LINEAR EQUATIONS WITH UNKNOWNS FROM A MULTIPLICATIVE GROUP

Jan-Hendrik Evertse (Leiden)

Intercity Number Theory Seminar, Delft

October 21, 2005

Notation:

K is an algebraically closed field of characteristic 0.
K^* is the multiplicative group of K.

Γ is a subgroup of K^* of finite rank, i.e., there is a free subgroup Γ_0 of Γ of finite rank such that for every $x \in \Gamma$ $\exists m \in \mathbb{N}$ with $x^m \in \Gamma_0$.

Define $\operatorname{rank} \Gamma := \operatorname{rank} \Gamma_0$.

Example:
$\Gamma = \{ \sqrt[m]{2^u 3^v 5^w} : u, v, w \in \mathbb{Z}, m \in \mathbb{N}\}$ has rank 3.

We consider equations

(1) $\quad a_1 x_1 + a_2 x_2 = 1 \quad$ in $x_1, x_2 \in \Gamma$

with $a_1, a_2 \in K^*$.

Siegel-Mahler-Lang (1927-1960): (1) has only finitely many solutions.

Theorem 1. (Beukers, Schlickewei, 1996) *Let* rank $\Gamma = r$. *Then eq.* (1) *has at most* $2^{16(r+1)}$ *solutions.*

Proof. Specialization (to reduce from arbitrary fields of characteristic 0 to number fields); Diophantine approximation (Thue-Siegel method).

It is easy to construct equations

(1) $a_1x_1 + a_2x_2 = 1$ in $x_1, x_2 \in \Gamma$.

with two solutions:
pick any two distinct pairs (x_1, x_2), (y_1, y_2) from Γ and solve a_1, a_2 from $a_1x_1+a_2x_2 = 1$, $a_1y_1 + a_2y_2 = 1$.

There are "few" equations (1) with more than two solutions.

Two equations

(1) $\quad a_1x_1 + a_2x_2 = 1 \quad$ in $x_1, x_2 \in \Gamma$

and $b_1x_1 + b_2x_2 = 1$ in $x_1, x_2 \in \Gamma$ have the same number of solutions if $b_1 = a_1u_1$, $b_2 = a_2u_2$ for some $u_1, u_2 \in \Gamma$.
Taking for (u_1, u_2) a solution of (1) we obtain an equation with the same number as solutions as (1), whose sum of coefficients is 1.

A pair of coefficients $(a_1, a_2) \in K^* \times K^*$ with $a_1 + a_2 = 1$ is called *normalized*.

Theorem 2. (Győry, Stewart, Tijdeman, E., 1988): *For every subgroup Γ of K^* of finite rank there are only finitely many normalized pairs (a_1, a_2) such that (1) has more than two solutions.*

We now consider equations in $n \geqslant 3$ variables

(2) $a_1x_1 + \cdots + a_nx_n = 1$ in $x_1, \ldots, x_n \in \Gamma$

with $a_1, \ldots, a_n \in K^*$.

A solution $(x_1, \ldots, x_n)$ is called *non-degenerate* if

$$\sum_{i \in I} a_i x_i \neq 0 \text{ for each non-empty } I \subset \{1, \ldots, n\}$$

and otherwise degenerate.

Degenerate solutions give rise to infinite families of solutions.

If $(x_1, \ldots, x_n)$ is a solution with $\sum_{i=1}^{m} a_i x_i = 0$ ($m < n$) then $(ux_1, \ldots, ux_m, x_{m+1}, \ldots, x_n)$ satisfies (2) for every $u \in \Gamma$.

Laurent, van der Poorten, Schlickewei, E. (1980's):
if Γ is a subgroup of K^* of finite rank, then

(2) $\quad a_1x_1+\cdots+a_nx_n=1 \qquad \text{in } x_1,\ldots,x_n \in \Gamma$

has only finitely many non-degenerate solutions.

Theorem 3. (Schlickewei, Schmidt, E., 2002): *Let* rank $\Gamma = r$. *Then eq. (2) has at most* $\exp\Big((6n)^{4n}(r+1)\Big)$ *non-degenerate solutions.*

Proof: Specialization; Diophantine approximation (Thue-Siegel-Roth-Schmidt method)

Let $n \geqslant 3$.

A tuple $(a_1, \ldots, a_n)$ is called normalized if $(1, \ldots, 1)$ is a non-degenerate solution of

(2) $\quad a_1x_1 + \cdots + a_nx_n = 1$ in $(x_1, \ldots, x_n) \in \Gamma$

i.e., $a_1 + \cdots + a_n = 1$ and $\sum_{i \in I} a_i \neq 0$ for each non-empty $I \subset \{1, \ldots, n\}$.

Question: Does there exist an upper bound H independent of Γ such that for all but finitely normalized tuples $(a_1, \ldots, a_n)$, Eq. (2) has at most H non-denegerate solutions?

No: *For every h, there exist a multiplicative subgroup Γ of K^* of finite rank, and infinitely many normalized tuples $(a_1, \ldots, a_n) \in (K^*)^n$, such that (2) has at least h non-degenerate solutions.*

Proof. ($n = 3$). For $i = 1, \ldots, h$, pick $u_{i1}, u_{i2} \in K^*$ with $u_{i1} + u_{i2} = 2$.
Let Γ be the group generated by u_{i1}, u_{i2} ($i = 1, \ldots, h$).

Then for every $b \in K$ with $b \neq 0, 1$ the equation

$$\frac{b}{2}x_1 + \frac{b}{2}x_2 + (1 - b)x_3 = 1$$

has h solutions in Γ, i.e., $(u_{i1}, u_{i2}, 1)$ ($i = 1, \ldots, h$).

For all but finitely many b, the tuple of coefficients is normalized and the solutions are non-degenerate.

Remark. The solutions in this construction all lie in the subspace $x_1 + x_2 - 2x_3 = 0$.

Theorem 4. (Győry, E., 1989)
For every subgroup Γ *of* K^* *of finite rank, there is a finite collection* $\mathcal{E}_\Gamma$ *of normalized tuples, such that for every normalized tuple* $(a_1, \ldots, a_n) \in (K^*)^n$ *outside* $\mathcal{E}_\Gamma$*, the set of solutions of*

$$a_1 x_1 + \cdots + a_n x_n = 1 \quad \textit{in } x_1, \ldots, x_n \in \Gamma$$

is contained in the union of at most $2^{(n+1)!}$ *proper linear subspaces of* K^n*.*

Theorem 5. (E.,2004) *For every subgroup* Γ *of* K^* *of finite rank, there is a finite collection* $\mathcal{E}_\Gamma$ *of normalized tuples, such that for every normalized tuple* $(a_1, \ldots, a_n) \in (K^*)^n$ *outside* $\mathcal{E}_\Gamma$*, the set of* **non-degenerate** *solutions of*

$$a_1x_1 + \cdots + a_nx_n = 1 \quad \textit{in } x_1, \ldots, x_n \in \Gamma$$

is contained in the union of at most

$$2^n$$

proper linear subspaces of K^n*.*

Remark 1. The degenerate solutions lie in at most 2^n subspaces $\sum_{i \in I} a_ix_i = 0$ $(I \subseteq \{1, \ldots, n\})$.

Remark 2. The bound 2^n is probably far from best possible. (n???)

Ingredients of the proof:

1) The result of Schlickewei, Schmidt, E. that

$$a_1 x_1 + \cdots + a_n x_n = 1 \quad \text{in } x_1, \ldots, x_n \in \Gamma$$

has at most $\exp\Big((6n)^{4n}(r+1)\Big)$ non-degenerate solutions, where $r = \mathbf{rank}\,\Gamma$.

(In fact we will need only that this bound is independent of $a_1, \ldots, a_n$).

2) A result by Laurent on points in algebraic subvarieties of $(K^*)^n$ with coordinates in Γ.

Laurent's result.

As before, K is an algebraically closed field of characteristic 0 and Γ a subgroup of K^* of finite rank.

View $(K^*)^n$ as an algebraic group with coordinatewise multiplication $(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n)$.

An algebraic subvariety of $(K^*)^n$ is a set

$$X = \{\mathbf{x} \in (K^*)^n : \; f_1(\mathbf{x}) = \cdots f_m(\mathbf{x}) = 0\}$$

with $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$.

An algebraic subgroup of $(K^*)^n$ is an algebraic subvariety closed under coordinatewise multiplication.

A translate of an algebraic subgroup is a coset $\mathbf{x} * H = \{\mathbf{x} * \mathbf{u} : \; \mathbf{u} \in H\}$ where $\mathbf{x} \in (K^*)^n$ and H is an algebraic subgroup.

Let X be an algebraic subvariety of $(K^*)^n$.

Call a point $\mathbf{x} \in X$ *degenerate* if there is a positive dimensional algebraic subgroup H of $(K^*)^n$ with $\mathbf{x} * H \subset X$, and non-degenerate otherwise.

Theorem. (Laurent, 1980's)
X has at most finitely many non-degenerate points with coordinates in Γ.

Example. Let $X = \{a_1 x_1 + \cdots + a_n x_n = 1\}$. Then $\mathbf{x} = (x_1, \ldots, x_n)$ is non-degenerate $\iff$ $\sum_{i \in I} a_i x_i \neq 0$ for each non-empty $I \subset \{1, \ldots, n\}$.

A useful fact.

Every m-dimensional algebraic subgroup H of $(K^*)^n$ can be expressed as a direct product

$$H_0 \times G$$

where $H_0 \cong (K^*)^m$ and G is a finite group.

An algebraic subgroup of positive dimension contains points of any finite order.

Construction of a variety.

Let Γ be a subgroup of K^* of finite rank.

There is a uniform bound A such that for every $\mathbf{a} = (a_1, \ldots, a_n) \in (K^*)^n$ the equation

(2) $\quad a_1x_1 + \cdots + a_nx_n = 1 \quad$ in $x_1, \ldots, x_n \in \Gamma$

has at most A non-degenerate solutions.

(E.g., the bound of Schlickewei, Schmidt, E.)

Given a normalized tuple $\mathbf{a} = (a_1, \ldots, a_n)$, we can order the non-degenerate solutions of

$$(2) \quad a_1 x_1 + \cdots + a_n x_n = 1 \quad \text{in } x_1, \ldots, x_n \in \Gamma$$

in a sequence

$$(1, \ldots, 1), (x_{21}, \ldots, x_{2n}), \ldots, (x_{A1}, \ldots, x_{An}),$$

where we have copied some of the solutions if the number of non-degenerate solutions is smaller than A.

Thus we get

$$\text{rank} \begin{pmatrix} 1 & \cdots & 1 & 1 \\ x_{21} & \cdots & x_{2n} & 1 \\ \vdots & & \vdots & \vdots \\ x_{A1} & \cdots & x_{An} & 1 \end{pmatrix} \leqslant n \,.$$

This defines an algebraic subvariety X of $(K^*)^{n(A-1)}$ which is independent of $\mathbf{a}$.

Each normalized tuple of coefficients $\mathbf{a} = (a_1, \ldots, a_n)$ gives rise to a point $(x_{21}, \ldots, x_{An}) \in X$ with coordinates in Γ.

$\mathbf{a} \in$ **CLASS I**
if $(x_{21}, \ldots, x_{An})$ is a non-degenerate point of X.

$\mathbf{a} \in$ **CLASS II**
if $(x_{21}, \ldots, x_{An})$ is a degenerate point of X.

We will prove:

CLASS I is finite.

If $\mathbf{a}$ is in CLASS II, then the non-degenerate solutions of

$$a_1x_1 + \cdots + a_nx_n = 1 \quad \text{in } x_1, \ldots, x_n \in \Gamma$$

lie in at most 2^n subspaces of K^n.

CLASS I.

$\mathbf{a} = (a_1, \ldots, a_n)$ is such that $(x_{21}, \ldots, x_{An})$ is a non-degenerate point with coordinates in Γ of

$$X: \text{ rank } \begin{pmatrix} 1 & \cdots & 1 & 1 \\ x_{21} & \cdots & x_{2n} & 1 \\ \vdots & & \vdots & \vdots \\ x_{A1} & \cdots & x_{An} & 1 \end{pmatrix} \leqslant n\,.$$

By Laurent's Theorem, $(x_{21}, \ldots, x_{An})$ belongs to a finite set independent of $\mathbf{a}$.

We can determine $\mathbf{a}$ uniquely from $(x_{21}, \ldots, x_{An})$ by solving

$$\begin{aligned} a_1 + \cdots + a_n &= 1 \\ a_1 x_{i1} + \cdots + a_n x_{in} &= 1 \quad (i = 2, \ldots, A). \end{aligned}$$

Hence CLASS I is finite.

CLASS II.

$\mathbf{a} = (a_1, \ldots, a_n)$ is such that $\mathbf{x} = (x_{21}, \ldots, x_{An})$ is a degenerate point of

$$X: \text{ rank } \begin{pmatrix} 1 & \cdots & 1 & 1 \\ x_{21} & \cdots & x_{2n} & 1 \\ \vdots & & \vdots & \vdots \\ x_{A1} & \cdots & x_{An} & 1 \end{pmatrix} \leqslant n\,.$$

Then there is a positive dimensional algebraic group H such that $\mathbf{x} * H \subset X$.

Take $\mathbf{p} \in H$ of order 2, $\mathbf{p} = (\varepsilon_{21}, \ldots, \varepsilon_{An})$, say, with $\varepsilon_{ij} \in \{\pm 1\}$ and not all equal to 1.

Then $\mathbf{p} * \mathbf{x} \in X$, i.e.,

$$\text{rank } \begin{pmatrix} 1 & \cdots & 1 & 1 \\ \varepsilon_{21} x_{21} & \cdots & \varepsilon_{2n} x_{2n} & 1 \\ \vdots & & \vdots & \vdots \\ \varepsilon_{A1} x_{A1} & \cdots & \varepsilon_{An} x_{An} & 1 \end{pmatrix} \leqslant n\,.$$

There are $b_0, b_1, \ldots, b_n$, not all 0, such that

$$b_1 + \cdots + b_n = b_0$$
$$b_1\varepsilon_{i1}x_{i1} + \cdots + b_n\varepsilon_{in}x_{in} = b_0 \ \ (i = 1, \ldots, A).$$

Recall that $(1, \ldots, 1)$, $(x_{i1}, \ldots, x_{in})$ $(i = 2, \ldots, A)$ contain all non-degenerate solutions of

(2) $\quad a_1x_1 + \cdots + a_nx_n = 1$ in $x_1, \ldots, x_n \in \Gamma$.

Hence each non-degenerate solution of (2) satisfies one of the 2^n equations

$$\pm b_1x_1 \pm \cdots \pm b_nx_n = b_0\,.$$

Thus, if $\mathbf{a} \in$ CLASS II, then the non-degenerate solutions of (2) lie in at most 2^n proper linear subspaces of K^n.

QED

Analogues for abelian varieties.

Let A be an abelian variety and X a subvariety of A, both defined over an algebraically closed field K of characteristic 0.
Denote by $+$ the group operation and by 0 the zero element of A.

A point $\mathbf{x} \in X$ is called degenerate if there is a positive dimensional abelian subvariety B of A such that $\mathbf{x} + B \subset X$, and non-degenerate otherwise.
Denote by X^{ND} the set of non-degenerate points of X.

A subvariety X of A is called normalized if $0 \in X^{ND}$

Every subvariety can be made normalized after a translation.

Abelian varieties vs. linear equations

$A(K)$	$\longleftrightarrow$	$(K^*)^n$
X	$\longleftrightarrow$	$\{a_1x_1 + \cdots + a_nx_n = 1\}$
X^{ND}	$\longleftrightarrow$	$\sum_{i \in I} a_i x_i \neq 0$ for all I
0	$\longleftrightarrow$	$(1, \ldots, 1)$
X normalized $(0 \in X^{ND})$	$\longleftrightarrow$	$(a_1, \ldots, a_n)$ normalized ($(1, \ldots, 1)$ non-deg. sol.)

A qualitative finiteness result.

Let A be an abelian variety and X a subvariety of A, both defined over an algebraically closed field K of characteristic 0.
Let Γ be a subgroup of $A(K)$ of finite rank.

Theorem 6. (Conjectured by Lang; proved by Faltings, Hindry, McQuillan, 1990's)
$X^{ND}(K) \cap \Gamma$ *is finite.*

Proof: Diophantine approximation (Faltings); Kummer theory and specialization (Hindry, McQuillan).

Rémond's result.

Let A be an abelian variety defined over an algebraically closed field K of characteristic 0.
We may view A as a projective subvariety of $\mathbb{P}^N$ for some N.

Denote by $\mathcal{V}(n, D)$ the collection of subvarieties X of A with the following properties:
(i) X (viewed as a subvariety of $\mathbb{P}^N$) is defined by polynomials of degree $\leqslant D$ with coefficients in K;
(ii) $\dim X = n$;
(iii) X is normalized, i.e., $0 \in X^{ND}$.

Theorem 7. (Rémond, 2004)
For every subgroup Γ *of* $A(K)$ *of finite rank, there is a finite subcollection* $\mathcal{E}_\Gamma$ *of* $\mathcal{V}(n,D)$ *such that for every* $X \in \mathcal{V}(n,D) \setminus \mathcal{E}_\Gamma$*, the set* $X^{ND}(K) \cap \Gamma$ *is contained in the union of at most*

$$(2D^{n+1})^{2(\dim A)^2}$$

$(n-1)$*-dimensional subvarieties of* X*, each given by polynomials of degree at most* D*.*

Proof. Theorem 6 + arguments similar to those going into the proof of the result for linear equations.

Application to curves

Let A be an abelian variety defined over $\overline{\mathbb{Q}}$, viewed as a subvariety of $\mathbb{P}^N$. For every number field L, the group $A(L)$ is finitely generated (Mordell-Weil theorem).

Let $\mathcal{C}(D)$ be the collection of curves $C \subset A$ of genus $\geqslant 2$ defined over $\overline{\mathbb{Q}}$ such that $0 \in C$ and such that C is defined by polynomials of degree $\leqslant D$.

By applying Theorem 8 with $n = 1$, $\Gamma = A(L)$ we obtain:

Corollary. *For every number field L there is a finite subcollection $\mathcal{E}_L$ of $\mathcal{C}(D)$ such that for every curve $C \in \mathcal{C}(D) \setminus \mathcal{E}_L$, the number of L-rational points of C is at most*

$$(2D^2)^{3(\dim A)^2}.$$

Final remark.

Rémond proved a more general result for subvarieties of semi-abelian varieties which contains as special cases both his result for abelian varieties, and my result for linear equations.