Quadrics over function fields in one (and more) variable(s) over a $\mathfrak{p}$-adic field

J.-L. Colliot-Thélène
CNRS, Université Paris-Sud, z.Z. HIM

Hausdorff Institut für Mathematik
Trimester zum Thema Diophantische Gleichungen
Endtagung, 23. bis 29. April 2009

Theorem (Parimala and Suresh 2007)

Let K be a $\mathfrak{p}$-adic field, $p = char(\mathbb{F}) \neq 2$. Let F be a function field in one variable over K. A quadratic form in $n > 8$ variables over F has a nontrivial zero.

$n > 8$ best possible

natural conjecture by analogy to $K = \mathbb{F}((t))$

There is also a natural conjecture for function fields in s variables over K.

History, up to April 2009

Before 1987 : not even known if isotropy for $n > n_0$

$n > 26$ Merkurjev preprint1997 (use of Merkurjev 1982 and Saltman 1997)

$n > 22$ Hoffmann and van Geel 1998 (use of Merkurjev 1982 and Saltman 1997)

$n > 10$ Parimala and Suresh 1998 (use of Kato's results in higher class field theory)

$n > 8$ Parimala and Suresh preprint2007 (use of recent results by Saltman on algebras of prime index)

Other methods giving $n > 8$

T. Wooley. New circle method, announced 2007; should also say something for $n \geq 5$; should give results for (diagonal) *forms of arbitrary degree*.

D. Harbater, J. Hartmann, D. Krashen preprint2008 (patching techniques); CT, Parimala, Suresh preprint2008 (builds upon HHK; new results for $n \leq 8$). Method gives results for *homogeneous spaces of rational linear algebraic groups*

D. Leep April 2009. Use of results by Heath-Brown; gives results for quadrics over *higher dimensional function fields over* K and for any prime p (also $p = 2$).

I. The cohomological method

Merkurjev
Hoffmann-van Geel
Parimala-Suresh 1
Parimala-Suresh 2

Let k be a field, $char(k) \neq 2$. In 1934, E. Witt put the isomorphy classes of all (nondegenerate) quadratic forms over k into a single abelian group $W(k)$, actually a ring. The class of a diagonal form $a_1x_1^2 + \cdots + a_nx_n^2$ is denoted $< a_1, \ldots, a_n >$. The class $H =< 1, -1 >$ is trivial.

Two quadratic forms of the same rank are isomorphic if and only if they have the same class in $W(k)$ (Witt's cancellation theorem). In particular : if a quadratic form q of rank n has the same Witt class as a quadratic form of rank $m < n$, then q has a nontrivial zero.

There is a “fundamental ideal” $Ik \subset Wk$ of forms of even rank. We have $Wk/Ik = Z/2$, then $Ik/I^2k = k^*/k^{*2} = H^1(k, \mathbf{Z}/2)$. The quotients $I^nk/I^{n+1}k$ and their relation to the Galois cohomology groups $H^n(k, \mathbf{Z}/2)$ have been the object of much study (Pfister, Arason, Merkurjev, Rost, Voevodsky).

The general idea here is : start with a form q. There is a quadratic form q_1 of rank at most 2 with discriminant $\pm a$ such that $q \perp -q_1$ has even rank and trivial signed discriminant, hence belongs to I^2k.

There is a map (Clifford, Hasse, Witt)

$I^2k \to \mathrm{Br}(k)[2] = H^2(k, \mathbf{Z}/2)$.

There is map $I^3k \to H^3(k, \mathbf{Z}/2)$.

Suppose

(B_2) Any class in $\mathrm{Br}(k)[2]$ can be represented by a quadratic form in I^2k of rank at most N_2.

We then get a form q_2 of rank at most N_2 such that $q \perp -q_1 \perp -q_2$ is in I^2k and has trivial image in $\mathrm{Br}(k)[2]$.

Merkurjev 1982 proved the deep theorem that the kernel of the map $I^2k \to \mathrm{Br}(k)[2]$ is the ideal I^3k.
Suppose
($cd3$) The 2-cohomological dimension of k is at most 3.
A result of Arason-Elman-Jacob 1986 then ensures $I^4k = 0$ and that $I^3k \to H^3(k, \mathbf{Z}/2)$ is an isomorphism.

Then suppose
(B_3) any class in $H^3(k, \mathbf{Z}/2)$ can be represented by a quadratic form in I^3k of rank at most N_3.
Then we find a quadratic form q_3 of rank at most N_3 such that $q \perp -q_0 \perp -q_1 \perp -q_2 \perp -q_3$ is trivial in $W(k)$. By Witt simplification, this implies that if the rank of q is at least $2 + N_2 + N_3 + 1$, then the quadratic form q is isotropic.
We thus get a universal upper bound for the dimension of an isotropic quadratic form.

Using the fact that a Pfister form $< 1, -a_1 > \otimes \cdots \otimes < 1, -a_n >$ is sent to the cup-product $(a_1) \cup \cdots \cup (a_n) \in H^n(k, \mathbf{Z}/2)$, to prove statements B_2 and B_3 it is enough to establish that elements in $H^2(k, \mathbf{Z}/2)$ and in $H^3(k, \mathbf{Z}/2)$ are expressible as sums of a bounded number of symbols $(a_1) \cup \cdots \cup (a_n)$.

This is where the arithmetic of function fields in one variable over a $\mathfrak{p}$-adic field comes in.
First of all, it is a classical result that a function field F in one variable over a $\mathfrak{p}$-adic field has cohomological dimension 3.
What about B_2 and B_3 ?

A key result here is :

Theorem (D. Saltman, 1997)
Let $l \neq p$ be prime numbers. Let K be a $\mathfrak{p}$-adic field which contains the l-th roots of 1. Let F be a function field in one variable over K. Given a finite set of central simple algebras each of exponent l in the Brauer group of F, there exist two rational functions $f, g \in F$ such that the field extension $F(f^{1/l}, g^{1/l})$ splits each of these algebras.

This leads to : for $p \neq 2$, any element in $H^2(F, \mathbf{Z}/2)$ is the sum of two symbols, and one may take $N_2 = 8$.

The idea of Saltman's paper is to kill off the ramification of an algebra of exponent l by extracting l-th roots (Motto : ramification gobbles up ramification) then use the classical theorem

Theorem (Lichtenbaum 1969, building on Tate; Grothendieck 1969, using M. Artin).
Let A be the ring of integers of a $\mathfrak{p}$-adic field K. Let Y/A be a regular, flat, proper relative curve over A. Then the Brauer group of Y is trivial.

As for B_3 for $H^3(F, \mathbf{Z}/2)$ and F as above, Merkurjev and Hoffmann-van Geel proved that any element is the sum of at most 4 elementary symbols. This immediately leads to the rough bound $N_3 = 32$.

The paper Parimala-Suresh 1998 used $H^3_{nr}(F, \mathbf{Z}/2) = 0$ for F as above (with $p \neq 2$) (Kato 1986, analogue for H^3 of the Tate-Lichtenbaum result for H^2) to show that for such an F any class in $H^3(F, \mathbf{Z}/2)$ is represented by just one symbol. Hence B_3 holds with $N_3 = 8$.

Thus any form in $n > 18$ variables has a zero.
With more care and the same algebraic and arithmetic tools, Parimala and Suresh could show (1998) that this holds for $n > 10$.

Building upon work of Saltman 2007 on the ramification pattern of central simple algebras of prime index over F, they finally reached $n > 8$.

II. The patching method

(D. Harbater)
D. Harbater and J. Hartmann
D. Harbater, J. Hartmann and D. Krashen (HHK)
CT-Parimala-Suresh (CTPS) (builds upon HHK)

Here A is a complete discrete valuation ring, K its field of fractions, k its residue field (*arbitrary*).
$F = K(X)$ the function field of a smooth, projective, geometrically connected curve over K.
Ω the set of all discrete rank one valuations on F; such valuations either are trivial on K or induce (a multiple of) the given valuation on K.
To each place $v \in \Omega$ one associates the completion F_v.

Theorem (CTPS 2008) *Assume* $char(k) \neq 2$. *Let* $q(x_1, \ldots, x_n)$ *be a quadratic form in* $n \geq 3$ *variables over* F. *If it has a nontrivial zero in each* F_v, *then it has a nontrivial zero in* F.

Let k be a finite field, i.e. let K be a $\mathfrak{p}$-adic field.
For $n > 8$ the local conditions are always fulfilled. One then recovers the Parimala-Suresh result (already recovered in HHK).
For $n = 2$ the theorem does not hold. An element in F may be a square in all F_v but not in F.
For $n = 3, 4$ it is enough to impose solutions in the F_v for v trivial on K. Consequence of Lichtenbaum's theorem.
For $n = 6, 7, 8$ consideration of the valuations trivial on K in general is not enough.

Idea of proof. The first part is HHK's argument.

There exists a connected, regular, flat model $\mathcal{X}/A$ of X/K, such that $q = < a_1, \ldots, a_n >$ with the $a_i \in F^*$ and such that the components of the special fibre $\mathcal{X}_s$ and the components of the divisors of the a_i's define a strict normal crossings divisor Δ on $\mathcal{X}$ One then produces a finite set S of closed points of $\mathcal{X}_s$ which contains all singular points of Δ, and there is a "nice" morphism from $f : \mathcal{X} \to \mathbf{P}^1_A$ such that S is the inverse image of the ∞-point on $\mathbf{P}^1_k$.

Then the support of $\mathcal{X}_s \setminus S$ is a finite union of smooth connected curves U/k.
For each U one lets $R_U \subset F$ be the ring of functions which are regular on U. One may arrange that $U \subset \mathrm{Spec}\, R_U$ is defined by one equation $s_U \in R_U$.
One then lets $\hat{R}_U$ be the completion of R_U with respect to the ideal (s_U) (or π_R). This has a residue ring $k[U]$, a Dedekind domain. One lets F_U be the fraction field of $\hat{R}_U$.
For $P \in S$, one lets $\hat{R}_P = \hat{O}_{\mathcal{X},P}$. This is a local ring of dimension 2. One lets F_P be the fraction field of $\hat{R}_P$.

Theorem (Harbater, Hartmann, Krashen)
For a system $\{U\}, S$ *as above (with* $n \geq 3$*), if* $q = 0$ *has nontrivial solutions in all* F_U *and* F_P *then it has a nontrivial solution in* F*.*

It then remains to show :
If $q = 0$ has nontrivial solutions in all completions F_v for $v \in \Omega$, then it has solutions in the F_U's and the F_P's.

The fields F_U

We have

$$q \simeq < b_1, \ldots, b_n, s_u.c_1, \ldots, s_u.c_m >$$

with all b_i and $c_i \in R_U^*$.
The hypothesis that there is a point in the DVR R_v of F associated to the generic point of U and a known theorem of Springer together imply that one of $< b_1, \ldots, b_n >$ or $< c_1, \ldots, c_m >$ has a solution in the residue field of R_v, which is the fraction field of $k[U]$. Using the fact that the b_i, c_i are units in R_U, and the fact that $k[U]$ is Dedekind, and a variant of Hensel's lemma, one gets that q has a nontrivial solution in R_U, hence in F_U.

The fields F_P

Here one looks at the local ring of $\mathcal{X}$ at a point P of S. The normal crossing divisors assumption implies that q may be written as $q = q_1 \perp xq_2 \perp yq_3 \perp xyq_4$ where x, y span the maximal ideal of R_P and the q_j are regular quadratic forms over R_P. One then uses Springer's theorem and Hensel's lemma. The DVR involved are those attached to the components of Δ passing through S. Ultimately one shows that one of the q_i has a nontrivial zero over the residue field at P, hence over the complete local ring, hence over its fraction field F_P.

Remark : the theorem holds if one replaces Ω by the set of rank one discrete valuations associated to points of codimension 1 on arbitrary connected, regular, flat, proper models $\mathcal{X}/A$ of X/K.

The HHK theorem more generally handles the case of homogeneous spaces Z/F of connected linear algebraic groups G/F such that :

(a) The underlying F-variety of G is F-rational, i.e. birational to affine space. [Very unlikely that one can dispense with this condition.] The group $SO(q)$ is F-rational.

(b) For any overfield L/F, the action of $G(L)$ on $Z(L)$ is transitive. Here there are two basic examples :

(b1) The variety Z/F is projective (as the quadrics considered above)

(b2) Z is a principal homogeneous space of G.

Under the two assumptions
(a) The underlying F-variety of G is F-rational.
(b2) Z is a principal homogeneous space of G.
a local-global theorem with respect to places of Ω is given in [CTPS].

When applied to $G = PGL_n$, it implies
The natural map $\mathrm{Br}\ F \to \prod_{v \in \Omega} \mathrm{Br}\ F_v$ is injective.
If k is finite field, this is closely related to Lichtenbaum's theorem; in that case one may then restrict attention to valuations on F which are trivial on K.

A few words on the papers HH and HHK.

The "nice" map $\mathcal{X} \to \mathbf{P}^1_A$ enables one to reduce the patching problem to the very special case where $\mathcal{X} = \mathbf{P}^1_A$, the set S consists of the ∞-point on $\mathbf{P}^1_k$ and there is just one U, namely $U = \mathbf{A}^1_k$ the complement of ∞ in $\mathbf{P}^1_k$.
We have already seen the fields F_U and F_P.
There is third character. This is the field of fractions of the completion of the DVR defined by the U on the completion of the local ring of $\mathbf{P}^1_A$ at P.
There are obvious inclusions $F_U \subset F_{P,U}$ and $F_P \subset F_{P,U}$.
One has $F = F_P \cap F_U \subset F_{P,U}$.

We are given a point $M_P \in Z(F_P)$ and a point $M_U \in Z(F_U)$. By hypothesis (b) there exists an element $g \in G(F_{P,U})$ such that $g.M_P = M_U \in Z(F_{P,U})$.
If one manages to write $g = g_U.g_P$ with $g_P \in G(F_P)$ and $g_U \in G(F_U)$ then one finds
$g_P.M_P = g_U^{-1}.M_U \in Z(F_P) \cap Z(F_U) = Z(F)$, hence $Z(F) \neq \emptyset$.

Consider the very special case $A = k[[t]]$. For G an F-rational group, the equality $G(F_{P,U}) = G(F_U).G(F_P)$ is related to the equality

$$k((x))[[t]] = k[1/x][[t]] + k[[x,t]].$$

III. The revival of C_i-fields

Let $i \geq 0$.
A field k is called a C_i–field if for each degree d every homogeneous form over k of degree $d > 0$ in $n > d^i$ variables has a nontrivial zero.
This implies (Lang, Nagata) : for each degree d and each integer r every system of r forms of degree d in $n > r.d^i$ variables has a nontrivial zero. (Proof involves introducing various other degrees.)

Definition : for a fixed integer d, a field k is called $C_i(d)$ if for each integer r every *system* of r forms of degree d in $n > r.d^i$ variables has a nontrivial zero.

A field is C_0 if and only if is algebraically closed.

A finite field is C_1 (Chevalley)

A function field in s variables over a $C_i(d)$ field is $C_{i+s}(d)$ (Tsen, Lang, Nagata for C_i; proof for $C_i(d)$ similar (Pfister, Leep). (Proof by discussing finite degree extensions and purely transcendental extension in one variable)

If K is C_i then $K((t))$ is C_{i+1} (Greenberg)
If $\mathbb{F}$ is a finite field, a function field in s variables over the local field $\mathbb{F}((t))$ is a C_{2+s}-field.
This raises the question : does the same hold for a function field in s variables over a p-adic field ?
NO, even for $s = 0$.
A p-adic field of characteristic zero is not a C_2 field, it is not a C_n field for any n (Terjanian, ...)

Solution : Look for substitutes. Replace rational points by zero-cycles of degree 1.

Definition. A field k is $C_i(d)$ *for zero-cycles of degree 1*, in short $C_i^0(d)$, if for each integer r and each *system* of r forms of degree d in $n > r.d^i$ variables there are solutions to the system in finite field extensions of k of coprime degree as a whole.

A field k is C_i *for zero-cycles of degree 1*, in short C_i^0, if for every d it is $C_i^0(d)$. For this it is enough that for each degree d any form of degree d in $n > d^i$ variables has solutions in finite field extensions of k of coprime degree as a whole.

For simplicity, assume $char.k = 0$. The field k is $C_i^0(d)$ if and only if the the fixed field of each pro-Sylow sugroup of $Gal(\overline{k}/k)$ is $C_i(d)$ (for rational solutions).

There are stability properties à la Lang-Nagata.
Proposition. If a field k is $C_i^0(d)$, then a function field in s variables over k is $C_{i+s}^0(d)$.
(Proof : reduce to $C_i(d)$ for fixed fields of Sylow subgroups.)

Conjecture (Kato–Kuzumaki 1986) :

A $\mathfrak{p}$-adic field is C_2^0.

(Special case of a more general conjecture on stability of C_i^0-property for complete DVR's)

Some evidence

Theorem. *Let $H(x_0, \ldots, X_n)$ be a homogeneous form of degree d in $n+1 \geq d^2$ variables over a $\mathfrak{p}$-adic field K. If the degree of H is prime, then $H = 0$ has a nontrivial zero in finite extensions of K of coprime degrees.*

Proofs.

Implicit : T. A. Springer (1955) ; Birch and Lewis (1958/59)

Explicit : Kato and Kuzumaki (1986).

The (module theoretic) first and third proofs yield existence of a point in an extension of K of degree $< d$.

Using Kollár's 2006 result that PAC fields of characteristic zero are C_1 (Ax's conjecture), one proves :

Theorem (CT 2008) *Let A be a discrete valuation ring with residue field k of characteristic zero. Let K be the fraction field of A. Let X/A be a regular, proper, flat connected scheme over A. Assume the generic fibre is a smooth hypersurface over K defined by a form of degree d in $n > d^2$ variables. Then the special fibre $X \times_A k$ has a component of multiplicity one which is geometrically integral over k.*

Would that theorem also hold when the residue field k of A is a finite field, then an application of the Lang-Weil estimates would (nearly) yield that $\mathfrak{p}$-adic fields are C_2^0.

Observation (CT-Parimala-Suresh 2008) If $\mathfrak{p}$-adic fields are C_2^0, then over a function field F in s variables over a $\mathfrak{p}$-adic field K, any quadratic form in more than 4.2^s variables has a nontrivial zero. Indeed, such a field F would be C_{2+s}^0. Thus a quadratic form in $n > 4.2^s$ variables over F would have a point in an extension of odd degree of F. But a theorem of T.A. Springer (1952) (conjectured by Witt 1937) then implies that the form has a zero over F.

Independent observation (D. Leep 2009) If $\mathfrak{p}$-adic fields are $C_2^0(2)$, then over a function field F in s variables over a $\mathfrak{p}$-adic field K, any quadratic form in more than 4.2^s variables has a nontrivial zero.

Theorem (Heath-Brown 27th April 2009)
A system of r quadratic forms in more than $4r$ variables over a $\mathfrak{p}$-adic field K has a rational solution if the residue field has order at least $(2r)^r$.

Consideration of unramified extensions of K of arbitrary high degree yields that $\mathfrak{p}$-adic fields are $C_2^0(2)$.

Combination of the previous arguments gives

Theorem (Leep 2009)
A quadratic form in more than 4.2^s variables over a function field in s variables over a $\mathfrak{p}$-adic field has a nontrivial zero.