Michigan Math. J. 53 (2005)

On the Pfister–Leep Conjecture on C_0^d-Fields

Hamza Ahmad

1. Introduction

In analogy to algebraically closed fields, a field k is called a C_0^d*-field* if every system of r homogeneous forms of degree d over k in n variables ($n > r$) has a common nontrivial zero over k. For a prime p, a field k is called a p*-field* if $[L : k]$ is a power of p for every finite extension L/k.

In [3], Pfister proves the following theorem.

Theorem [3, Thm. 2]. *If k is a p-field then, for any d not divisible by p, k is a C_0^d-field.*

See also [4, Thm. 2]. A special case is as follows.

Corollary [3, Cor. 1]. *If k is a p-field for some prime $p \neq 2$, then k is a C_0^2-field.*

Pfister conjectured that the converse of this corollary is true.

Pfister's Conjecture [3, Conjecture 3]. *If k is a C_0^2-field, then k is a p-field for some prime $p \neq 2$.*

In [2, Thms. 5.4 & 5.5], Leep proved this conjecture for fields of characteristic 0 or 2 and gave the following generalized version of Pfister's conjecture to higher-degree forms (see [2, 1.4]).

The Conjecture of Pfister–Leep. *For a fixed d, if k is a C_0^d-field then k is a p-field for some prime $p \nmid d$.*

In this note we show (Corollary 3.2) that the Pfister–Leep conjecture is true if d is a power of the characteristic of the field k. Note that if k is a $C_0^{q^i}$-field then k is also a C_0^q-field (because if $\{F_1, \dots, F_r\}$ is a system of forms of degree q, then $\{F_1^{q^{i-1}}, \dots, F_r^{q^{i-1}}\}$ is an equivalent system of forms of degree q^i). Therefore, we need only consider the case when d is equal to the characteristic of k.

Received November 7, 2003. Revision received June 8, 2004.

2. A System of Forms

Let k be a fixed field and let $d > 1$ be a fixed integer. In this section, we define a system of forms of degree d that will be used in the proof of the special case of the conjecture. We take our variables to be $Z, X_1, X_2, \dots$.

Define $f\colon \{2,3,\dots\} \to \{1,2,\dots\}$ and $g\colon \{2,3,\dots\} \to \{d,d^2,\dots\}$ as follows. For $n \ge 2$, let $n = a_0 + a_1 d + \cdots + a_r d^r$ be the d-adic expansion of n, where $a_t \in \{0,1,\dots,d-1\}$ for $0 \le t \le r$ and $a_r \ne 0$. Set $g(n) = d^{r+1}$, and set

$$f(n) = \begin{cases} d^{r-1} & \text{if } n = d^r, \\ d^r & \text{if } n = a_r d^r \text{ and } a_r > 1, \\ a_0 d + a_1 d^2 + \cdots + a_{r-1} d^r & \text{if } n \ne a_r d^r. \end{cases}$$

Define the form ϕ_n of degree d as follows:

$$\phi_n = \begin{cases} X_n Z^{d-1} - X_{f(n)}^d & \text{if } n = d^r, \\ X_n^d - X_{g(n)}^{a_r} Z^{d-a_r} & \text{if } n = a_r d^r \text{ and } a_r > 1, \\ X_n^d - X_{f(n)} X_{g(n)}^{a_r} Z^{d-a_r-1} & \text{otherwise.} \end{cases}$$

REMARK 2.1.

(i) Since $n < d^{r+1} = g(n)$ and $f(n) < d^{r+1}$, the form ϕ_n does not involve the variables X_t, $t > d^{r+1}$.
(ii) If $n < d^m$ then $f(n) < d^m$ and $g(n) \le d^m$.
(iii) If $n = a_r d^r$ then $dn = a_r g(n)$. If $n \ne a_r d^r$, then $g(n) > n$ and $dn = f(n) + a_r g(n)$.
(iv) If $n \ne a_r d^r$ and $a_r = d-1$, then $n - f(n) = (d-1)(g(n) - n) > 0$.

Let $n = a_t d^t + \cdots + a_r d^r$ be the d-adic expansion of n, where $a_t \ne 0$, $a_r \ne 0$, $0 \le t \le r$, and $n \le d^m$. Define the "length" of n, $l(n)$, by $l(n) = r - t$.

We note that if $n \ne a_r d^r$ then $l(f(n)) < l(n)$. In addition, if $n \ne a_r d^r$ and $n < d^m$, it follows that $f(n) = a_0 d + a_1 d^2 + \cdots + a_{r-1} d^r < d^{r+1} \le d^m$.

LEMMA 2.2. *Let m be an integer ≥ 1, and let $z, x_1, x_2, \dots$ be elements from a field. If $z = 0$ and if the forms $\phi_2, \dots, \phi_{d^m}$ defined as before Remark 2.1 vanish on $(z, x_1, x_2, \dots)$, then $x_n = 0$ for $n < d^m$.*

Proof. The proof is by induction on $l(n)$. First assume $l(n) = 0$, so that $n = a_r d^r$. Since $\phi_{d^r} = X_{d^r} Z^{d-1} - X_{f(d^r)}^d$ vanishes on $(0, x_1, x_2, \dots)$ for $1 \le r \le m$, it follows that $x_{d^{r-1}} = x_{f(d^r)} = 0$. If $n = a_r d^r$ and $1 < a_r < d$, then the vanishing of $\phi_n = X_n^d - X_{g(n)}^{a_r} Z^{d-a_r}$ on $(0, x_1, x_2, \dots)$ implies that $x_n = 0$. This completes the case $l(n) = 0$.

Now assume $l(n) \ge 1$, so that $n \ne a_r d^r$. Since $l(f(n)) < l(n)$ and $f(n) < d^m$, the induction hypothesis implies $x_{f(n)} = 0$. Since $\phi_n = X_n^d - X_{f(n)} X_{g(n)}^{a_r} Z^{d-a_r-1}$ vanishes on $(0, x_1, x_2, \dots)$ and since $x_{f(n)} = 0$, it follows that $x_n = 0$. $\square$

LEMMA 2.3. *Let m be an integer ≥ 1, and let $z, x_1, x_2, \ldots$ be elements from a field. If $z = 1$ and the forms $\phi_2, \ldots, \phi_{d^m}$ defined previously vanish on $(z, x_1, x_2, \ldots)$, then*

$$x_n = \varepsilon_n x_1^n \quad \textit{for } n \leq d^m,$$

where ε_n is a d-power root of unity.

REMARK 2.4. From the proof of this lemma we shall see that:

(i) $\varepsilon_n = 1$ if $n = d^r$ (in particular, for any n, $\varepsilon_{g(n)} = 1$ since $g(n)$ is a d-power);
(ii) ε_n is a dth root of unity if $n = ad^r$, $1 < a < d$; and
(iii) $\varepsilon_n = \varepsilon\varepsilon_{f(n)}^{1/d}$, where ε is a dth root of unity if $n \neq ad^r$, $1 \leq a < d$.

Proof of Lemma 2.3. The proof is by induction on $l(n)$. We begin with the case $l(n) = 0$, so that $n = a_r d^r$.

If $a_r = 1$, so that $n = d^r$, we will prove by induction on r that $x_{d^r} = x_1^{d^r}$ for $0 \leq r \leq m$. If $r = 0$, then $x_1 = x_1^1$. Now assume that $r \geq 1$. Since $\phi_{d^r} = X_{d^r} Z^{d-1} - X_{f(d^r)}^d = X_{d^r} Z^{d-1} - X_{d^{r-1}}^d$ vanishes on $(1, x_1, x_2, \ldots)$, it follows that $x_{d^r} = x_{d^{r-1}}^d$. The induction hypothesis implies that $x_{d^r} = x_{d^{r-1}}^d = (x_1^{d^{r-1}})^d = x_1^{d^r}$. If $n = a_r d^r$ $(1 < a_r < d)$, then the vanishing of $\phi_n = X_n^d - X_{g(n)}^{a_r} Z^{d-a_r}$ on $(1, x_1, x_2, \ldots)$ implies that $x_n^d = x_{g(n)}^{a_r}$. Since $n < d^m$, we have $g(n) = d^{r+1} \leq d^m$ by Remark 2.1(ii) and $x_{g(n)} = x_1^{g(n)}$ by the previous case. Hence $x_n^d = x_{g(n)}^{a_r} = x_1^{a_r g(n)} = x_1^{dn}$, by Remark 2.1(iii). Therefore $x_n = \varepsilon_n x_1^n$, where ε_n is a dth root of unity. This completes the case $l(n) = 0$.

Now assume that $l(n) = r - t > 0$, so that $n \neq a_r d^r$. Then $n < d^m$ and $g(n) \leq d^m$ and hence $x_{g(n)} = x_1^{g(n)}$. Thus the vanishing of $\phi_n = X_n^d - X_{f(n)} X_{g(n)}^{a_r} Z^{d-a_r-1}$ on $(1, x_1, x_2, \ldots)$ implies that $x_n^d = x_{f(n)} x_1^{a_r g(n)}$. Since $n \neq a_r d^r$, we have $l(f(n)) < l(n)$ and $f(n) < d^m$. Therefore, the induction hypothesis implies that $x_{f(n)} = \varepsilon_{f(n)} x_1^{f(n)}$, where $\varepsilon_{f(n)}$ is a d-power root of unity. Then

$$x_n^d = x_{f(n)} x_1^{a_r g(n)} = \varepsilon_{f(n)} x_1^{f(n)} x_1^{a_r g(n)} = \varepsilon_{f(n)} x_1^{f(n)+a_r g(n)} = \varepsilon_{f(n)} x_1^{dn}$$

by Remark 2.1(iii). Hence $x_n = \varepsilon\varepsilon_{f(n)}^{1/d} x_1^n$, where ε is a dth root of unity. Then $x_n = \varepsilon_n x_1^n$, where $\varepsilon_n = \varepsilon\varepsilon_{f(n)}^{1/d}$ is a d-power root of unity. □

3. The Main Result

In this section we will prove our main result, stated as follows.

THEOREM 3.1. *Let k be a field of characteristic d. Given a polynomial h over k of degree d^m $(m \geq 1)$ in one variable, there exists a system S of r $(= d^{m-1})$ forms of degree d in $r + 1$ variables such that h has a zero in k if and only if the system S has a common nontrivial k-zero.*

As a corollary, we have the following.

COROLLARY 3.2. *Let k be a field of characteristic d. If k is a C_0^d-field, then*:

(i) *every polynomial in $k[X]$ of d-power degree has a zero in k; and*
(ii) *k is a p-field for some prime p not dividing d.*

Proof. Since k is a C_0^d-field, the system S in Theorem 3.1 has a nontrivial k-zero. Therefore, the polynomial h has a zero in k; hence (i) follows. Now (ii) follows from (i) and the following proposition, which was proved by Leep for the case $d = 2$; the proof of the general case is identical.

PROPOSITION 3.3 [1, Prop. 4.4]. *A field k is a p-field for some prime number p not dividing d if and only if every polynomial in $k[X]$ of d-power degree has a zero in k.*

Before starting the proof of Theorem 3.1, we need the following definitions.

Define the functions $i\colon \{d, d+1, d+2, \ldots\} \to \{1, 2, \ldots\}$ and $j\colon \{d, d+1, d+2, \ldots\} \to \{1, d, d^2, \ldots\}$ as follows. For any integer $n \geq d$, write the d-adic expansion of n as $n = a_0 + a_1 d + \cdots + a_r d^r$, where $a_r \neq 0$. Set $j(n) = d^r$, and set

$$i(n) = \begin{cases} a_r d^{r-1} & \text{if } n = a_r d^r, \\ a_0 + a_1 d + \cdots + a_{r-1} d^{r-1} & \text{if } n \neq a_r d^r. \end{cases}$$

Now, for $n \geq 0$, define the monomials Y_n (of degree d) as

$$Y_n = \begin{cases} X_1^n Z^{d-n} & \text{if } 0 \leq n < d, \\ X_{i(n)}^d & \text{if } d \leq n = a_r d^r, \\ X_{i(n)} X_{j(n)}^{a_r} Z^{d-a_r-1} & \text{if } d < n \neq a_r d^r. \end{cases}$$

Given a polynomial $h = X^{d^m} + c_{d^m-1} X^{d^m-1} + \cdots + c_1 X + c_0$ with coefficients c_i from k, let ϕ_h (a form of degree d) be

$$\phi_h = Y_{d^m} + c_{d^m-1} Y_{d^m-1} + \cdots + c_1 Y_1 + c_0 Y_0.$$

REMARK 3.4.

(i) Note that $i(n) < d^r = j(n)$. Also, if $d \leq n < d^m$ then $r < m$, hence $i(n) < d^{m-1}$ and $j(n) \leq d^{m-1}$. In particular, for h of degree d^m, the form ϕ_h involves only the variables $Z, X_1, \ldots, X_{d^{m-1}}$.
(ii) Let $n \geq d$. If $n = a_r d^r$ then $d\,i(n) = n$, and if $n \neq a_r d^r$ then we have $n = i(n) + a_r j(n)$.
(iii) If h has degree d, then ϕ_h is the homogenization of h.

Proof of Theorem 3.1. Let k be a field of characteristic d. Throughout the proof, for $n > 0$ let $n = a_0 + \cdots + a_r d^r$ ($a_r \neq 0$) be the d-adic expansion of n. For any elements $z, x_1, x_2, \ldots, x_{d^{m-1}}$ of k and for $n = 0, \ldots, d^m$, let

$$y_n = \begin{cases} x_1^n z^{d-n} & \text{if } 0 \leq n < d, \\ x_{i(n)}^d & \text{if } d \leq n = a_r d^r, \\ x_{i(n)} x_{j(n)}^{a_r} z^{d-a_r-1} & \text{if } d < n \neq a_r d^r. \end{cases}$$

Take S to be the system consisting of the d^{m-1} forms $\phi_h, \phi_2, \ldots, \phi_{d^{m-1}}$. These forms have degree d. By Remarks 2.1(i) and (ii) and Remark 3.4(i), the system involves the $d^{m-1}+1$ variables $Z, X_1, \ldots, X_{d^{m-1}}$.

Claim: The system S has a nontrivial k-zero if and only if the polynomial h has a k-zero.

If $m = 1$ then, as noted in Remark 3.4(iii), $S = \{\phi_h\}$ is just the homogenization of h and hence the claim is proved in this case. So we may assume $m > 1$.

First, assume that the system $\phi_h, \phi_2, \ldots, \phi_{d^{m-1}}$ has a nontrivial common zero $(z, x_1, x_2, \ldots, x_{d^{m-1}})$ over k. Then z cannot be zero. Otherwise, if $z = 0$ then (by Lemma 2.2) $x_n = 0$ for $1 \le n < d^{m-1}$. By Remark 3.4(i), $d \le n < d^m$ implies $i(n) < d^{m-1}$. Hence $x_{i(n)} = 0$ for $d \le n < d^m$, which implies that $y_n = 0$ for $0 \le n < d^m$. Therefore, the vanishing of ϕ_h on $(z, x_1, x_2, \ldots, x_{d^{m-1}})$ implies $0 = y_{d^m} = x_{i(d^m)}^d$. But $i(d^m) = d^{m-1}$, so $x_{d^{m-1}} = 0$. Thus $z = 0$ leads to the trivial solution—a contradiction.

We may therefore assume that $z = 1$. We'll show that x_1 is a zero of h. Note that, since the characteristic of k is d, all the d-power roots of unity are equal to 1. By Lemma 2.3, $x_n = x_1^n$ for $1 \le n \le d^{m-1}$. Hence, for $0 \le n \le d^m$,

$$\begin{aligned} y_n &= \begin{cases} x_1^n & \text{if } 0 \le n < d \\ x_1^{di(n)} & \text{if } d \le n = a_r d^r \\ x_1^{i(n)+a_r j(n)} & \text{if } d < n \ne a_r d^r \end{cases} \\ &= x_1^n \quad \text{(by Remark 3.4(ii))}. \end{aligned}$$

Since ϕ_h vanishes on $(1, x_1, \ldots, x_{d^{m-1}})$, we have

$$\begin{aligned} 0 &= y_{d^m} + c_{d^m-1} y_{d^m-1} + \cdots + c_0 y_0 \\ &= x_1^{d^m} + c_{d^m-1} x_1^{d^m-1} + \cdots + c_0 \\ &= h(x_1). \end{aligned}$$

Hence x_1 is a zero of h.

Conversely, assume that there exists an $\alpha \in k$ such that $h(\alpha) = 0$. Put $z = 1$ and $x_n = \alpha^n$ for $n \ge 1$. We verify that $(z, x_1, \ldots, x_{d^{m-1}})$ is a common zero of the forms $\phi_h, \phi_2, \ldots, \phi_{d^{m-1}}$. As before, by Remark 3.4(ii) we have

$$\begin{aligned} y_n &= \begin{cases} \alpha^n & \text{if } 0 \le n < d \\ \alpha^{di(n)} & \text{if } d \le n = a_r d^r \\ \alpha^{i(n)+a_r j(n)} & \text{if } d < n \ne a_r d^r \end{cases} \\ &= \alpha^n. \end{aligned}$$

Therefore,

$$\begin{aligned} 0 = h(\alpha) &= \alpha^{d^m} + c_{d^m-1}\alpha^{d^m-1} + \cdots + c_0 \\ &= y_{d^m} + c_{d^m-1} y_{d^m-1} + \cdots + c_0 y_0 \end{aligned}$$

and hence ϕ_h vanishes on $(z, x_1, \ldots, x_{d^{m-1}})$.

To verify that ϕ_n vanishes on $(z, x_1, \dots, x_{d^{m-1}})$ for $1 < n \le d^{m-1}$, first assume that $n = d^r$. Then $f(n) = d^{r-1}$ and therefore $x_n z^{d-1} - x_{f(n)}^d = \alpha^n - \alpha^{df(n)} = \alpha^{d^r} - \alpha^{d(d^{r-1})} = 0$. Hence, ϕ_n vanishes on $(z, x_1, \dots, x_{d^{m-1}})$ in this case. Now assume that $n = a_r d^r$ for $a_r \ne 1$. Then $g(n) = d^{r+1}$ and we have $x_n^d - x_{g(n)}^{a_r} z^{d-a_r} = \alpha^{dn} - \alpha^{a_r g(n)} = \alpha^{a_r d^{r+1}} - \alpha^{a_r d^{r+1}} = 0$; hence ϕ_n vanishes on $(z, x_1, \dots, x_{d^{m-1}})$ in this case, too. Finally, assume that $n \ne a_r d^r$. By Remark 2.1(iii), $dn = f(n) + a_r g(n)$; hence

$$x_n^d - x_{f(n)} x_{g(n)}^{a_r} z^{d-a_r-1} = \alpha^{dn} - \alpha^{f(n)+a_r g(n)} = \alpha^{dn} - \alpha^{dn} = 0,$$

so ϕ_n vanishes on $(z, x_1, \dots, x_{d^{m-1}})$. This completes the proof of the theorem. □

ACKNOWLEDGMENT. The proofs of Lemmas 2.2 and 2.3 as given in this note are due to the referee and are an improvement over the author's original proofs. The author thanks the referee for providing them.

References

[1] D. Leep, *Systems of quadratic forms,* J. Reine Angew. Math. 350 (1984), 109–116.

[2] ———, *Pfister's conjecture on quadratic C_0-fields,* J. Reine Angew. Math. 404 (1990), 209–220.

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

[4] ———, *A new proof of the homogeneous nullstellensatz for p-fields and applications to topology,* Recent advances in real algebraic geometry and quadratic forms, 1991–1992 (B. Jacob, T. Y. Lam, R. Robson, eds.), Contemp. Math., 155, pp. 221–230, Amer. Math. Soc., Providence, RI, 1994.

Department of Mathematical Sciences
Saginaw Valley State University
University Center, MI 48710