Boletín de la Sociedad Matemática Mexicana Vol. 28, No. 1, 1983

ON THE HOPF CONDITION OVER AN ARBITRARY FIELD

BY SERGEY YUZVINSKY

1. Introduction

Throughout this paper, F will always denote a field of characteristic different from 2. Let (U, q_u), (V, q_v), (W, q_w) be regular quadratic spaces over F of dimensions m, n, and p. By a *pairing* of (U, q_u) and (V, q_v) in (W, q_w) we mean a bilinear mapping $\mu: U \times V \to W$ such that

$$q_w(\mu(x, y)) = q_u(x) \cdot q_v(y), \quad x \in U, y \in V. \tag{1}$$

We will call such a μ a pairing of *type* $[m, n, p]$. When the forms q_u, q_v, and q_w can be represented over F as sums of squares, μ is often called a *normed map.* The problem to find all triples (m, n, p) for which a normed map of type $[m, n, p]$ exists is usually referred to as the (generalized) Hurwitz problem. One can find a history of the problem and a description of known results in an expository paper [7].

In this paper we are mainly concerned with the Hopf condition.

Definition. Let (m, n, p) be a triple of positive integers. We say that it satisfies the *Hopf condition* if

$$\binom{p}{k} \equiv 0 \pmod 2 \text{ whenever } k \geq 0 \text{ and } p - m < k < n.$$

Using topological techniques, H. Hopf proved in [4] that this condition is necessary for the existence of a pairing of type $[m, n, p]$ over $\mathbb{R}$ (see also [8] for a simple proof). F. Behrend generalized this result to any formally real field [3]. Recently K. Y. Lam and T. Y. Lam have found simple field theory arguments which allow them to generalize the result to any field of characteristic 0 (see [7]). For an arbitrary field (of characteristic different from 2) the necessity of the Hopf condition for the existence of a pairing of type $[m, n, p]$ has been proved only in several particular cases. For $n = p$ this follows from the much more general results of D. Shapiro [6]. J. Adem proved this for m, $n, p \leq 8$ in [1] and for $m = 3$ and arbitrary n, p in [2].

The goal of this paper is to prove that the Hopf condition is necessary for the existence of a pairing of type $[4, n, p]$ for any n, p and any F. In particular, we obtain the answer of the generalized Hurwitz problem for $m = 4$: it is the same as for the real field.

I would like to thank K. Y. Lam and D. B. Shapiro for re-stimulating my interest in the problem and useful discussions.

2. Reduction of the problem

We apply the following standard reduction of the problem. First of all, a pairing over a field F can be viewed as a pairing of the same type over the algebraical closure of F. It allows us to consider only algebraically closed fields and, in particular, to assume that the forms q_u, q_v, and q_w can be represented as sums of squares (we will use this only for q_u). Using this assumption, we fix a basis $\{e_l, \cdots, e_m\}$ in U such that $q_u(e_i, e_j) = \delta_{ij}$, $i, j = 1, \cdots, m$, and obtain the operators $A_1, \cdots, A_m$: $V \to W$ defined by

(2) $$A_i x = \mu(e_i, x), \qquad x \in V, i = 1, \ldots, m.$$

Here, by abuse of notation, we use q_v for the corresponding bilinear form also. Since the spaces V and W are regular, the conjugate operators $A_i^*: W \to V$ are well-defined by the usual equalities

$$q_v(A^*y, x) = q_w(y, Ax), \qquad x \in V, y \in W.$$

It is well-known (and easy to prove—cf. [1], [8]) that the above operators satisfy the following system of equations:

(3) $$A_i^* A_i = I_v,$$

(4) $$A_j^* A_i + A_i^* A_j = 0, \qquad i \neq, i, j = 1, \cdots, m.$$

Conversely, any m operators $A_1, \cdots, A_m: V \to W$ satisfying (3, 4) define by (2) and linearity a pairing of type $[m, n, p]$. Instead of the system (3, 4) one can consider the normalized system which one obtains replacing A_i by $A_i A_1^*$, $i = 2, \cdots, m$. To find the normalized system let us put $B_i = A_{i+1} A_1^*$, $i = 1, 2, \cdots, m - 1$. Then B_i for any i is an operator on W, $\rho = A_1 A_1^*$ is the orthogonal projection of W to its n-dimensional subspace $A_1(V)$ (along $A_1(V)^\perp$), and the system (3, 4) implies

(5) $$B_o^* B_i = \rho,$$

(6) $$\rho B_i + B_i^* \rho = 0,$$

(7) $$B_j^* B_i + B_i^* B_j = 0, \qquad i \neq j, i, j = 1, \cdots, m - 1.$$

In fact the system (5), (6), (7) is equivalent to (3), (4). One can easily see that putting in (5), (6), (7) $V = \rho(W)$, $A_1 = I_v$ and $A_{i+1} = B_{i|V}$, $i = 1, \ldots, m - 1$. In particular, when $m = 2$ we have one operator satisfying (5) and (6). We will use the elementary fact that if such an operator exists and $p = n$ then n is even.

To prove the necessity of the Hopf condition for the existence of a pairing over F one does not have to consider all triples (m, n, p). A simple argument [3] shows that it suffices to study only the cases when $p = m + n - 2$. In particular, for $m = 4$ it suffices to prove the nonexistence of pairings of types $[4, 4k + 1, 4k + 3]$ for any $k = 1, 2, 3, \cdots$.

We prove this result in Section 4. In Section 3, we study the structure of pairings of types $[2, n, p]$ with $p \leq n + 2$. We have to deal with not necessarily regular spaces and we use some standard notations and facts from the first four sections of the book [5]. In addition, for a quadratic space A and a subspace B of A, we denote by $B_A^\perp$ the orthogonal complement of B in A.

3. Preliminary results

In this section we denote by L a quadratic space over F of dimension p with a bilinear symmetric form f. In the first part of the section we do not assume that f is regular. Nevertheless we want to consider an operator $A:L \to L$ satisfying conditions which in the regular case whould be equivalent to (5, 6). For $n = p$ (that is $\rho = I_L$) these conditions are

$$A^2 = -I_L \tag{8}$$

$$f(Ax, y) = -f(x, Ay), \qquad x, y \in L \tag{9}$$

LEMMA 1. *Assume that $R = \text{rad } L$, S is a subspace of L such that $L = S \oplus R$, σ is the projection of L on S along R, and $A:L \to L$ is an operator satisfying* (8, 9). *Then $\sigma A_{|S}$ is an operator on S also satisfying* (8, 9).

Proof. i) By (9), $A(R) \subset R$. If we put $A_0 = \sigma A_{|S}$ and $\bar{\sigma} = 1 - \sigma$ then we have for any $x \in S$

$$A_0{}^2x = \sigma A \sigma A x = \sigma A(Ax - \bar{\sigma}Ax) = \sigma A^2 x = -\, x,$$

which implies (8) for A_0.

(ii) Let us denote by f_S the restriction of f to $S \times S$. By the definition of S, $f_S(\sigma x, \sigma y) = f(x, y)$ for any $x, y \in L$. Consequently, $f_S(A_0 x, y) = f(Ax, y)$ for any $x, y \in S$, which implies (9) for A_0.

COROLLARY 1. *If there exists an operator on L satisfying* (8, 9) *then* $\dim L - \dim R$ *is even.*

Proof. This follows from lemma 1 and the fact that any subspace S such that $L = S \oplus R$ is regular.

LEMMA 2. *Again let $R = \text{rad } L$ and let $A:L \to L$ be an operator satisfying* (8, 9). *If* $\dim R = 1$ *then there exists a subspace $S \subset L$ such that $L = S \oplus R$ and S is invariant with respect to A.*

Proof. According to Corollary 1, p is odd. We denote by S_1 an arbitrary subspace of L such that $S_1 \oplus R = L$ and use induction on p. The case $p = 1$ is trivial. Let us suppose that $p = 3$. If $A(S_1) = S_1$ then the statement is proved. Let $A(S_1) \neq S_1$. We set $T = S_1 \cap A(S_1)$ and notice that $\dim T = 1$. If $x \neq 0$ and $x \in T$ then, due to (8), x is an eigenvector of A and it follows from (9) that x is isotropic. Since S_1 is regular, there exists a vector $y \in S_1$ such that $f(y, y) = 0$ and $f(x, y) = 1$. If z is a non-zero vector from R then $\{x, y, z\}$ is a basis of L. It follows from (8, 9) that A preserves f; in particular, $f(Ay, Ay) = 0, f(Ax, Ay) = 1$. Using this and (8) again, one easily finds that the matrix of A with respect to the ordered basis (x, y, z) is

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & -\lambda & 0 \\ 0 & \alpha & \lambda \end{pmatrix}$$

where $\lambda^2 = -1$, $\alpha \neq 0$. It is clear that $y' = y + \frac{1}{2}\alpha\lambda z$ is an eigenvector of A and that the subspace S spanned by x and y' has the required properties.

We consider now $p > 3$ and assume that for all spaces of dimension $p - 2$ the statement is proved. It is again sufficient to consider the case when $A(S_1) \neq S_1$, which implies $\dim T = p - 2$ where $T = S_1 \cap A(S_1)$. Due to (8), T is invariant with respect to A. Since $p - 2$ is odd, $Q = \text{rad } T \neq 0$. On the other hand, $\dim Q \leq \dim T_{S_1}{}^{\perp} = \dim S_1 - \dim T = 1$; that is, $\dim Q = 1$. According to the induction hypothesis, there exists a subspace W of T such that $W \oplus Q = T$ and W is invariant with respect to A. Since A preserves f and W is regular, $W_L{}^{\perp}$ is invariant with respect to A and $\text{rad } W_L{}^{\perp} = \text{rad } L = R$. Since $\dim W_L{}^{\perp} = 3$, it follows from the first part of the proof that there exists an subspace $V \subset W_L{}^{\perp}$ such that $V \oplus R = W_L{}^{\perp}$ and V is invariant with respect to A. The space $S = W \oplus V$ clearly has the required properties.

In the remaining part of the section we assume that f is regular and we denote by ρ the orthogonal projection of L on a regular n-dimensional subspace V. We fix an operator $A: L \to L$ such that

$$A^*A = \rho, \tag{10}$$

$$\rho A + A^*\rho = 0. \tag{11}$$

We set $B = \rho A$, $C = A - B = (1 - \rho)A$. Using (10, 11) and the obvious inclusions $\text{Im } B \subset V$, *Ker* $B^* \supset V^{\perp}$, $\text{Im } C \subset V^{\perp}$, $\text{Ker } C^* \supset V$, one obtains the conditions on B and C equivalent to (10, 11):

$$B^* + B = 0, \tag{12}$$

$$-B^2 + C^*C = \rho \tag{13}$$

(in a matrix form these conditions are contained implicitly in [8] and explicitly in [1]).

LEMMA 3. *Let either $p = n + 1$ or $p = n + 2$ and n is odd. Then the subspace $W = V \cap A^{-1}(V)$ of L is invariant with respect to A and the restriction A_0 of A to W satisfies* (8, 9).

Proof. If $x \in W$, then $y = Ax \in V$, that is $y = Bx$, $Cx = 0$. This and (13) imply that $B = B^2x = -x$. To prove the lemma it suffices to prove that $Cy = 0$. We put $U = \text{Im } C \subset V^{\perp}$. For any $u \in U$ (that is, $u = Cv$ for some $v \in L$) we have

$$f(Cy, u) = f(Cy, Cv) = f(C^*Cy, v) = f(y + B^2y, v) = 0.$$

In other words, $Cy \in \text{rad } U$. We will consider now two different cases.

(i) Let $p = n + 1$. It implies that $\dim V^{\perp} = 1$. Since $V^{\perp}$ is a regular space, $Cy = 0$.

(ii) Let $p = n + 2$ where n is odd. Let us suppose that $Cy \neq 0$. Since $V^{\perp}$ is a regular space of dimension 2, $\dim U = 1$ and U is totally isotropic. This implies that for any $z_1, z_2 \in L$ we have $f(C^*Cz_1, z_2) = f(Cz_1, Cz_2) = 0$. Therefore $C^*C = 0$ and the restriction B_0 of B to V satisfies $-B_0{}^2 = I_V$, $B_0 = -B_0{}^*$. But this contradicts the assumption that n is odd. The contradiction completes the proof.

LEMMA 4. *Under the conditions of lemma* 3 *the subspace* $W = V \cap A^{-1}(V)$ *of* L *is regular.*

Proof. If $W = V$ then the statement follows. If $W \neq V$ we will consider several cases.

(i) Let $p = n + 1$. This implies that $\dim W = n - 1$ and $\dim W_V{}^{\perp} = 1$. We put $R = \operatorname{rad} W$. Our goal is to prove that $R = 0$. Let us suppose that on the contrary $R \neq 0$ and consequently $\dim R = 1$. Applying lemma 2 to the operator $A_{|W}: W \to W$, we can find a subspace S of W such that $W = S \oplus R$ and $A(S) \subset S$. Since V is a regular space there exists a 1-dimensional isotropic subsapce R' of V such that $P = R \oplus R'$ is a hyperbolic plane and $V = S \perp P$. We put $R'' = A(R')$. Then the inclusion $A(S) \subset S$ and (11) imply that $R'' \subset S_L{}^{\perp}$ and therefore $S_L{}^{\perp} = P \oplus R'' = R \oplus R' \oplus R''$. Since L and S are regular spaces, $S_L{}^{\perp}$ is also a regular space. At the same time, applying again (10, 11) to an arbitrary non-zero vector $x \in R'$ we obtain $f(Ax, Ax) = f(A^*, Ax, x) = f(x, x) = 0$ and $f(ax, x) = f(x, A^*x) = -f(x, \rho Ax) = -f(x, Ax) + f(x, (1 - \rho)Ax) = -f(Ax, x)$ that is $f(x, Ax) = 0$. This implies that $R' \oplus R''$ is a totally isotropic space which contradicts the regularity of $S_L{}^{\perp}$.

(ii) Let $p = n + 2$ where n is odd. We again put $R = \operatorname{rad} W$ and consider several possibilities for the dimensions of W and R.

a) $\dim W = n - 1$. According to lemma 3 and corollary 1, $\dim W - \dim R$ is even. Since $\dim R \leq \dim W_V{}^{\perp} = 1$, $R = 0$.

b) dim $W = n - 2$. By an argument similar to the one in a), $\dim R \neq 2$. Let us suppose that $\dim R = 1$ and apply induction on n.

Let, firstly, $n = 3$ that is $W = R$. We denote by B_0 the restriction of B to V ($B_0 = \rho A \rho$). As it follows from Lemma 3, any non-zero vector of R is an eigenvector of B_0 associated with an eigenvalue i where $i^2 = -1$. Since B_0 is a skew-symmetric operator, it has also the eigenvalue $-i$. Let $w \in V$ be an eigenvector associated with $-i$. We have $C^*Cw = \rho w + B^2 w = 0$. Since under the assumptions on the dimensions of L, V, and W the operator C is surjective, it follows that C^* is injective and $Cw = 0$. That implies that $Aw = Bw + Cw = iw \in V$ and $w \in W$, which contradicts the equality $W = R$.

Let, now, $n > 3$. We take an arbitrary $a \in W$ such that $f(a, a) \neq 0$ and put $b = Aa$. As it follows from Lemma 3, the space Z spanned by a and b is A-invariant and regular. Thus the space $Z_L{}^{\perp}$ is A-invariant and regular. The induction hypothesis implies that $W \cap Z_L{}^{\perp}$ is a regular space. Since $W = Z \oplus (W \cap Z_L{}^{\perp})$, it is also regular.

COROLLARY 2. *Under the conditions of lemma* 3, $\dim(V \cap A^{-1}(V))$ *is even.*

Remark 1. This result holds for $F = \mathbb{R}$ without any restrictions on n and p. This is not so for an arbitrary F even if $p = n + 2$ and n is even.

Example. Let $F = GF(5)$, $L = F^4$ and $f(x, x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ where $x = (x_1, x_2, x_3, x_4)^t$, $x_i \in F$. Let $V = \{(x_1, x_2, 0, 0)^t\} \subset L$ and let A be the operator on L given by the matrix

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 2 & 0 & 0 \end{pmatrix}.$$

Then A satisfies (10, 11) but $W = V \cap A^{-1}(V) = \{(x, -x, 0, 0)^t\}$, $x \in F$; $\dim W = 1$. Here $p = 4$, $n = 2$.

4. Nonexistence of pairings of type [4, 4k + 1, 4k + 3]

In this section we prove the main result of this paper.

THEOREM 1. *No pairing of type* $[4, 4k + 1, 4k + 3]$ $(k = 1, 2, \cdots)$ *can exist over any field F.*

Proof. Let us suppose that, on the contrary, there exists a field F, a positive integer k, regular quadratic spaces V and W over F of dimensions $4k + 1$ and $4k + 3$, and four operators $A_i: V \to W$, $i = 1, 2, 3, 4$, satisfying (3, 4). We put $V_i = \operatorname{Im} A_i$, $V_{ij} = V_i \cap V_j$, $i \neq j$, $i, j = 1, 2, 3, 4$. If $i \neq j$ we can apply corollary 2 to the operator $A_jA_i^*$ and the subspace V_i of W. According to the equality $A_jA_i^* = (A_iA_{j|V_i}^*)^{-1}$ and corollary 2, $\dim(V_i \cap A_jA_i^*(V_i))$ is even. Since $A_jA_i^*(V_i) = V_j$, we conclude that $\dim V_{ij} = 4k$ and, consequently, $\dim(V_i + V_j) = 4k + 2$. We put $R = \operatorname{rad}(V_i + V_j)$. Then $\dim R \leq \dim(V_i + V_j)^\perp = 1$. If S is a subspace of $V_i + V_j$ such that $V_i + V_j = R \oplus S$ and ρ is the projection of $V_i + V_j$ on S along R, then ρ preserves the quadratic form of W (cf. lemma 1). This implies that the operators ρA_i and ρA_j define a pairing of type $[2, 4k + 1, 4k + 2 - \dim R]$ and therefore $R = 0$. Let us fix now $h \in \{1, 2, 3, 4\}$, $h \neq i$, $h \neq j$, and consider $\bar{V} = V_i + V_j + V_h$. If $\bar{V} = V_i + V_j$ then $\bar{V}$ is a regular space and A_i, A_j, A_h define a pairing of type $[3, 4k + 1, 4k + 2]$. This contradicts [2]. Consequently, $\bar{V} \neq V_i + V_j$ that is $\bar{V} = W$. Let us consider now the inclusion $V_{ij} + V_h \subset (V_i + V_h) \cap (V_j + V_h)$. The above calculation implies that $\dim(V_{ij} + V_h) = 4k + 1$; that is, $V_{ij} \subset V_h$. It follows that $V_0 = \cap_{k=1}^4 V_k = V_{ij}$. Therefore $\dim V_0 = 4k$ and V_0 is a regular space. Again applying lemma 3 to the operator $A_jA_i^*$ and the space V_i for an arbitrary ordered pair (i, j) we conclude that $U = A_i^{-1}(V_0)$ does not depend on i and that the operators A_i define a pairing of type $[4, 4k, 4k]$. Considering the orthogonal complements $U_V^\perp$ and $(V_0)_W^\perp$ we obtain a pairing of type $[4, 1, 3]$, which is impossible. This contradiction completes the proof.

UNIVERSITY OF OREGON

REFERENCES

[1] J. ADEM, *On the Hurwitz problem over an arbitrary field* I, Bol. Soc. Mat. Mexicana **25** (1980), 29–51.

[2] ———, *On the Hurwitz problem over an arbitrary field* II, Bol. Soc. Mat. Mexicana, **26** (1981), 29–41.

[3] F. BEHREND, *Über Systeme reeler algebraischer Gleichungen*, Compositio Math. **7** (1939), 1–19.

[4] H. HOPF, *Ein topologischer Beitrag zur reelen Algebra*, Comment. Math. Helv. **13** (1940/41), 219–239.

[5] T. Y. LAM, The Algebraic Theory of Quadratic Forms, W. A. Benjamin, Inc., Reading, Massachusetts, 1973.

[6] D. B. SHAPIRO, *Spaces of Similarities* IV, Pacific J. Math. **69** (1977), 223–244.

[7] ———, Products of sums of squares, preprint 1982.

[8] S. YUZVINSKY, *Orthogonal pairings of Euclidean spaces*, Michigan Math. J. **28** (1981), 131–145.