PACIFIC JOURNAL OF MATHEMATICS
Vol. 180, No. 1, 1997

ON ZEROS OF BOUNDED DEGREE OF SYSTEMS OF HOMOGENEOUS POLYNOMIAL EQUATIONS

Georg Eulering and Martin Krüskemper

Let F be a finite or algebraically closed field and $R = F[T_1, \dots , T_s]$, the polynomial ring in $T_1, \dots , T_s$ over F. Then by Tsen-Lang, any system of homogeneous polynomials $f_1(X), \dots, f_r(X) \in R[X]$ of degree d, where $X = (X_1, \dots , X_n)$, has a non-trivial common zero in R^n provided the number of variables n is sufficiently large. In this note we want to give an effective bound B such that there exists a zero $0 \neq (a_1, \dots , a_n) \in R^n$ with $\max\{\deg(a_1), \dots , \deg(a_n)\} \leq B$. The bound depends on d, r, s and the maximal degree of the coefficients of the f_j where $j = 1, \dots , r$. In particular, if F is finite, a common zero can be computed effectively.

Let F be an arbitrary field. We fix $d, n, r, s \in \mathbb{N}$. Let $R_s = F[T_1, \dots , T_s]$ be the polynomial ring in $T_1, \dots , T_s$ over F. Recall that if $f \in R_s$ is a polynomial of total degree d then it has $\binom{s+d}{s}$ coefficients. A homogeneous $f \in R_s$ of degree d has $\binom{s+d-1}{s-1}$ coefficients. If $\alpha = (a_1, \dots , a_n) \in R_s^n$, we define the degree of α, $\deg(\alpha) := \max\{\deg(a_1), \dots , \deg(a_n)\}$ where $\deg(a_j)$ denotes the total degree of $a_j = a_j(T_1, \dots , T_s)$ for $j = 1, \dots , r$.

Let $X = (X_1, \dots , X_n)$, $R_s[X] = R_s[X_1, \dots , X_n]$ where X_j are new variables. If $f_1(X), \dots , f_r(X) \in R_s[X]$ are forms (i.e., homogeneous polynomials) of degree d, then a non-trivial common zero of $f_1, \dots , f_r$ is some $0 \neq \alpha = (a_1, \dots , a_n) \in R_s^n$ such that $f_j(a_1, \dots , a_n) = 0$ for any $j = 1, \dots , r$. Let $\deg(f_1, \dots , f_r)$ denote the maximal degree of the coefficients of the f_j where $j = 1, \dots , r$.

Let $i \geq 0$. A field F is called C_i-field if any form $f \in F[X] = F[X_1, \dots , X_n]$ of degree d has a non-trivial zero provided $n > d^i$. See [**L**]. Recall that F is C_0 if and only if F is algebraically closed. Further, if F is C_i then $F(T_1, \dots , T_s)$ is C_{i+s}. A survey on Tsen-Lang theory can be found in [**Lo**] for instance. In [**P1**], Pfister defined the property $C_i(d)$ for any $d \in \mathbb{N}$: A field F satisfies $C_i(d)$ if any system of r forms of degree d over F in n variables has a non-trivial common zero in F provided $n > d^i r$. For instance the field of real numbers $\mathbb{R}$ is not C_i for any i but $\mathbb{R}$ is $C_0(d)$ for all odd d. See [**P1**] for a proof.

Let F be C_i. We ask the following question: Given $f_1, \dots , f_r \in R_s[X]$ of degree d, is there a bound B depending on i, d, r, s and $\deg(f_1, \dots , f_r)$

such that there exists a common non-trivial zero $\alpha \in R_s^n$ with $\deg(\alpha) \leq B$? Following Cassels [C], Prestel showed that for any field F, a quadratic form $f \in F[T_1][X]$ which has a non-trivial zero, has a zero of degree $\leq \deg(f)(n-1)/2$. This bound is best possible. If the polynomial ring is in two or more variables, then [P], Theorem 2 shows that there is no bound anymore for arbitrary base field F. In connection with problems of real algebraic geometry, Mahé ([M]) and the first author both needed to find zeros of bounded degree of a quadratic form with values in $C[T_1, \dots, T_s]$ where C is algebraically closed. In the following we want to give such a bound B for arbitrary systems of forms by a modification of Lang's arguments in [L]: We will replace Lang's induction on s by some effective computations.

For some important remarks the authors would like to thank L. Bröcker and A. Pfister.

Let $a \in \mathbb{R}$. Let $n \in \mathbb{Z}$ such that $n-1 < a \leq n$. Then we set $\lceil a \rceil := n$.

Proposition 1. *Suppose F is $C_i(d)$. Let $R_s = F[T_1, \dots, T_s]$ and $f_1(X), \dots, f_r(X) \in R_s[X]$ be forms of degree d. Let $g := \deg(f_1(X), \dots, f_r(X))$. If $n > rd^{i+s}$, then the system $f_1, \dots, f_r$ has a non–trivial common zero $\alpha \in R_s^n$ such that $\deg(\alpha) \leq \lceil g/\tau \rceil$ where $\tau := \sqrt[s]{n/(d^i r)} - d$.*

Proof. For any $\beta = (l_1, \dots, l_s)$ where $0 \leq l_j$, we set $T^\beta := T_1^{l_1} \dots T_s^{l_s}$. For $m \in \mathbb{N}$ we set $\Lambda(m) := \{\beta = (l_1, \dots, l_s) | 0 \leq l_j \ for \ j = 1, \dots, s, \ \sum_{j=1}^s l_j \leq m\}$. Now we fix some m. For any $\beta \in \Lambda(m)$ we choose n new variables $X_{1,\beta}, \dots, X_{n,\beta}$. We substitute $X_j = \sum_{\beta \in \Lambda(m)} X_{j,\beta} T^\beta$ for $j = 1, \dots, n$ in $f_1, \dots, f_r$ and obtain for $k = 1, \dots r$,

$$f_k(\{X_{j,\beta}\}) = \sum_{\beta \in \Lambda(dm+g)} f_{k,\beta} T^\beta$$

where the $f_{k,\beta}$ are homogeneous over F of degree d in $n\binom{s+m}{s}$ variables $X_{j,\beta}$. The number of forms $f_{k,\beta}$ is $r\binom{dm+g+s}{s}$. Now we set $m := \lceil g/\tau \rceil$ where $\tau := \sqrt[s]{n/(d^i r)} - d$. We claim

$$(*) \quad n\binom{s+m}{s} > d^i r \binom{dm+g+s}{s}.$$

Then the system of forms $f_{k,\beta}$ has a non-trivial common zero in $F^{n\binom{s+m}{s}}$ and a substitution proves the first statement of Proposition 1. To show $(*)$, note that $g \le m\tau$ and hence

$$\begin{aligned} s!d^i r\binom{dm+g+s}{s} &= d^i r\prod_{j=1}^{s}(dm+g+j) \\ &\le d^i r\prod_{j=1}^{s}((d+\tau)m+j) \\ &< d^i r\prod_{j=1}^{s}(d+\tau)(m+j) = n\prod_{j=1}^{s}(m+j) = s!n\binom{s+m}{s}. \end{aligned}$$

□

Since any field F is $C_0(1)$ we obtain:

Corollary 1. *Let F be a field and $R_s = F[T_1, \dots, T_s]$. Let $f_1(X), \dots, f_r(X) \in R_s[X]$ be linear forms. Let $g := \deg(f_1(X), \dots, f_r(X))$. If $n > r$, then the system $f_1, \dots, f_r$ has a non-trivial common zero $\alpha \in R_s^n$ such that $\deg(\alpha) \le \lceil g/\tau \rceil$ where $\tau := \sqrt[s]{n/r} - 1$. The last bound is best possible if $s = 1$ and $n = r + 1$.*

Proof. If $s = 1$ and $n = r+1$, then the above bound is best possible: Consider the system of r linear forms $X_1 - T_1^g X_2,\ X_2 - T_1^g X_3, \dots, X_r - T_1^g X_{r+1}$. □

Remarks.

(1) If F is a finite field then F is C_1. If $n > rd^{s+1}$, then Proposition 1 shows that a non-trivial common zero of the system $f_1, \dots, f_r$ can be computed effectively, since only finitely many $\alpha \in R_s^n$ have to be checked.

(2) Prestel's counter example is defined over the field $\mathbb{R}$ of real numbers which does not satisfy any property C_i. If the base field F is arbitrary one should expect that unless $d = 1$ or $r = s = 1, d = 2$ there exist no bounds on the size of a zero of a system $f_1, \dots, f_r$. The case $r = s = 1, n = 2$ is one more exception:

(3) Let $s = 1$ and $f_1(X_1, X_2) \in R_1[X_1, X_2]$ be homogeneous of degree d. We show that there exists a non-trivial zero of f_1 of degree $\le g = \deg(f_1)$ provided f_1 has a non-trivial zero. Wlog we may assume $(a/b, 1)$ is the zero of f_1 where $a, b \in R, b \ne 0$. Then Gauß' theorem shows that $f_1(X_1, 1) = h(X_1)(X_1 - c)$ where $h \in R_1[X_1]$ and $c \in R_1, \deg(c) \le g$. Hence $(c, 1)$ is a zero of $f_1(X_1, X_2)$. Of course the bound is best possible.

If the base field F is finite, we can apply a stronger version of the theorem of Chevalley, Warning. If we apply [**LN**], Theorem 6.11, page 274 we can improve the statement of Proposition 1 as follows:

Corollary 2. *Let F be a finite field with q elements. Let $R_s = F[T_1, \dots, T_s]$. Let $f_1(X), \dots, f_r(X) \in R_s[X]$ be forms of degree d. Let $g := \deg(f_1(X), \dots, f_r(X))$. Suppose $n > rd^{s+1}$ and $m \geq \lceil g/\tau \rceil$, where $\tau := \sqrt[s]{n/(dr)} - d$. Then the system $f_1, \dots, f_r$ has at least $q^{n\binom{s+m}{s} - rd\binom{dm+g+s}{s}}$ different common zeros $\alpha \in R_s^n$ such that $\deg(\alpha) \leq m$. In particular if $s = 1, n > rd^2, m \geq grd$, we have $q^{(n-rd^2)m+n-rd(g+1)}$ different zeros of degree $\leq m$.*

Example. Let F be a finite field with q elements. Proposition 1 shows that a quadratic form $f \in F[T_1][X]$ in $n \geq 5$ variables with $g := \deg(f)$ has a non-trivial zero of degree $\leq 2g$. Hence in this case, Prestel's bound gives the same result. By Corollary 2, if $m \geq 2g$, there exist at least $q^{(n-4)m+n-2(g+1)}$ different zeros in $F[T_1]^n$ of degree $\leq m$.

By Tsen, if F is C_i and F admits normic forms of level i of arbitrary degree, then any homogeneous system $f_1(X), \dots, f_r(X) \in F[X]$ of degree $d_1, \dots, d_r$ has a non-trivial common zero provided $n > \sum_{j=1}^r d_j^i$. (See [**Lo**], page 158.) This holds for instance, if F is finite for $i = 1$.

Proposition 2. *Let F be a C_i field such that F admits normic forms of level i of arbitrary degree. Let $R_s = F[T_1, \dots, T_s]$. Let $f_1(X), \dots, f_r(X) \in R_s[X]$ be forms of degree $d_1, \dots, d_r$. Let $g := \deg(f_1(X), \dots, f_r(X))$. If $n > \sum_{j=1}^r d_j^{i+s}$, then the system $f_1, \dots, f_r$ has a non-trivial common zero $\alpha \in R_s^n$ such that $\deg(\alpha) \leq \lceil s(g+2)^s n/\tau \rceil$ where $\tau := n - \sum_{j=1}^r d_j^{i+s}$. In particular, $\deg(\alpha) \leq ns(g+2)^s$.*

Proof. For $m \in \mathbb{N}$ we set $\Omega(m) := \{\beta = (l_1, \dots, l_s) | 0 \leq l_j \leq m \ for \ j = 1, \dots, s\}$. Now we fix some m. For any $\beta \in \Omega(m)$ we choose n new variables $X_{1,\beta}, \dots, X_{n,\beta}$. We substitute $X_j = \sum_{\beta \in \Omega(m)} X_{j,\beta} T^\beta$ for $j = 1, \dots, n$ in $f_1, \dots, f_r$ and obtain for $k = 1, \dots r$,

$$f_k(\{X_{j,\beta}\}) = \sum_{\beta \in \Omega(dm+g)} f_{k,\beta} T^\beta$$

where the $f_{k,\beta}$ are homogeneous over F of degree d in $n(m+1)^s$ variables $X_{j,\beta}$. The number of forms $f_{k,\beta}$ is $\sum_{j=1}^r (d_j m + g + 1)^s$. The system of forms $f_{k,\beta}$ has a non–trivial common zero if $n(m+1)^s > \sum_{j=1}^r d_j^i (d_j m + g + 1)^s$, that is

$$(*) \qquad \sum_{l=0}^{s} \binom{s}{l} m^l \left(n - \sum_{j=1}^{r} d_j^{i+l} (g+1)^{s-l} \right) > 0.$$

The highest coefficient of this polynomial in m is $\tau > 0$. Hence $(*)$ is equivalent to $\tau m^s > \sum_{l=0}^{s-1} -\binom{s}{l} m^l (n - \sum_{j=1}^r d_j^{i+l} (g+1)^{s-l})$. Assume we have

$$(**) \qquad \tau m > \sum_{l=0}^{s-1} \left| \binom{s}{l} \left(n - \sum_{j=1}^{r} d_j^{i+l} (g+1)^{s-l} \right) \right| .$$

Then $(*)$ holds since we get

$$\tau m^s > \sum_{l=0}^{s-1} \binom{s}{l} m^l \left| \left(n - \sum_{j=1}^{r} d_j^{i+l} (g+1)^{s-l} \right) \right| .$$

We have $|n - \sum_{j=1}^{r} d_j^{i+l}(g+1)^{s-l}| < n(g+1)^{s-l}$. Thus $(**)$ holds if

$$\tau m \geq \sum_{l=0}^{s} n \binom{s}{l} (g+1)^{s-l} = n(g+2)^s .$$

Now set $m := \lceil (g+2)^s n/\tau \rceil$ and a substitution proves Proposition 2. $\square$

Remarks.

(a) The last proof works also if $d_1 = \cdots = d_r$ and F is $C_i(d_1)$ or if all d_j are odd and $F = \mathbb{R}$.

(b) Instead of forms and we could also consider polynomials without constant term if we replace C_i by 'strongly C_i'. See [L].

References

[C] J.W.S. Cassels, *Bounds for the least solution of homogeneous quadratic equations*, Proc. Camb. Phil. Soc., **51** (1995), 262-264.

[L] S. Lang, *On quasialgebraic closure*, Ann. of Math., **55** (1952), 373-390.

[LN] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, London, Amsterdam, Don Mills, Sydney, Tokio, 1983.

[Lo] F. Lorenz, *Einführung in die Algebra*, Teil 2, BI, Mannheim, Wien, Zürich, 1990.

[M] L. Mahé, unpublished preprint.

[P1] A. Pfister, *Systems of quadratic forms*, Bull. Soc. Math. France Memoire, **59** (1979), 115-123.

[P] A. Prestel, *On the size of zeros of quadratic forms over rational function fields*, J. Reine Angew. Math., **378** (1987), 101-112.

Received April 1, 1996.

Mathematisches Institut der Universität
Einsteinstrasse 62
D-48149 Münster, Germany
E-mail address: kruskem@math.uni-muenster.de