P-adic decomposable form inequalities

Jan-Hendrik Evertse
Universiteit Leiden

report on work of Junjiang Liu (Leiden, Bordeaux)
(PhD-student of Pascal Autissier and J.-H. E.)

Erdős Centennial Conference, Budapest, July 4, 2013
Thue inequalities

Let \( F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d \in \mathbb{Z}[X, Y] \) be an irreducible binary form of degree \( d \geq 3 \). Define

\[
N(F, m) := \# \{ (x, y) \in \mathbb{Z}^2 : |F(x, y)| \leq m \}.
\]

**Theorem (Thue, 1909)**

\( N(F, m) < \infty \) for all \( m > 0 \).
Let $F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d \in \mathbb{Z}[X, Y]$ be an irreducible binary form of degree $d \geq 3$. Define

$$N(F, m) := \# \{(x, y) \in \mathbb{Z}^2 : |F(x, y)| \leq m\}.$$

**Theorem (Thue, 1909)**

$N(F, m) < \infty$ for all $m > 0$.

Let $V(F, m) := \text{area}\left(\{(x, y) \in \mathbb{R}^2 : |F(x, y)| \leq m\}\right)$.

Then $V(F, m) = V(F, 1)m^{2/d}$.

**Theorem (Mahler, 1933)**

$N(F, m) = V(F, 1)m^{2/d} + O_F(m^{1/(d-1)})$ as $m \to \infty$. 
Let $F \in \mathbb{Z}[X, Y]$ be an irreducible binary form of degree $d \geq 3$.

**Theorem (Bean, 1994)**

$$V(F, 1) \leq 16|D(F)|^{-1/d(d-1)}, \text{ where } D(F) \text{ denotes the discriminant of } F.$$
Let $F \in \mathbb{Z}[X, Y]$ be an irreducible binary form of degree $d \geq 3$.

<table>
<thead>
<tr>
<th>Theorem (Bean, 1994)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V(F, 1) \leq 16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Theorem (Thunder, 2001)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N(F, m) \leq C(d)m^{2/d}$ for $m \geq 1$.</td>
</tr>
</tbody>
</table>
Let $F \in \mathbb{Z}[X, Y]$ be an irreducible binary form of degree $d \geq 3$.

**Theorem (Bean, 1994)**

$$V(F, 1) \leq 16|D(F)|^{-1/d(d-1)},$$
where $D(F)$ denotes the discriminant of $F$.

**Theorem (Thunder, 2001)**

$$N(F, m) \leq C(d)m^{2/d}$$
for $m \geq 1$.

**Theorem (Thunder, 2005)**

Assume that $d$ is odd. Then

$$|N(F, m) - V(F, 1)m^{2/d}| \leq C'(d)m^{2/(d+1)}.$$
Norm form inequalities

Let $K$ be a number field of degree $d$, $\alpha_1, \ldots, \alpha_n \in K$ and $b \in \mathbb{Z} \setminus \{0\}$ such that

$$F := bN_{K/\mathbb{Q}}(\alpha_1 X_1 + \cdots + \alpha_n X_n) \in \mathbb{Z}[X_1, \ldots, X_n].$$

Define $W := \{x_1 \alpha_1 + \cdots + x_n \alpha_n : x_i \in \mathbb{Q}\}$ and

$$W^J := \{\xi \in W : \xi J \subseteq W\} \text{ for each subfield } J \text{ of } K.$$

The norm form $F$ is called **non-degenerate**, if
- $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$, and
- $W^J = (0)$ for each subfield $J$ of $K$ with $J \neq \mathbb{Q}$, imag. quadr. field.

**Theorem (Schmidt, 1971)**

*For every $m > 0$, the norm form inequality $|F(x)| \leq m$ has only finitely many solutions $x \in \mathbb{Z}^n$ if and only if $F$ is non-degenerate.*
Let \( F \in \mathbb{Z}[X_1, \ldots, X_n] \) be a decomposable form, i.e., \( F = \ell_1 \cdots \ell_d \) with \( \ell_1, \ldots, \ell_d \) homogeneous linear forms in \( n \) variables with algebraic coefficients.

We can express \( F \) as a product of (possibly equal) norm forms

\[
F = b \prod_{i=1}^{q} N_{K_i/\mathbb{Q}}(\alpha_{i1}X_1 + \cdots + \alpha_{in}X_n).
\]

Define the \( \mathbb{Q} \)-algebra \( \Omega := K_1 \times \cdots \times K_q \) with coordinatewise addition

\[
(\alpha_1, \ldots, \alpha_q) + (\beta_1, \ldots, \beta_q) = (\alpha_1 + \beta_1, \ldots, \alpha_q + \beta_q)
\]

and multiplication

\[
(\alpha_1, \ldots, \alpha_q) \cdot (\beta_1, \ldots, \beta_q) = (\alpha_1 \beta_1, \ldots, \alpha_q \beta_q),
\]

and

\[
W := \left\{ \sum_{j=1}^{n} x_j \alpha_j : x_j \in \mathbb{Q} \right\}, \quad \alpha_j = (\alpha_{1j}, \ldots, \alpha_{qj}) \in \Omega,
\]

\[
W^A := \left\{ \xi \in W : \xi A \subseteq W \right\} \quad (A \text{ } \mathbb{Q} \text{-subalgebra of } \Omega).
\]
Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form. Write as before

$$F = b \prod_{i=1}^{q} N_{K_i/\mathbb{Q}}(\alpha_i X_1 + \cdots + \alpha_{in}X_n), \quad \Omega = K_1 \times \cdots \times K_q,$$

$$W := \{ \sum_{j=1}^{n} x_j \alpha_j : x_j \in \mathbb{Q} \}, \quad \alpha_j = (\alpha_{1j}, \ldots, \alpha_{qj}),$$

$$W^A := \{ \xi \in W : \xi A \subseteq W \} \quad (A \ \mathbb{Q}\text{-subalgebra of } \Omega).$$

We call $F$ non-degenerate if
- $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$, and
- $W^A = (0)$ for every $\mathbb{Q}$-subalgebra $A$ of $\Omega$ with $A \nsubseteq \mathbb{Q}$, im. quadr. field.

**Theorem (Győry, E., 1980’s, 1990’s)**

For every $m > 0$, the inequality $|F(x)| \leq m$ has only finitely many solutions $x \in \mathbb{Z}^n$

$\iff$ $F$ is non-degenerate.
Thunder’s results on decomposable form inequalities (I)

Let \( F = \ell_1 \cdots \ell_d \in \mathbb{Z}[X_1, \ldots, X_n] \) be a decomposable form of degree \( d \), with linear factors \( \ell_1, \ldots, \ell_d \) with algebraic coefficients. Define

\[
N(F, m) := \#\{x \in \mathbb{Z}^n : |F(x)| \leq m\},
\]

\[
V(F, m) := \text{Vol}\left(\{x \in \mathbb{R}^n : |F(x)| \leq m\}\right).
\]

Then \( V(F, m) = V(F, 1)m^{n/d} \).

**Theorem (Thunder, 2001)**

*It can be effectively decided in terms of \( \ell_1, \ldots, \ell_d \) whether \( V(F, 1) \) is finite. If this is the case, then*

\[
V(F, 1) \leq C_1(n, d).
\]
Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree $d$.

We say that $F$ is of \textit{finite type} if for every non-zero linear subspace $T$ of $\mathbb{R}^n$ defined over $\mathbb{Q}$, the set $\{x \in T : |F(x)| \leq 1\}$ has finite volume in $T$.

\textbf{Theorem (Thunder)}

Assume $F$ is of finite type. Then

(i) $N(F, m) \leq C_2(n, d) m^{n/d}$ (2001),

(ii) $N(F, m) = V(F, 1) m^{n/d} + O_F(m^{n/(d+n-2)})$ as $m \to \infty$ (2001),

(iii) $|N(F, m) - V(F, 1) m^{n/d}| \leq C_3(n, d) m^{n/(d+(n-1)^{-2})}$ if $\gcd(n, d) = 1$ (2005).
Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree $d$.

We say that $F$ is of \textit{finite type} if for every non-zero linear subspace $T$ of $\mathbb{R}^n$ defined over $\mathbb{Q}$, the set $\{x \in T : |F(x)| \leq 1\}$ has finite volume in $T$.

\textbf{Theorem (Thunder)}

Assume $F$ is of finite type. Then

(i) $N(F, m) \leq C_2(n, d)m^{n/d}$ (2001), 

(ii) $N(F, m) = V(F, 1)m^{n/d} + O_F(m^{n/(d+n-2)})$ as $m \to \infty$ (2001), 

(iii) $|N(F, m) - V(F, 1)m^{n/d}| \leq C_3(n, d)m^{n/(d+(n-1)^{-2})}$ if $\gcd(n, d) = 1$ (2005).

\textbf{Fact:}

$F$ is of finite type $\iff F$ is non-degenerate.
P-adic decomposable form inequalities

Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form and $S = \{\infty, p_1, \ldots, p_t\}$, where $p_1, \ldots, p_t$ are distinct primes.

Let $|\cdot|_\infty$ denote the ordinary absolute value, and $|\cdot|_p$ the $p$-adic absolute value with $|p|_p = p^{-1}$.

We consider the inequality

$$(1) \quad \prod_{p \in S} |F(x)|_p \leq m \quad \text{in } x \in \mathbb{Z}^n \text{ with } \gcd(x, p_1 \cdots p_t) = 1$$

where $\gcd(x, p_1 \cdots p_t) := \gcd(x_1, \ldots, x_n, p_1 \cdots p_t)$ for $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$.

**Fact:**

$$\prod_{p \in S} |F(x)|_p \leq m \iff \exists a, z_1, \ldots, z_t \in \mathbb{Z} \text{ with } F(x) = ap_1^{z_1} \cdots p_t^{z_t}, \quad z_i \geq 0, \quad |a| \leq m.$$
Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form and $S = \{\infty, p_1, \ldots, p_t\}$, where $p_1, \ldots, p_t$ are distinct primes.

Let $|\cdot|_{\infty}$ denote the ordinary absolute value, and $|\cdot|_p$ the $p$-adic absolute value with $|p|_p = p^{-1}$.

We consider the inequality

\[
\prod_{p \in S} |F(x)|_p \leq m \quad \text{in } x \in \mathbb{Z}^n \text{ with } \gcd(x, p_1 \cdots p_t) = 1
\]

where $\gcd(x, p_1 \cdots p_t) := \gcd(x_1, \ldots, x_n, p_1 \cdots p_t)$ for $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$.

**Aim:**

Compare the number $N(F, S, m)$ of solutions of (1) with the “volume” $V(F, S, m)$ of a subset of $\prod_{p \in S} \mathbb{Q}_p^n$. 
Measures

Define

\[ \mu_\infty = \text{Lebesgue measure on } \mathbb{R} = \mathbb{Q}_\infty \text{ with } \mu_\infty([0,1]) = 1, \]
\[ \mu_p = \text{Haar measure on } \mathbb{Q}_p \text{ with } \mu_p(\mathbb{Z}_p) = 1 \text{ (} p \text{ prime)}, \]
\[ \mu_S = \prod_{p \in S} \mu_p = \text{product measure on } \prod_{p \in S} \mathbb{Q}_p = \left\{ (x_p)_{p \in S} : x_p \in \mathbb{Q}_p \right\}, \]
\[ \mu_S^n = \text{product measure on } \prod_{p \in S} \mathbb{Q}_p^n. \]

We view \( \mathbb{Q} \) as a subset of \( \prod_{p \in S} \mathbb{Q}_p \) via the diagonal embedding

\[ \mathbb{Q} \hookrightarrow \prod_{p \in S} \mathbb{Q}_p : x \mapsto (x)_p. \]
Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree $d$, and $S = \{\infty, p_1, \ldots, p_t\}$ where $p_1, \ldots, p_t$ are primes. Define

\[N(F, S, m) := \# \left\{ x \in \mathbb{Z}^n : \prod_{p \in S} |F(x)|_p \leq m, \ \gcd(x, p_1 \cdots p_t) = 1 \right\},\]

\[V(F, S, m) = \mu_S^n \left( \left\{ (x_p)_{p \in S} \in \prod_{p \in S} \mathbb{Q}_p^n : \prod_{p \in S} |F(x_p)|_p \leq m, \ |x_{p_i}|_{p_i} = 1 \text{ for } i = 1, \ldots, t \right\} \right),\]

where $|x|_p := \max_i |x_i|_p$ for $x = (x_1, \ldots, x_n) \in \mathbb{Q}_p^n$.

We have $V(F, S, m) = V(F, S, 1)m^{n/d}$. 
Asymptotic formulas

\[ N(F, S, m) = V(F, S, m) + O_{F, S}(m^{a(n,d)}) \]
\[ = V(F, S, 1)m^{n/d} + O_{F, S}(m^{a(n,d)}) \quad \text{as} \; m \to \infty \]

with \( a(n, d) < n/d \)

have been derived in the following cases:

- \( F \in \mathbb{Z}[X, Y] \) irreducible binary form of degree \( d \geq 3 \) (Mahler, 1933)

- \( F \in \mathbb{Z}[X_1, \ldots, X_n] \) norm form of degree \( d \geq (5n^5)^{1/3} \) with some additional constraints (R. de Jong, Master thesis, Leiden, 1998)
Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree $d$, $S = \{\infty, p_1, \ldots, p_t\}$. Write

$$F = b \prod_{i=1}^{q} N_{K_i/\mathbb{Q}}(\alpha_1 X_1 + \cdots + \alpha_n X_n), \quad \Omega = K_1 \times \cdots \times K_q,$$

$$\mathcal{W} := \{ \sum_{j=1}^{n} x_j \alpha_j : x_j \in \mathbb{Q} \}, \quad \alpha_j = (\alpha_{1j}, \ldots, \alpha_{qj}).$$

**Theorem (Győry, E., 1990’s)**

*For every $m, S$, the number $N(F, S, m)$ of $x \in \mathbb{Z}^n$ with $\prod_{p \in S} |F(x)|_p \leq m$ and $\gcd(x, p_1 \cdots p_t) = 1$ is finite*

$\iff$

- $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$, and
- $\mathcal{W}^A = (0)$ for every $\mathbb{Q}$-subalgebra $A$ of $\Omega$ with $A \neq \mathbb{Q}$. 
New results

Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree $d$ and $S = \{\infty, p_1, \ldots, p_t\}$. Define

$$N(F, S, m) = \# \{ \mathbf{x} \in \mathbb{Z}^n : \prod_{p \in S} |F(\mathbf{x})|_p \leq m, \gcd(\mathbf{x}, p_1 \cdots p_t) = 1 \},$$

$$V(F, S, 1) = \mu_S^n \left( \{ (\mathbf{x}_p)_{p \in S} \in \prod_{p \in S} \mathbb{Q}_p^n : \prod_{p \in S} |F(\mathbf{x}_p)|_p \leq 1, \right.\

$$

$$\left. |\mathbf{x}_{p_i}|_{p_i} = 1 \forall i \} \right).$$

Assume that

- $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$, and
- $W^A = (0)$ for every $\mathbb{Q}$-subalgebra $A$ of $\Omega$ with $A \not= \mathbb{Q}$. 
New results

Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree $d$ and $S = \{\infty, p_1, \ldots, p_t\}$. Define

$$N(F, S, m) = \#\{x \in \mathbb{Z}^n : \prod_{p \in S} |F(x)|_p \leq m, \gcd(x, p_1 \cdots p_t) = 1\},$$

$$V(F, S, 1) = \mu_S^n \left(\left\{(x_p)_{p \in S} \in \prod_{p \in S} \mathbb{Q}_p^n : \prod_{p \in S} |F(x_p)|_p \leq 1, \right.\right.$$

$$\left.\left|x_p\right|_{p_i} = 1 \forall i\right\}.$$

Assume that

- $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$, and
- $W^A = (0)$ for every $\mathbb{Q}$-subalgebra $A$ of $\Omega$ with $A \not\cong \mathbb{Q}$.

**Theorem (Liu, 2013)**

(i) $N(F, S, m) = V(F, S, 1)m^{n/d} + O_{F,S}(m^{n/(d+n^2)})$ as $m \to \infty$.

(ii) $N(F, S, m) \leq C_1(n, d, S)m^{n/d}$.

(iii) $V(F, S, 1) \leq C_2(n, d, S)$. 
Open problems

Theorem (Liu, 2013)

(i) \( N(F, S, m) = V(F, S, 1)m^{n/d} + O_{F,S}(m^{n/(d+n^{-2})}) \) as \( m \to \infty \).

(ii) \( N(F, S, m) \leq C_1(n, d, S)m^{n/d} \).

(iii) \( V(F, S, 1) \leq C_2(n, d, S) \).

Known: \( N(F, S, 1) \leq (2^{34} d^2)^{n^3(t+1)} \) (E., 1996).

Can the dependence on \( S \) in Liu’s bounds be replaced by a dependence on the cardinality of \( S \), and can the dependence on \( F \) in the error term be removed, i.e.,

- \( N(F, S, m) \leq C_1(n, d, t)m^{n/d} \);

- \( V(F, S, 1) \leq C_2(n, d, t) \);

- \( |N(F, S, m) - V(F, S, 1)m^{n/d}| \leq C_3(n, d, t)m^{a(n,d)} \) with \( a(n, d) < n/d \).
Ingredients of the proof

- The quantitative $p$-adic Subspace Theorem, to deal with the “large” solutions.
- Adelic geometry of numbers, to deal with the “medium” solutions (p-adization of Thunder’s method).
- Interpretation of the set of “small” solutions as $S \cap \mathbb{Z}^n$ where $S$ is a bounded subset of $\prod_{p \in S} \mathbb{Q}_p^n$, and estimation of $|\#(S \cap \mathbb{Z}^n) - \mu_S^n(S)|$. 
Thank you for your attention!