K[X]/\langle g \rangle$

Such a  $\varphi$  is called a non-degenerate Tschirnhaus transform.

If  $f = X^n + a_{n-1}X^{n-1} + \dots + a_0$  and if  $x$  denotes the class of  $X$

$\varphi$  is uniquely determined by the image of  $x$  which has the form

$$y(x) = r_0 + r_1 x + \dots + r_{n-1} x^{n-1}$$

and satisfies  $f(y(x)) = 0$

Given  $f$  of degree  $n$  we would like to compute the minimal number of algebraically independent coefficients of  $f$  up to Tschirnhaus transformation

examples:  $n=2$   $f = X^2 + ax + b$   $\xrightarrow{\varphi_1}$   $g = X^2 + c$   $c = b - \frac{a^2}{4}$   
 $\uparrow$   $\varphi(x) = x - \frac{a}{2}$   $\uparrow$   
 2 parameters if  $\text{char}(k) \neq 2$  1 parameter

$n=3$   $f = X^3 + ax^2 + bx + c$   $\xrightarrow{\varphi_1}$   $g = X^3 + b'x + c'$   $\xrightarrow{\varphi_2}$   $h = X^3 + dx + d$   
 $\uparrow$   $\varphi_1(x) = \frac{c'}{b'}x$   $\uparrow$   
 3 parameters if  $\text{char}(k) \neq 3$  if  $cb' \neq 0$  1

$n=4$   $f \xrightarrow{\varphi_1}$   $X^4 + b'x^2 + c'x + d$   $\xrightarrow{\varphi_2}$   $X^4 + ax^2 + bx + b$   
 $\uparrow$   $\varphi_2(x) = \frac{c'}{b'}x$   $\uparrow$   
 4 parameters if  $\text{char}(k) \neq 2$  2 parameters and not 1 in general

All cases are recovered by the general polynomial of degree  $n$

$$f_{\text{gen}}^{(n)} = X^n + a_1 X^{n-1} + \dots + a_n$$

where the  $a_i$  are algebraically independent variables over  $k$ .

The minimal number of alg coefficients of  $f_{\text{gen}}^{(n)}$  up to Tschirnhaus Transformation will be denoted by  $d_k(n)$

$$\text{char } k = 0$$

$$d_k(2) = d_k(3) = 1$$

$$d_k(4) = 2$$

- Hermite in 1861 shows that  $f_{\text{gen}}(5)$  can be brought to the form  $x^5 + ax^3 + bx + b$

$$\text{and thus } d_k(5) \leq 2$$

- Klein showed in 1884 that  $d_k(5) \neq 1$  which he called the "Kronecker's Theorem"

$$\Rightarrow d_k(5) = 2$$

- Joubert in 1867 shows that  $f_{\text{gen}}(6)$  can be brought to the form  $t^6 + at^4 + bt^2 + ct + c$

$$\Rightarrow d_k(6) \leq 3$$

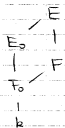
Questions: behaviour of  $d_k(n)$ , bounds?

## §2 Butler and Reichstein's approach (1995)

$$\text{char}(k) = 0$$

Def. Let  $E/F$  be a field extension of degree  $n$  and  $F_0 \subset F$ .  $E/F$  is said to be defined over  $F_0$ , if  $\exists$  an extension  $E_0/F_0$  of degree  $n$ , contained in  $E$ , such that  $E_0 F = E$ .

picture:



the essential dimension of  $E/F$ ,

denoted by  $\text{ed}_k(E/F)$ ,

is the minimal value of  $\text{trdeg}(F_0/k)$

where  $F_0$  ranges over the subfield over which  $E/F$  is defined.

Now take  $f_{\text{gen}}(n) = x^n + a_1 x^{n-1} + \dots + a_n$  be the generic polynomial of deg  $n$

let  $F_n = k(a_1, \dots, a_n)$  and  $E_n = F_n[X] / \langle f_{\text{gen}}(n) \rangle$

then  $\text{ed}(E_n/F_n) = d_k(n)$  (exercise)

Lemma 1: If  $E/F$  is a Galois extension with group  $G$   
 Then  $\exists F_1 \subset F$  and a Galois extension  $E_1/F_1$  with group  $G$   
 such that  $\text{trdeg}(F_1/k) = \text{ed}(E/F)$

Lemma 2: Let  $E/F$  be an extension of degree  $n$  and let  $E^\#$  be the normal closure of  $E$  over  $F$ . Then  $\text{ed}(E/F) = \text{ed}(E^\#/F)$ .

Let  $X_1, \dots, X_n$  be the roots of the generic polynomial  $f_{\text{gen}}(x)$

$$\text{then } F_n = k(a_1, \dots, a_n) = k(X_1, \dots, X_n)^{S_n}$$

and 
$$E_n = F_n[X] / \langle f_{\text{gen}}(X) \rangle \cong F_n(X_1) = k(X_1, \dots, X_n)^{S_n}(X_1)$$

but  $E_n^\# = k(X_1, \dots, X_n)$

$$\begin{aligned} \text{so } d_k(n) &= \text{ed}_k(E_n/F_n) = \text{ed}_k(E_n^\#/F_n) \\ &= \text{ed}_k(k(X_1, \dots, X_n) / k(X_1, \dots, X_n)^{S_n}) \end{aligned}$$

(Now comes the geometric approach)

$\hookrightarrow$  Galois extension  
with group  $S_n$

$G$  finite group,  $X$  a  $G$ -variety, that is an irreducible algebraic variety over  $k$ , together with a map of varieties  $G \times X \rightarrow X$ . A  $G$ -variety  $X$  is called faithful if  $G \rightarrow \text{Aut}(X)$  is injective

Definition: Let  $X$  be a faithful  $G$ -variety. The essential dimension of  $X$  is the minimal dimension of a faithful  $G$ -variety  $Y$  such that there exists a  $G$ -companion  $X \dashrightarrow Y$  that is a dominant  $G$ -equivariant rational morphism. This is denoted by  $\text{ed}_k(X)$

if  $X$  is a vector space the variety is called linear  $G \rightarrow GL(X)$

emphasis on linear faithful representation

Lemma 3: Let  $X$  be a faithful  $G$ -variety, let  $E = k(X)$  = rational functions  
 and  $F = E^G$  =  $G$ -invariant rational functions  
 Then  $ed_k(X) = ed_k(E/F)$

Thm - Definition: Let  $X$  be a faithful  $G$ -variety and  $V$  be any  
 faithful linear representation of  $G$ . Then

$$ed_k(X) \leq ed_k(V)$$

In particular  $ed_k(V) = ed_k(V)^G$  for all faithful linear representation  $V$

The number  $ed_k(V)$  is called the essential dimension of  $G$  and denoted by  $ed_k(G)$

example  $d_k(n) = ed_k(k(x_1, \dots, x_n) / k(x_1, \dots, x_n)^{S_n})$

$$= ed_k(k(V) / k(V)^{S_n}) = ed_k(V) = ed_k(S_n)$$

$\uparrow$   
 $V = A^n$  the affine  $n$ -space

Remark: if  $H \leq G$  then  $ed_k(H) \leq ed_k(G)$

Corollary:  $d_k(n) \leq d_k(n+1)$

proof:  $S_n \leq S_{n+1} \neq$

Known facts: if  $k$  contains a primitive  $p^{\text{th}}$ -root of unity, then

$$ed_k(\underbrace{\mathbb{Z}/p \times \dots \times \mathbb{Z}/p}_{r \text{ times}}) = r$$

Corollary:  $ed_k(S_n) \geq \lfloor \frac{n}{2} \rfloor$

proof:  $\underbrace{\mathbb{Z}/2 \times \dots \times \mathbb{Z}/2}_{\lfloor \frac{n}{2} \rfloor \text{ times}} \leq S_n \neq$

very little is known  
 on  $ed_k(G)$   
 for finite groups

other result:  $ed_k(S_n) \leq n-3 \quad \forall n \geq 5$

$$\Rightarrow d_k(4) = d_k(5) = 2 \quad d_k(6) = 3$$

still unknown  
 $d_k(7) = \begin{cases} 3 \\ 4 \end{cases}$

### §3 Reichstein's generalization

$k$  algebraically closed of char 0,  $G$  algebraic group over  $k$ .

A  $G$ -variety  $X$  is called generically free if  $G$  acts freely (with trivial stabilizers) on a dense open subset of  $X$  (here  $X$  is not necessarily irreducible)

def: Let  $X$  be a generically free  $G$ -variety. A  $G$ -compression of  $X$  is a dominant  $G$ -equivariant rational map  $X \dashrightarrow X'$  where  $X'$  is another generically free  $G$ -variety.

$$ed_k(X) \stackrel{\text{def}}{=} \min \{ \dim X' - \dim G \}$$

where the min is taken over all  $G$ -compressions  $X \dashrightarrow X'$

Thm: same as for  $G$  finite but replace faithful by generically free

Known facts: 1)  $ed_k(G \times H) \leq ed_k(G) + ed_k(H)$

2)  $ed_k(H) + \dim H \leq ed_k(G) + \dim G$  if  $H$  closed subgroup of  $G$

3)  $ed_k(SL_n) = ed_k(SL_n) = 0$   
 $ed_k(G_m^r) = 0$  } more generally:  $ed(G) = 0 \iff H^1(k, G) = 0$   
 $\checkmark k$

4)  $ed_k(O_n) = n$      $ed_k(SO_n) = n-1 \quad \forall n \geq 2$  ( $ed_k(SO_2) = 0$ )

$ed_k(PGL_n) \leq n^2 - 2n \quad \forall n \geq 4$

$ed_k(PGL_n) \geq 2^r$  for any  $n \geq 2^r \quad r \geq 1$

$ed(PGL_n) = 2$  if  $n = 2, 3, 6$

if  $n_1, n_2$  are relatively primes then

-  $ed(PGL_{n_1}) \leq ed(PGL_{n_1, n_2})$

-  $ed(PGL_{n_1, n_2}) \leq ed(PGL_{n_1}) + ed(PGL_{n_2})$

-  $ed(G_2) = 3$

$ed(PO_n) \geq n-1$

-  $ed(F_4) = 5$

-  $9 \leq ed(E_8)$

-  $20 \leq \dots$

## §4 Merkurjev's functional point of view

Let  $k$  be any field, denote by  $\mathcal{C}_k$  the category of all field extensions of  $k$

Definition: Let  $F: \mathcal{C}_k \rightarrow \text{Sets}$  be a covariant functor

For  $K/k$  and  $a \in F(K)$  we write  $\text{ed}(a) \leq n$  if there exists  $E \in \mathcal{C}_k$  such that

i)  $a \in \text{im}(F(E) \rightarrow F(K))$

ii)  $\text{trdeg}(E/k) = n$

Of course  $\text{ed}(a) = n$  if  $\text{ed}(a) \leq n$  and  $\text{ed}(a) \not\leq n-1$

We put  $\text{ed}_k(F) = \sup_{K/k} \{ \text{ed}(a) \mid a \in F(K) \} \in \mathbb{N} \cup \{\infty\}$

### example of functors

1) Let  $X$  be a  $k$ -scheme. It defines a functor  $X: \mathcal{C}_k \rightarrow \text{Sets}$

by setting  $X(K) = \text{Hom}(\text{Spec } K, X) = K\text{-rational points of } X$

2) More generally let  $X$  be a  $k$ -scheme and  $G$  be a  $k$ -group-scheme acting on  $X$ . We have an orbit functor denoted by  $X/G: \mathcal{C}_k \rightarrow \text{Sets}$

$$K \mapsto X(K)/G(K)$$

3) Let  $G$  be a group-scheme of finite type, then we have the Galois cohomology functor  $K \mapsto H^1(K, G)$

$$\text{ed}_k(H^1(-, G)) \stackrel{\text{rot}}{=} \text{ed}_k(G)$$

advantages: -  $k$  any field

- easier statements

- compare functors

-  $F \supseteq G \Rightarrow \text{ed}(F) = \text{ed}(G)$

$$\text{ed}(F \times G) \leq \text{ed}(F) + \text{ed}(G)$$

Known facts:  $\text{ed}_k(X) = \dim X$

= if  $F \rightarrow G$  is a surjective morphism (i.e.  $F(K) \rightarrow G(K) \forall K/k$ )

$$\text{then } \text{ed}_k(G) \leq \text{ed}_k(F)$$

- cohomological invariants

Corollary:  $\text{ed}_k(O_n) \leq n$

proof:  $H^1(K, O_n) \leftrightarrow$  isomorphism classes of non-degenerate quadratic forms of rank  $n$  over  $K$   $\stackrel{\text{not}}{=} Q_n(K)$

$$\begin{array}{ccc} \text{variety of} & \rightarrow & G_m \times \dots \times G_m \longrightarrow Q_n \\ \text{dimension } n & & (a_1, \dots, a_n) \longmapsto \langle a_1, \dots, a_n \rangle \end{array}$$

$$\text{ed}_k(Z/4) = \begin{cases} 1 & \text{if } -1 = \square \text{ mod char } \neq 2 \\ 2 & \text{otherwise} \end{cases}$$

$$\text{ed}_k(S^1) = \begin{cases} 0 & \text{if } -1 = \square \text{ mod char } \neq 2 \\ 1 & \text{otherwise} \end{cases}$$

$$\text{ed}_k(G) = \text{ed}_{k(t)}(G) \text{ for any infinite field } k$$

Special case of  $\text{ed}(X/G) \leftarrow$  hard in general

$X_{d,n}$  = projective space of homogeneous polynomial of degree  $d$  in  $n$  variables  $\simeq \mathbb{P}^{m-1}$

$$G = \text{PGL}_n$$

$$F_{d,n} = X_{d,n} / \text{PGL}_n$$

$$\text{where } m = \binom{d+n-1}{n-1}$$

$$F_{3,n} = \text{Cub}_n$$

Thm: if char  $\neq 2, 3$  then

(2003)

$$\text{ed}_k(\text{Cub}_3) = 3$$

to coefficients

+ other results

## § 5 canonical dimension (geometric)

We look closer at  $\text{ed}_k(X/E)$

let  $\bar{x} \in X(L)$  a  $L$ -rational point  $\alpha: \text{Spec } L \rightarrow X$

and take  $Y$  a  $k$ -model of  $L$  ( $k$ -scheme such that  $k(Y) \cong L$ )

$\alpha$  induces a rational morphism  $\varphi_{\alpha}: Y \dashrightarrow X$  (and universal)

In the same way  $g \in E(L)$  induces  $\varphi_g: Y \dashrightarrow G$

and  $g \cdot \alpha \in X(L)$  is given by

$$F_{g,\alpha}: Y \dashrightarrow G \times X \xrightarrow{\cdot} X \\ y \mapsto (\varphi_g(y), \varphi_{\alpha}(y))$$

So to find  $g \in E(L)$  such that  $g \cdot \alpha$  is defined over a minimal extension (for today) is the same as to find  $\varphi_g: Y \dashrightarrow G$

such that  $\dim(F_{g,\alpha}(Y))$  is minimal (exercise)

$$\text{ed}([\alpha]) = \min_{g \in E(L)} \{ \dim F_{g,\alpha}(Y) \}$$

If  $X$  is irreducible, take  $\alpha = \text{pt}$  the generic point of  $X$

$$Y = X \quad \varphi_{\alpha} = \text{id}_X: X \dashrightarrow X$$

$$f = \varphi_g: X \dashrightarrow G$$

$$F: X \dashrightarrow X \quad \leftarrow \text{canonical form map} \\ \alpha \mapsto f(\alpha) = \alpha$$

$$\text{ed}([f]) = \min_{f: X \dashrightarrow G} \{ \dim F(X) \}$$



Berthy-Reichstein definition (2004)

$\text{char } k = 0 \quad \bar{k} = k$

$$\text{cd}(X, G) = \min_{\substack{F \text{ rational} \\ \text{form map}}} \{ \dim F(X) - \dim X + \dim G \}$$

remembers  $F: X \dashrightarrow X$  is canonical if it is of the form  $x \mapsto f(x) \cdot x$   
where  $f: X \dashrightarrow G$ .

When  $X$  is generically free  $F: X \dashrightarrow X$  is canonical  
iff it commutes with the rational quotient map  $X \xrightarrow{\pi} X/G$

Prop if  $V$  is a generically free linear representation of  $G$   
def and  $X$  is any generically free  $G$ -variety then  $\text{cd}(X, G) \leq \text{cd}(V, G)$   
 $\text{cd}(G) = \text{cd}(V, G)$  for some  $V$  generically free =  $\max_{\substack{X \text{ gen free} \\ G\text{-variety}}} \text{cd}(X, G)$

back to  $\text{ed}(F_{d,n}) = \text{ed}(\mathbb{P}^{m-1}/\text{PGL}_n)$ :

$$\begin{aligned} \text{cd}(F_{d,n}) &\geq \text{ed}([n]) = \text{cd}(\mathbb{P}^{m-1}, \text{PGL}_n) + \dim \mathbb{P}^{m-1} - \dim \text{PGL}_n \\ &= \text{cd}(\mathbb{P}^{m-1}, \text{PGL}_n) + m-1 - n^2 + 1 \\ &= \text{cd}(\mathbb{P}^{m-1}, \text{PGL}_n) + m - n^2 && \text{ed}(F_{d,n}) \geq \text{ed}([n]) \\ &= \text{cd}(A^m, G_m \times G_n) + m - n^2 && \text{but don't know how} \\ &\uparrow && \text{to prove the equality} \\ \text{lemma} &&& \end{aligned}$$

$$\begin{aligned} \text{for } \text{gcd}(n, d) &\rightsquigarrow \det \\ (n, d) &= \text{cd}(G_m \times G_n) + m - n^2 \\ &= \text{cd}(G_n/\mu_d) + m - n^2 \\ &\uparrow \\ \text{lemma} & \end{aligned}$$

known: special iff  $\text{gcd}(n, d) = 1$

$$\text{cd}(G) = \text{cd}(G^0), \text{cd}(G) = 0 \text{ iff } G^0 \text{ is special}$$

Rajwenter

## § 6 Canonical dimension (functional)

If  $X$  is a generically free  $G$ -variety the rational quotient map may be viewed as a  $G$ -torsor or principal homogeneous space over  $G$

$$\begin{array}{ccc}
 T & \longrightarrow & X \\
 \text{generic fiber} \rightsquigarrow \downarrow & & \downarrow \\
 \text{Spec } k(X/G) & \longrightarrow & X/G
 \end{array}
 \quad k(X/G) = k(X)^G = K$$

$X$  defines an element  $\alpha \in H^1(K, G)$

Lemma: For any canonical form map  $F: X \dashrightarrow X$  the following are equivalent

i)  $\alpha_E = 1_E \in H^1(E, G) \quad (K \subseteq E)$

ii)  $F(X)$  has a  $E$ -rational point

in particular  $k(F(X)) = E \iff \alpha_{k(F(X))}$  is a splitting field

One can show that  $k(F(X))$  is a generic splitting field for  $\alpha$

So that  $cd(X, G) = \min \text{trdeg}(L:K) \quad K = k(X)^G$

where  $L$  runs through the generic splitting fields for  $\alpha$

This leads to the following generalisation:

let  $F: \mathcal{C}_k \rightarrow \text{Sets}^*$  be a covariant functor  
with values in the category of pointed sets

let  $K/k$  and  $a \in F(K)$ . A splitting field for  $a$   
is an extension  $L/k$  such that  $a_L = * \in F(L)$

A splitting field  $E/k$  is called generic for  $a$  if  $\forall L/k$  splitting field  
there exists a  $k$ -place  $\psi: E \rightarrow L$

The canonical dimension of  $a$ ,  $cd(a)$ , is the min of  $\text{trdeg}(E:k)$   
for all generic splitting fields  $E/k$  of  $a$ .

$$cd(F) = \sup_{L/k} \{cd(a) \mid a \in F(L)\}$$

$$cd(G) = cd(H^1(-, G)) \quad \text{by our considerations}$$

This is helpful for computations and it generalizes to  $k$  arbitrary

Aim: Study more carefully what happens for neighborhoods of functors  $F \rightarrow G$

Recently Karpenko and Merkurjev gave another functional approach  
which generalises this one. They compute  $cd(G)$   
for a large class of algebraic groups using Chow theory.