Pradic Zeros of Systems of Quadratic Forms

Roger Heath-Brown

Oxford University
The problem: Let $K$ be a field, and let $r \in \mathbb{N}$. Define $\beta(r; K)$ as the largest integer $n$ for which there exist quadratic forms $q_i^r(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ $(1 \leq i \leq r)$ having only the trivial common zero over $K$.

$\beta(1; \mathbb{R}) = \infty$ $(x_1^2 + \cdots + x_n^2$ has no non-trivial zero over $\mathbb{R}, \forall n)$

$\beta(1; \mathbb{C}) = 1$ $(x_1^2 = 0 \Rightarrow x_1 = 0)$

$\beta(r; \mathbb{Q}) = r \quad \forall r \in \mathbb{N}$

Primarily interested in $K = \mathbb{Q}_p$:

$\beta(1; \mathbb{Q}_p) = 4$ (e.g. $p = 3$, $x_1^2 + x_2^2 + 3(x_3^2 + x_4^2)$ has no zero, but 5 variables suffice).

What can one say about $\beta(r; \mathbb{Q}_p)$?
Why should one care?

Local-to-Global principles. The circle method sometimes will provide a solution of \( q^{(n)}(x) = \ldots = q^{(n)}(z) = 0 \) over \( \mathbb{Z} \), given that there are solutions locally.

(But note that i) we also need to handle solvability over \( \mathbb{R} \); and ii) the circle method requires non-singular local solutions.)

Systems of quadratics are important—we can reduce general Diophantine equations to systems of quadratics.

A \( p \)-adic quadratic form in \( n \) variables has a zero if \( p \neq 2 \), and \( n \) variables suffice for any system of 16 linear forms and 8 quadratic forms.
What might we expect?

Arkin's Conjecture: A pradic form of degree $d^2$ in more than $d^2$ variables has a non-trivial zero.

$$\Rightarrow \beta(r; \mathbb{Q}_p) \leq 4r$$

and if $q(x_1, \ldots, x_4)$ has only the trivial zero, the system $q_1 = q(x_1, \ldots, x_4), q_2 = q(x_5, \ldots, x_9), q_3 = q(x_9, \ldots, x_{12})$ has 4r variables, and only the trivial zero.

Hence \(\beta(r; \mathbb{Q}_p) \geq 4r\).

Conjecture: \(\beta(r; \mathbb{Q}_p) = 4r\).

However, Arkin's conjecture is known to be false.

None the less the above conjecture remains open.
Ax-Kochen (1965). Artin’s Conjecture holds for $p = p(d)$.

\[ \forall r \in \mathbb{N} \text{ s.t. } \beta(r; \mathcal{O}_p) = 4^r \forall p \geq p(r). \]

\[ \begin{align*}
    r = 1 : & \quad \beta(1; \mathcal{O}_p) = 4 \quad (?. 19^{th} \text{ Century, Hasse 1924}) \\
    r = 2 : & \quad \beta(2; \mathcal{O}_p) = 8 \quad (Demyanov, 1956) \\
    r = 3 : & \quad \beta(3; \mathcal{O}_p) = 12 \quad \text{for } p \geq 11 \\
        & \quad (Schmur, 1980; Birch & Lewis 1965) 
\end{align*} \]

Open Question: $\beta(3; \mathcal{O}_p) = 12 \forall p$?
1st line of attack: Birch, Lewis & Murphy 1962, Birch & Lewis 1965, Schmidt 1980

WLOG $q^{(i)}(x) \in \mathbb{Z}_p[x]$. Reduce to $\mathbb{F}_p$,
$q^{(i)}(x) \rightarrow q^{(r)}(x) \in \mathbb{F}_p[x].$

If the system $Q^{(1)}, ..., Q^{(r)}$ has a non-singular zero over $\mathbb{F}_p$, then $q^{(1)}, ..., q^{(r)}$ will have a non-singular zero over $\mathbb{Q}_p$, by Hensel's Lemma.

By the Chevalley-Warning Theorem there will be a non-trivial zero over $\mathbb{F}_p$ if $n > 2r$. So the key issue is non-singularity.

Not every system $Q^{(1)}, ..., Q^{(r)}$ has a smooth zero e.g. if all the $Q^{(i)}$ vanish identically.

We need a good model over $\mathbb{Z}_p$, with excess factors in a sense.
We may make linear changes of variable $\sigma \rightarrow \tau$ without changing the problem ("Does $q^{(i)}$, ..., $q^{(r)}$ have a simultaneous zero")

Similarly we can make linear changes amongst the $q^{(i)}$.

Let $M^{(i)}$ be symmetric matrices $\sigma \rightarrow \sigma_i$ representing $q^{(i)}$.

$F(x_1, ..., x_r) := \det(X, M^{(i)} + \cdots + x_i M^{(i)})$

$P(q^{(i)}), ..., q^{(r)}) := \text{Res} \left( \frac{\partial F}{\partial x_1}, \frac{\partial F}{\partial x_2}, ..., \frac{\partial F}{\partial x_r} \right)$

It suffices to consider systems with $P \neq 0$.

Any such system has a "Minimal model", in which $q^{(i)}(x) \in \mathbb{Z}_p[x]$, and $|P(q^{(i)}, ..., q^{(r)})|_p$ is maximal.
Assume \( n > 4r \)

For a minimal model, \( Q^{(1)}(0, 0, x_3, x_4, ..., x_n) \in \mathbb{F}_p(x_1, x_2) \) cannot vanish identically.

Set \( q^{(i)'} = q^{(i)}(p x_1, p x_2, x_3, x_4, ..., x_n) \) and \( q^{(i)''} = q^{(i)}(p x_1, p x_2, x_3, ..., x_n) \) for \( 2 \leq i \leq r \).

Then \( \left| P(q^{(1)'}, q^{(2)'}, ..., q^{(r)'}) \right|_p > 1P(q^{(1)}, ..., q^{(r)}) \).

Similarly, \( Q^{(1)}(0, 0, 0, 0, x_5, x_6, ...) \) and \( Q^{(2)}(0, 0, 0, 0, x_5, x_6, ...) \) cannot both vanish identically.

Or any \( j \) of the forms, with \( x_1 = ... = x_{2j} = 0 \),

Even after making \( SL_n(\mathbb{F}_p) \) transforms on the \( x_i \),

or \( SL_r(\mathbb{F}_p) \) transforms among the \( Q^{(i)} \).

Eg \( r=1, p \neq 2 \), Diagonalize \( Q^{(1)} \) as

\[ a_1 x_1^2 + ... + a_m x_m^2 + 0 \cdot x_{m+1}^2 + ... + 0 \cdot x_n^2 \quad , \quad a_1 a_2 \cdots a_m \neq 0. \]

Then \( m \geq 3 \). Chevalley-Warning gives \( (x_1, x_2, x_3) \neq 0 \) with \( a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0 \), a non-singular zero.
\( r=1 \): easily cover \( p=2 \) too

\( r=2 \): Can show that \( q^{(1)}, q^{(2)} \) minimal, 
\( n \geq 9 \) (i.e. \( n > 4r \)) \( \Rightarrow q^{(1)}, q^{(2)} \) has a 
non-singular zero \( / \mathbb{F}_p \) \( \Rightarrow q^{(1)}, q^{(2)} \) has a 
common non-trivial zero. (Demyanov; 
Birch, Lewis \& Murphy)

\( r=3 \): Similarly, if \( p=11 \) (Schwar) — harder, 
many cases to consider.

But one cannot handle all primes this way.

\( p=2 \):

\[ Q^{(1)} = x_1x_2 + x_3 + x_2x_4 + x_5 \]
\[ Q^{(2)} = x_5x_6 + x_2^2 + x_2x_7 + x_8^2 \]
\[ Q^{(3)} = x_1^2 + x_1x_2 + x_2^2 + x_5x_7 + x_6x_8 + x_7^2 + x_8^2 \]

Satisfies the minimality condition

e.g. no linear combination vanishes when we set two 
variables to zero.

And: (Cover \( \mathbb{F}_2 \))

\( Q^{(1)} = 0 \) \( \Rightarrow \) \((x_1, \ldots, x_n) = (0, 0, 0)\) or \( x_1^2 + x_2 + x_2^2 = 1 \)

\( Q^{(2)} = 0 \) \( \Rightarrow \) \( x_5x_7 + x_6x_8 + x_7^2 + x_8^2 = 0 \)
So \( Q^{(1)} = Q^{(2)} = Q^{(3)} = 0 \Rightarrow x_1 = x_2 = x_3 = x_4 = 0 \)

\[ \Rightarrow \forall Q^{(4)} = 0 \text{ : singular zero.} \]

Conclusion: This line of attack cannot prove

\[ \beta(r; \mathbb{Q}_p) = 4r \quad \forall p, \text{ if } r \geq 3. \]

——

However one can show by this method:

Theorem (H-B, 2010)

\[ \forall r \text{ one has } \beta(r; \mathbb{Q}_p) = 4r \text{ if } p \geq (2r)^p. \]

Indeed if \( K \) is any finite extension of \( \mathbb{Q}_p \) with residue field \( F \), then \( \beta(r; K) = 4r \) if \( \# F \geq (2r)^p. \)

——

Recall: Ax-Kochen - \[ \beta(r; \mathbb{Q}_p) = 4r \text{ for } \]

\[ p = p(r) \]
One can specify \( p(r) \) - a 7-fold exponential. (!)

One can apply the Ax-Kochen method to show \( \beta(r; k) = 4r \) if \( X_F \geq p(r; k; \omega, i) \).

A condition on \( X_F \), not \( \#F \).

Idea for proof of (H-B, 2000)

Give a lower bound for the total number of zeros of \( q^{(0)} = \ldots = q^{(r)} = 0 \) if, and an upper bound for the number of singular zeros, \( \Rightarrow \exists (\) lots of \( ) 
non-singular zeros.

Show that "few" linear combinations
\[ a_1 q^{(n)} + \ldots + a_r q^{(r)} \quad (a_i \in F) \]
have "small" rank, using minimality conditions.
Corollary to (H-B, 2010) by Leep, to appear

Let \( L = Q_p(T_1, \ldots, T_k) \), then

\[
\beta(1; L) = 2^{2+k} \quad \forall \, p.
\]

Indeed one also has \( \beta(2; L) = 2^{3+k} \quad \forall \, p \).

No restriction on \( p \) !!

Idea: Let \( q(x_1, \ldots, x_n) \in L(x_1, \ldots, x_n) \) be given.

Let \( L^*/L \) be an extension of odd degree.

By a theorem of Springer, if \( q \) has a zero over \( L^* \) it has a zero over \( L \).

Take \( L^* = K(T_1, \ldots, T_k) \), \( K/Q_p \) odd

To solve \( q = 0 \) over \( L^* \) it suffices to solve a system of \( R \) quadratics in \( N \) variables, all over \( K \) ("restriction of scalars")
$N > 4R$, $N, R$ depend on $g$, but not on $K$.

We can solve this system (by HB, 2010) if the residue field of $K$ has

$\# F \geq (2R)^R$ depending only on $g$.

So choose the extension $K/\mathbb{Q}_p$ accordingly.

Springer's theorem makes the constraint on

$\# F$ disappear
A second route to $\beta(r; \mathbb{Q}_p)$ providing estimates $A_p$.

Induction on $r$: Leep 1984, ...

Work over $\mathbb{Q}_p$, not over $\overline{\mathbb{F}}_p$.

Suppose we can find a $\mathbb{Q}_p$-linear space, $L$, projective dimension $= \beta(r; \mathbb{Q}_p)$, on which $q^{(1)}, \ldots, q^{(r-k)}$ all vanish; then the remaining forms $q^{(r-k+1)}, \ldots, q^{(r)}$ must vanish on $L$.

Define $\beta(r; \mathbb{Q}_p, m)$ as the largest integer $n$ for which $\exists$ quadratic forms $q^{(1)}(x_1, \ldots, x_n), \ldots, q^{(r)}$ where there is no $\mathbb{Q}_p$-linear space of projective dimension $m$ on which all the forms vanish.

$\beta(r; \mathbb{Q}_p) \leq \beta(r-k; \mathbb{Q}_p, \beta(k))$
Suppose \( \mathbb{F} \) (\( m-1 \))-dimensional space, \( L \), spanned by \( \xi_0, \ldots, \xi_{m-1} \). To find \( \xi_m = \xi \), let \( \mathcal{Q}_p = L \oplus L^* \) and require \( \xi \in L^* \), \( \therefore \xi_0, \ldots, \xi_m \) will be independent.

\[
q(i; \xi_j, \xi) = 0 \quad (i \leq r, \ 0 \leq j \leq m) \quad \text{rm linear constraints}
\]

and \( q(i; \xi) = 0 \quad (1 \leq i \leq r) \)

We can find \( \xi \) when \( \dim L^* \geq r(m + \beta(r; \mathcal{Q}_p)) \)

\( \therefore \) when \( n \geq (r+1)m + \beta(r; \mathcal{Q}_p) \)

\[
\beta(r; \mathcal{Q}_p, m) \leq (r+1)m + \beta(r; \mathcal{Q}_p)
\]

So \( \beta(r; \mathcal{Q}_p) \leq \beta(r-1; \mathcal{Q}_p, \beta(c1)) \)

\[
= \beta(r-1; \mathcal{Q}_p, 4) \leq 4r + \beta(r-1; \mathcal{Q}_p)
\]

Induction \( \beta(1; \mathcal{Q}_p) = 4, \ \beta(2; \mathcal{Q}_p) = 8 \)

\[
\Rightarrow \beta(r; \mathcal{Q}_p) \leq \begin{cases} 2r^2 & \text{r even} \\ 2r^2 + 2 & \text{r odd} \end{cases} \quad \text{(Martin 1997)}
\]
\[ \beta(r; \mathcal{C}, M) \leq (r+1)M + \beta(r; \mathcal{C}, \mathcal{C}) \]

\( r = 1 \) : \( \beta(1; \mathcal{C}, M) \leq 2M + 4 \)

Best possible

\( r = 2 \) : \( \beta(2; \mathcal{C}, M) \leq 3M + 8 \).

Improvement due to Dietmann, 2005 (a refined H-B, 2010)

Theorem (Amer, 1976) Let \( K \) be any field with \( \chi_K \neq 2 \). Then \( \beta(2; K, M) \leq \beta(1; K(x), M) \), \( \forall M \geq 0 \).

[\( M = 0 \); \( \beta(2; K) \leq \beta(1; K(x)) \), Bruner, 1978]

Generally \( \beta(1; F, M) \leq 2M + \beta(1; F) \)

So \( \beta(1; K(x), M) \leq 2M + \beta(1; K(x)) \)

\therefore \( \beta(2; \mathcal{C}, M) \leq 2M + \beta(1; \mathcal{C}, \mathcal{C}) \)

Recall Leep (Corollary to H-B, 2010)
So \( \beta(1; \mathcal{Q}_p(x)) = 8 \)

\[ \beta(2; \mathcal{Q}_p, m) \leq 2m + 8 \]

(Best Possible)

**Question?** \( \beta(3; \mathcal{Q}_p, m) \leq 2m + O(1) \) ?

Previously:

\[ \beta(r; \mathcal{Q}_p) \leq \beta(r-k; \mathcal{Q}_p, \beta(k)) \]

\[ \Rightarrow \beta(r; \mathcal{Q}_p) \leq \beta(2; \mathcal{Q}_p, \beta(r-2)) \]

\[ \leq 2 \beta(r-2; \mathcal{Q}_p) \]

\[ \Rightarrow \beta(3; \mathcal{Q}_p) \leq 2 \beta(1; \mathcal{Q}_p) + 8 = 8 + 8 = 16 \]

(Martin - \( \beta(3; \mathcal{Q}_p) \leq 20 \))

\[ \beta(4; \mathcal{Q}_p) \leq 2 \beta(2; \mathcal{Q}_p) + 8 \leq 24 \]

\[ \beta(5; \mathcal{Q}_p) \leq 2 \beta(3; \mathcal{Q}_p) + 8 \leq 40 \]

\[ \beta(6; \mathcal{Q}_p) \leq 2 \beta(4; \mathcal{Q}_p) + 8 \leq 56 \]
Leep's induction \[ \Rightarrow \]

\[ \beta(r; \chi_p) \leq \begin{cases} 2r^2-14, & r \text{ odd } \geq 7 \\ 2r^2-16, & r \text{ even } \geq 8 \end{cases} \]

Improves previous bound by 16.

\[ r = 3 : \quad 12 \leq \beta(3; \chi_p) \leq 16 \]
1) \( K/\mathbb{Q}_p \) finite \( \# F > (2r)^r \), can solve \( r \) equations in \( \geq 4r+1 \) variables

2) Can solve \( q(x_1, \ldots, x_p) = 0 \), over \( K(X) \), if
   \( q \) is defined over \( \mathbb{Q}_p(X) \) and \( \# F \geq q \)

3) Can solve \( q(x_1, \ldots, x_q) = 0 \), over \( \mathbb{Q}_p(X) \)

4) \( \exists \) linear space of solutions of
   \( q(x_1, \ldots, x_n) = 0 \), all over \( \mathbb{Q}_p(X) \)

5) \( \exists \) linear space of solutions of
   \( q_1(x_1, \ldots, x_n) = q_2(x_1, \ldots, x_n) = 0 \), over \( \mathbb{Q}_p \)

6) \( \exists \) non-trivial zero \( \neq 0 \)
   \( q_1(x_1, \ldots, x_{17}) = q_2(x_1, \ldots, x_{17}) = q_3(x_1, \ldots, x_{17}) = 0 \)
   over \( \mathbb{Q}_p \)