C.R. Math. Rep. Acad. Sci. Canada

Vol. XV, No. 6 **December 1993 décembre**

CONTENTS

C.R. Math. Rep. Acad. Sci. Canada - Vol. XV, No. 6, December 1993 décembre

CUBIC CURVES RELATED TO A QUADRANGLE

H.S.M. Coxeter, F.R.S.C.

By counting the number of terms in the general cubic polynomial in x, y, z, we see that a unique cubic curve can usually be drawn through 9 coplanar points, and a 'pencil' (∞^1) of cubic curves through 8. An exceptional situation arises when the 9 points are the 3×3 intersections of two such curves, say $U = 0$ and $V = 0$; for then the 9 points lie on all the curves of the pencil $U + \lambda V = 0$, which is the pencil determined by any 8 of the 9. Thus eight points of general position determine a ninth 'associated' point, and the same pencil is determined by any eight of these *nine associated points*. One example consists of the vertices of a triangle ABC along with the incentre I, the excentres I_a, I_b, I_c, and any two *isogonal conjugate* points such as the circumcentre O and the orthocentre H, or Poncelet's circular points at infinity, which will be seen to have surprisingly simple trilinear coordinates.

1. Projective Geometry

In a projective plane, any four points, no three collinear, are the vertices of a *quadrangle* and may be taken to have homogeneous coordinates

(1.1) $$(1,\ \pm 1,\ \pm 1)$$

so that the quadrangle's 'diagonal triangle' is the triangle of reference

(1.2) $$(1,\ 0,\ 0)\quad (0,\ 1,\ 0)\quad (0,\ 0,\ 1)$$

(Coxeter 1992, pp. 180, 190). The quadrangle determines a pencil (or 'one-parameter family') of conics

$$ux^2 + vy^2 + wz^2 = 0, \qquad u + v + w = 0$$

all passing through the four vertices. There is one such conic for each point (u, v, w) on the line

$$x + y + z = 0 .$$

With respect to such a conic, the condition for (x, y, z) and (x', y', z') to be conjugate points is

$$uxx' + vyy' + wzz' = 0 .$$

Hence, if

$$xx' = yy' = zz' ,$$

those two points are conjugate with respect to every conic in the pencil. In the terminology of Baker (1943, p. 56) they are *conjugate with respect to the quadrangle*. Such conjugacy yields an involutory 'quadratic transformation' (Todd 1946, p. 198) which takes each point (x, y, z) to (yz, zx, xy), and each line to a conic circumscribing the triangle of reference.

It follows that the locus of pairs of conjugate points whose joins pass through a fixed point (p, q, r) is the cubic curve

$$\begin{vmatrix} p & q & r \\ x & y & z \\ yz & zx & xy \end{vmatrix} = 0$$

or

$$px(y^2 - z^2) + qy(z^2 - x^2) + rz(x^2 - y^2) = 0 \tag{1.3}$$

(Rubio 1989, p. 165), which passes through seven further fixed points, (1.1) and (1.2).

Since the last four of these seven points are *self*-conjugate, the four lines joining them to (p, q, r) are are *tangents*. Similarly, the four tangents

$$qy = rz, \quad rz = px, \quad px = qy , \qquad (q^2 - r^2)px + (r^2 - p^2)qy + (p^2 - q^2)rz = 0 ,$$

at $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, (p,q,r), all pass through the point

$$T = (p^{-1}, q^{-1}, r^{-1}),$$

conjugate to (p,q,r).

Since there is one such cubic curve for each point (p,q,r) in the plane, there is altogether a *bundle* of ∞^2 cubic curves through those seven points: a special case of the bundle through seven points of general position. Our bundle is reduced to a pencil (∞^1) when (p,q,r) is restricted to lie on a fixed line E. Then the nine *associated* points that lie on all the curves of the pencil consist of the above-mentioned seven along with the two conjugate points on E. In other words, any two conjugate points form, with the seven, a set of nine associated points.

2. Euclidean Geometry

In the case of (homogeneous) *trilinear* coordinates in the Euclidean plane, the four points

$$(1, 1, 1), \quad (-1, 1, 1), \quad (1, -1, 1), \quad (1, 1, -1)$$

are the incentre and excentres of the triangle of reference, and 'conjugates' are *isogonal* conjugates (Eddy and Wilker 1992). Although E may be *any* line, two positions are especially interesting.

If E is the *line at infinity* $[a, b, c]$ or $[\sin A, \sin B, \sin C]$, so that $ap + bq + cr = 0$, the last two of the nine associated points are Poncelet's *circular points* at infinity, and we have a pencil of 'circular' cubic curves. If, on the other hand, E is the *Euler line*, the last two of the nine are the *circumcentre* and the *orthocentre*,

$$(\cos A, \cos B, \cos C) \quad \text{and} \quad (\sec A, \sec B, \sec C)$$

(Coxeter 1992, p. 196).

The one common member of these two pencils is the *Neuberg cubic*, for which we can compute the values of p, q, r in (1.3) by making them satisfy both the equations

$$p \sin A + q \sin B + r \sin C = 0$$

and

$$p \sin 2A \sin(B-C) + q \sin 2B \sin(C-A) + r \sin 2C \sin(A-B) = 0 .$$

Eliminating $r \sin C$, we find

$$\begin{aligned} 0 &= p \sin 2A \sin(B-C) + q \sin 2B \sin(C-A) - 2(p \sin A + q \sin B) \cos C \sin(A-B) \\ &= p \sin A\{-\cos(B+C)\sin(B-C) + \cos(A+B)\sin(A-B)\} \\ &\quad + q \sin B\{-\cos(C+A)\sin(C-A) + \cos(A+B)\sin(A-B)\} , \end{aligned}$$

$$p \sin A\{2 \sin 2B - \sin 2C - \sin 2A\} = q \sin B\{2 \sin 2A - \sin 2B - \sin 2C\} ,$$

$$p\{2 \cos B - \cos(C-A)\} = q\{2 \cos A - \cos(B-C)\} ,$$

$$p(\cos B - 2 \cos C \cos A) = q(\cos A - 2 \cos B \cos C) .$$

Thus we may choose

$$p = \cos A - 2 \cos B \cos C , \qquad q = \cos B - 2 \cos C \cos A$$

and similarly

$$r = \cos C - 2 \cos A \cos B .$$

This Neuberg cubic (Neuberg 1885, Brown 1925) contains surprisingly many notable points in addition to $A, B, C, I, I_a, I_b, I_c, O, H$ and the circular points; for instance, it contains A', B', C', the images of A, B, C by reflection in BC, CA, AB, and the six points A_1, B_1, C_1, A_2, B_2, C_2 which form equilateral triangles with BC, CA, AB

(see Figure 1). Further points on the same curve were observed by Moore & Neelley (1925, p. 242) and by Cundy (1994). Since (p, q, r) is the point at infinity on the Euler line, the real asymptote of the curve is parallel to that line. Brown (1925, pp. 112, 114) proved that these two lines are parallel also to the cubic's tangents at I, I_a, I_b, I_c, and that its tangents at A, B, C are TA, TB, TC, where T lies on the circumcircle ABC and also on the cubic itself and its asymptote.

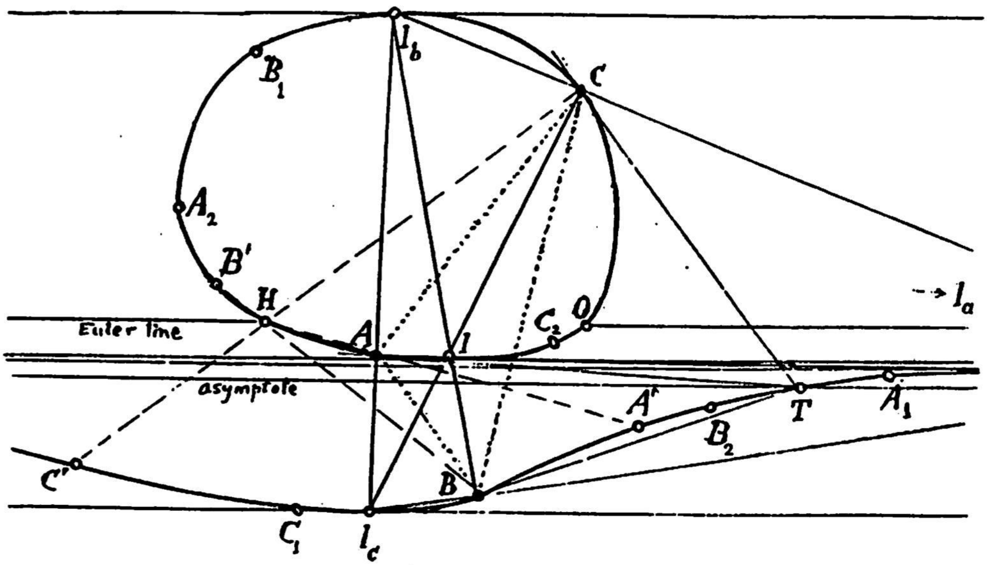

FIGURE 1. The Neuberg cubic

Some work of Robson (1947, p. 180) suggests that the circular points have the surprisingly simple trilinear coordinates

$$(e^{\pm Bi}, \quad e^{\mp Ai}, \quad -1).$$

Since $a\cos B + b\cos A = c$ and $a\sin B - b\sin A = 0$, it is clear that these coordinates satisfy both the equations

$$ax + by + cz = 0 \quad \text{and} \quad ax^{-1} + by^{-1} + cz^{-1} = 0$$

for the line at infinity and the circumcircle of ABC (Coxeter 1992, p. 195).

References

H.F. Baker 1943. *An Introduction to Plane Geometry*, Cambridge University Press.

B.H. Brown 1925. The 21-point cubic, *Amer. Math. Monthly* **32**, 110–115, 247.

H.S.M. Coxeter 1992. *The Real Projective Plane*, 3rd ed., Cambridge University Press.

H.M. Cundy and C.F. Parry 1994. Cubics associated with a triangle. To appear.

H.L. Dorwart 1978. The Neuberg cubic: A nostalgic look, *California Mathematics* **3**, 31–38.

R.H. Eddy and J.B. Wilker 1992. Plane mappings of isogonal-isotomic type, *Soochow Journal of Math.* **18**, 123–126.

T.W. Moore and J.H. Neelley 1925. The circular cubic on twenty-one points of a triangle, *Amer. Math. Monthly* **32**, 241–246.

J. Neuberg 1885. Mémoire sur le tétraèdre, *Supplément V, Mathesis* 1885.

A. Robson 1947. *An Introduction to Analytical Geometry*, II, Cambridge University Press.

J.A. Todd 1946. *Projective and Analytical Geometry*, Pitman, New York.

Pablo Rubio 1989. Cubic lines relative to a triangle, *Journal of Geometry* **34**, 152–171.

Department of Mathematics
University of Toronto
Toronto, Ontario, Canada
M5S 1A1

Received December 9, 1993

C.R. Math. Rep. Acad. Sci. Canada - Vol. XV, No. 6 December 1993 décembre

A NOTE TO EQUILIBRIA FOR $\mathcal{U}$-MAJORIZED PREFERENCES

XIAN-ZHI YUAN

Presented by G.F.D. Duff, F.R.S.C.

Abstract: The purpose of this note is to give a general existence theorem of maximal elements for a new type of preference correspondences which are $\mathcal{U}$-majorized. As an application, an existence theorem of equilibria for a qualitative game is obtained in which the preferences are $\mathcal{U}$-majorized with an arbitrary (countable or uncountable) set of players and without compactness assumption on their domains in Hausdorff locally convex topological vector spaces. Finally, we obtain an existence theorem of equilibria for generalized games in which the intersection of constraint and preference mappings are $\mathcal{U}$-majorized and the set of players is any (countable or uncountable) set.

1. Introduction

The objective of this note is to give some existence theorems of maximal elements and equilibria in qualitative games and generalized games without the compactness (or paracompactness) assumption on the domain of the preferences which are majorized by upper semicontinuous correspondences instead of being majorized by correspondences which have lower open sections (e.g. see [3-4, 6, 8-9, 15-21] etc). Our intention is to merely illustrate a certain technique that we think will be of use in various problems of mathematical economics. Many other results of the type proved here may be proved under more general conditions.

Now we give some notions. Let A be a set, we shall denote by 2^A the family of all subsets (including the empty subset $\emptyset$) of A. If A is a subset of a topological space X, we shall denote by $cl_X(A)$ the closure of A in X. If A is a subset of a vector space, we shall denote by coA the convex hull of A. If A is a non-empty subset of a topological vector space E and $S, T : A \to 2^E$ are correspondences, then coT, $T \cap S : A \to 2^E$ are correspondences defined by $(coT)(x) = coT(x)$ and $(T \cap S)(x) = T(x) \cap S(x)$ for each $x \in A$, respectively. If X and Y are topological spaces and $T : X \to 2^Y$ is a correspondence, then (1) T is said to be upper semicontinuous at $x \in X$ if for any open subset U of Y containing $T(x)$, the set $\{z \in X : T(z) \subset U\}$ is an open neighborhood of x in X; (2) T is upper semicontinuous (on X) if T is upper semicontinuous at x for each $x \in X$; (3) the Graph of T, denoted by Graph(T), is the set $\{(x, y) \in X \times Y : y \in T(x)\}$; (4) the correspondence $\overline{T} : X \to 2^Y$

1991 MATHEMATICS SUBJECT CLASSIFICATION: 47H04, 47N10, 52A07, 90A14, 90D06.
KEY WORDS: $\mathcal{U}$-majorized, upper (lower) semicontinuous, maximal element, equilibrium, qualitative game, generalized game.

is defined by $\overline{T}(x) = \{y \in Y : (x, y) \in cl_{X\times Y}\text{Graph}(T)\}$ (here, the set $cl_{X\times Y}Graph(T)$ is called the adherence of the Graph T) and (5) the correspondence $clT : X \to 2^Y$ is defined by $clT(x) = cl_Y(T(x))$ for each $x \in X$. It is east to see that $clT(x) \subset \overline{T}(x)$ for each $x \in X$. We remark here that in defining the upper semicontinuity of T at $x \in X$, we do not require that $T(x)$ be non-empty. According to the definition of adherence of the Graph T, it is easy to see if the mapping T has convex values, then $\overline{T}$ also has closed convex values.

Let X be a topological space, Y be a non-empty subset of a vector space E, $\theta : X \to E$ be a map and $\phi : X \to 2^Y$ be a correspondence. Then (1) ϕ is said to be of class $\mathcal{U}_\theta$ if (a) for each $x \in X$, $\theta(x) \notin \phi(x)$ and (b) ϕ is upper semicontinuous with closed and convex values in Y; (2) ϕ_x is a $\mathcal{U}_\theta$-majorant of ϕ at x if there is a open neighborhood $N(x)$ of x in X and $\phi_x : N(x) \to 2^Y$ such that (a) for each $z \in N(x)$, $\phi(z) \subset \phi_x(z)$ and $\theta(z) \notin \phi_x(z)$ and (b) ϕ_x is upper semicontinuous with closed and convex values; (3) ϕ is said to be $\mathcal{U}_\theta$-majorized if for each $x \in X$ with $\phi(x) \neq \emptyset$, there exists a $\mathcal{U}_\theta$-majorant ϕ_x of ϕ at x. We remark that when $X = Y$ and $\theta = I_X$, the identity map on X, our notions of a $\mathcal{U}_\theta$-majorant of ϕ at x and a $\mathcal{U}_\theta$-majorized correspondence are generalization of upper semicontinuous correspondences which are irreflexive (i.e., $x \notin \phi(x)$ for all $x \in X$) and have closed convex values.

In this paper, we shall deal mainly with either the case (I) $X = Y$ and is a non-empty convex subset of the topological vector space E and $\theta = I_X$, the identity map on X, or the case (II) $X = \Pi_{i\in I}X_i$ and $\theta = \pi_j : X \to X_j$ is the projection of X onto X_j and $Y = X_j$ is a non-empty convex subset of a topological vector space. In both cases (I) and (II), we shall write $\mathcal{U}$ in place of $\mathcal{U}_\theta$.

Let I be a (countable or uncountable) set of players. A generalized game is a family $\Gamma = (X_i; A_i, B_i; P_i)_{i\in I}$ of quadruples $(X_i; A_i, B_i; P_i)$ where for each $i \in I$, X_i is a topological space, $A_i, B_i : X := \Pi_{j\in I}X_j \to 2^{X_i}$ are constraint correspondences and $P_i : X \to 2^{X_i}$ is a preference correspondence. Following Tan and Yuan [16]: an equilibrium point for Γ is a point $x^* \in X$ such that for each $i \in I$, $x_i^* = \pi_i(x^*) \in \overline{B_i}(x^*)$ and $A_i(x^*) \cap P_i(x^*) = \emptyset$ where $\pi_i : X \to X_i$ is the projection. We remark that when $\overline{B_i}(x^*) = cl_{X_i}B_i(x^*)$ (which is the case when B_i has a closed graph in $X \times X_i$; in particular, when $cl_{X_i}B_i$ is upper semicontinuous with closed values) for each $i \in I$, our definition of equilibrium points for a generalized game coincides with that of Borglin and Keiding [4]. Let $A_i(x) = B_i(x) = X_i$ for each $x \in X$, then generalized game is a family $\Gamma = (X_i; A_i, B_i; P_i)_{i\in I}$ is also called qualitative game (e.g., see Gale and Mas-Colell [9]). For each $i \in I$, let A_i be a non-empty subset of X_i; if $i \in I$ is arbitrarily fixed, we define: $\Pi_{j\neq i, j\in I}A_j \otimes A_i = \{x = (x_k)_{k\in I} \in X : x_k \in A_k \text{ for each } k \in I\}$.

2. Existence of Maximal Elements

We first need the following two Lemmas:

Lemma 2.1. Let X and Y be two topological spaces, A be a closed (respectively, open) subset of X. Suppose $F_1 : X \to 2^Y$, $F_2 : A \to 2^Y$ are lower semicontinuous (respectively, upper semicontinuous) such that $F_2(x) \subset F_1(x)$ for all $x \in A$. Then the map

$F : X \to 2^Y$ defined by

$$F(x) = \begin{cases} F_1(x), & \text{if } x \notin A; \\ F_2(x), & \text{if } x \in A \end{cases}$$

is also lower semicontinuous (respectively, upper semicontinuous).

The following results is essentially due to Hildenbrand [10, p.23-24] (see also [13, Theorem 7.3.10, p.86]):

Lemma 2.2. Let X be a topological space and Y be a normal space. If $F, G : X \to 2^Y$ have closed values and are upper semicontinuous at $x \in X$, then $F \cap G$ is also upper semicontinuous at x.

We remark here that in Lemma 2.2, we do not require $F(x) \cap G(x) \neq \emptyset$.

Theorem 2.3. Let X be a paracompact space and Y be a non-empty normal subset of a topological vector space E. Let $\theta : X \to E$ and $P : X \to 2^Y \setminus \{\emptyset\}$ be $\mathcal{U}$-majorized. Then there exists a correspondence $\Psi : X \to 2^Y \setminus \{\emptyset\}$ of class $\mathcal{U}$ such that $P(x) \subset \Psi(x)$ for each $x \in X$.

Proof: Since P is $\mathcal{U}$-majorized, for each $x \in X$, let $N(x)$ be an open neighborhood of x in X and $\psi_x : N(x) \to 2^Y \setminus \{\emptyset\}$ be such that (1) for each $z \in N(x)$, $P(z) \subset \psi_x(z)$ and $\theta(z) \notin \psi_x(z)$ and (2) ψ_x is upper semicontinuous with closed and convex values. Since X is paracompact and $X = \cup_{x \in X} N(x)$, by Theorem VIII.1.4 [7, p.162], the open covering $\{N(x)\}$ of X has an open precise neighborhood-finite refinement $\{N'(x)\}$. For each $x \in X$, define $\psi'_x : X \to 2^Y \setminus \{\emptyset\}$ by

$$\psi'_x(z) = \begin{cases} \psi_x(z), & \text{if } z \in N'(x); \\ Y, & \text{if } z \notin N'(x), \end{cases}$$

then ψ'_x is also upper semicontinuous on X by Lemma 2.1 such that $P(z) \subset \psi'_x(z)$ for each $z \in X$.

Now define $\Psi : X \to 2^Y \setminus \{\emptyset\}$ by $\Psi(z) = \cap_{x \in X} \psi'_x(z)$ for each $z \in X$. Clearly, Ψ has closed and convex values and $P(z) \subset \Psi(z)$ for each $z \in X$. Let $z \in X$ be given, then $z \in N'(x)$ for some $x \in X$ so that $\psi'_x(z) = \psi_x(z)$ and hence $\Psi(z) \subset \psi_x(z)$; as $\theta(z) \notin \psi_x(z)$, we must also have that $\theta(z) \notin \Psi(z)$. Thus $\theta(z) \notin \Psi(z)$ for all $z \in X$.

Now we shall show that Ψ is upper semicontinuous. For any given $u \in X$, then there exists an open neighborhood M_u of u such that the set $\{x \in X : M_u \cap N(x) \neq \emptyset\}$ is finite, say $= \{x(u,1), \cdots, x(u,n(u))\}$. Thus we have that $\Psi(w) = \cap_{x \in X} \psi'_x(w) = \cap_{i=1}^{n(u)} \psi'_{x(u,i)}(w)$ for all $w \in M_u$. By Lemma 2.2, $\Psi : X \to 2^Y$ is upper semicontinuius at u. Hence Ψ is of class $\mathcal{U}$. □

We now prove the following theorem concerning the existence of a maximal element:

Theorem 2.4. Let X be a non-empty convex subset of a Hausdorff locally convex topological vector space and D be a non-empty compact subset of X. Let $P : X \to 2^D$ be $\mathcal{U}$-majorized (i.e.. $\mathcal{U}_{\theta_X}$-majorized). Then there exists a point $x \in coD$ such that $P(x) = \emptyset$.

Proof: Suppose the contrary, i.e., for all $x \in coD$, $P(x) \neq \emptyset$. Then for each $x \in coD$, $P(x) \neq \emptyset$ and coD is also paracompact by Lemma 1 of [9, p.206] (see also [14, p.49]). Now applying Theorem 2.3, there exists a correspondence $\Psi : coD \to 2^D$ of class $\mathcal{U}$ such that for each $x \in coD$, $P(x) \subset \Psi(x)$. Since Ψ is upper semicontinuous with non-empty closed and convex values, by a fixed point Theorem of Himmelberg [11, Theorem 2, p.206], there exists $x \in coD$ such that $x \in \Psi(x)$. This contradicts that Ψ is of class $\mathcal{U}$. Hence the conclusion must holds. □

3. Existence of Equilibria in Locally Convex spaces

In this section, as an application of Theorem 2.4, we shall first give an existence of equilibria of qualitative games in which the preferences are $\mathcal{U}$-majorized. Finally, an existence theorem of equilibria of generalized games in which the set of players is any (countable or uncountable) set is obtained.

Theorem 3.1. Let $\Gamma = (X_i, P_i)_{i\in I}$ be a qualitative game such that for each $i \in I$: (a) X_i is a non-empty convex subset of a Hausdorff locally convex topological vector space E_i and D_i is a non-empty compact subset of X_i; (b) the set $E^i = \{x \in X : P_i(x) \neq \emptyset\}$ is open in X; (c) $P_i : E^i \to 2^{D_i}$ is $\mathcal{U}$-majorized; (d) there exists a non-empty compact and convex subset F_i of D_i such that $F_i \cap P_i(x) \neq \emptyset$ for each $x \in E^i$.
Then there exists a point $x \in X$ such that $P_i(x_i) = \emptyset$ for all $i \in I$.

Proof: Since D_i is a non-empty compact subset of X_i for each $i \in I$, the set $D = \Pi_{i\in I} D_i$ is also a non-empty compact subset of X. Now for each $x \in X$, let $I(x) = \{i \in I : P_i(x) \neq \emptyset\}$. Define a correspondence $P : X \to 2^D$ by

$$P(x) = \begin{cases} \cap_{i\in I(x)} P_i'(x), & \text{if } I(x) \neq \emptyset; \\ \emptyset, & \text{if } I(x) = \emptyset, \end{cases}$$

where $P_i'(x) = \Pi_{j\neq i, j\in I} F_j \otimes P_i(x)$ for each $x \in X$.

Then for each $x \in X$ with $I(x) \neq \emptyset$, $P(x) \neq \emptyset$. Let $x \in X$ be such that $P(x) \neq \emptyset$. Fix an $i \in I(x)$. By assumption (c), there exist an open neighborhood $N(x)$ of x in E^i and $\varphi_i : N(x) \to 2^{D_i}$ such that (i) for each $z \in N(x)$, $P_i(z) \subset \varphi_i(z)$ and $\pi_i(z) \notin \phi_i(z)$ and (ii) ϕ_i is upper semicontinuous with closed and convex values. Note that by (b), $N(x)$ is also an open neighborhood of x in X and for each $z \in N(x)$, $P_i(z) \neq \emptyset$ so that $i \in I(z)$ for each $z \in N(x)$. Now we define $\Phi_x : N(x) \to 2^D$ by $\Phi_x(z) = \Pi_{j\neq i, j\in I} F_j \otimes \phi_i(z)$ for each $z \in N(x)$. It is easy to see that Φ_x is an $\mathcal{U}$-majorant of P at x. Thus P is $\mathcal{U}$-majorized. Now by Theorem 2.4, there exists a point $x \in coD \subset X$ such that $P(x) = \emptyset$ which implies that $P_i(x) = \emptyset$ for all $i \in I$. □

The following is an existence theorem of equilibrium points for generalized games in which the intersection of constraint and preference correspondences are $\mathcal{U}$-majorized.

Theorem 3.2. Let $\mathcal{G} = (X_i; A_i, B_i, P_i)_{i\in I}$ be a generalized game where I is any (countable or uncountable) set of players such that

(a) for each $i \in I$, X_i is a non-empty convex subset of a locally convex Hausdorff topological vector space E_i and D_i is a non-empty compact subset of X_i;

(b) for each $i \in I$ and for each $x \in X$, $A_i(x)$ is non-empty, $A_i(x) \subset \overline{B_i}(x)$ and $B_i(x)$ is convex;

(c) for each $i \in I$, the set $E^i = \{x \in X : (A_i \cap P_i)(x) \neq \emptyset\}$ is paracompact and open in X;

(d) for each $i \in I$, $A_i \cap P_i$ is $\mathcal{U}$-majorized ;

(e) for each $i \in I$, $B_i(x) \subset D_i$ for each $x \in X$.

Then $\mathcal{G}$ has an equilibrium point in X, i.e., there exists a point $\hat{x} = (\hat{x}_i)_{i \in I} \in X$ such that for each $i \in I$, $\hat{x}_i \in \overline{B_i}(\hat{x})$ and $A_i(\hat{x}) \cap P_i(\hat{x}) = \emptyset$.

Proof: Let $D = \Pi_{i \in I} D_i$. Then D is a non-empty compact subset of X by (a). Define a mapping $B : X \to 2^D$ by $B(x) = \Pi_{i \in I}\overline{B_i}(x)$ for each $x \in X$, then B is upper semicontinuous since $B(X) = \cup_{x \in X} B(x) \subset D$ and B has a closed graph. For each $i \in I$. Let $I_0 = \{i \in I : E^i \neq \emptyset\}$. If $I_0 = \emptyset$, then $E^i = \emptyset$ for all $i \in I$ so that $(A_i \cap P_i)(x) = \emptyset$ for all $x \in X$. On the other hand, since B is upper semicontinuous with closed and convex values on X. By Theorem 2 of Himmelberg [11, p.206], there exists $x \in X$ such that $x \in B(x)$. It follows that $x_i \in \overline{B_i}(x)$ for all $i \in I$ and hence x is an equilibrium point of $\mathcal{G}$. Therefore we may assume that $I_0 \neq \emptyset$.

Case 1: Suppose $i \in I_0$. Note that E^i is paracompact by (c), and by (d) and Lemma 2, there exists an upper semicontinuous mapping $\psi_i : E^i \to 2^{X_i} \setminus \{\emptyset\}$ such that for each $x \in E^i$, (i) $\psi_i(x)$ is closed and convex, (ii) $\pi_i(x) \notin \psi_i(x)$ and (iii) $A_i(x) \cap P_i(x) \subset \psi_i(x)$. Since $\overline{B_i} : X \to 2^{D_i} \setminus \{\emptyset\}$ is upper semicontinuous with closed and convex values, the mapping $\psi_i \cap \overline{B_i} : E^i \to 2^{D_i} \setminus \{\emptyset\}$ is also upper semicontinuous with non-empty closed and convex values by Theorem 7.3.10 of Klein and Thompson [13, p.86]. Define a correspondence $\phi_i : X \to 2^{D_i} \setminus \{\emptyset\}$ by

$$\phi_i(x) = \begin{cases} \overline{B_i}(x), & \text{if } x \notin E^i; \\ (\psi_i \cap \overline{B_i})(x), & \text{if } x \in E^i. \end{cases}$$

Then Lemma 2.1 implies that ϕ_i is upper semicontinuous with non-empty closed and convex values.

Case 2: Suppose $i \in I \setminus I_0$. Define a correspondence $\phi : X \to 2^{D_i} \setminus \{\emptyset\}$ by $\phi_i = \overline{B_i}(x)$ for each $x \in X$. Then ϕ is upper semicontinuous with non-empty compact and convex values.

Now we define a correspondence $\Phi : X \to 2^D$ by $\Phi(x) = \Pi_{i \in I}\phi_i(x)$ for each $x \in X$. Then Φ is also upper semicontinuous and has non-empty compact and convex values. Since $\Phi(x) \subset B(x) \subset D$ for each $x \in X$, Himmelberg's fixed fixed point theorem again (e.g., see Theorem 2 of [11, p.206]) implies that there exists a point $x \in X$ such that $x \in \Phi(x)$. It follows that $\pi_i(x) \in \overline{B_i}(x)$ for all $i \in I$; and also $x \notin E^i$ for all $i \in I_0$. Hence we also have $A_i(x) \cap P_i(x) = \emptyset$ for all $i \in I$. □

For the existence of equilibria of abstract economies (or generalized games) in which preferences are not $\mathcal{U}$-majorized in topological vector spaces or locally convex topological vector spaces, we refer to [1-9, 8-9, 12, 15-21] and the references wherein.

ACKNOWLEDGEMENT: The author would like thank Professor K. K. Tan for many helpful discussions.

References

1. C. Aliprantis and D. Brown, *Equilibria in markets with Riesz spaces of commodities*, J. Math. Econ. 11 (1983), 189-207.
2. K. J. Arrow and G. Debreu, *Existence of an equilibrium for a competitive economy*, Econometrica 22 (1954), 265-290.
3. T. Bergstrom, *Maximal elements of acyclic preference relations on compact sets*, J. Economic Theory 10 (1975), 403-404.
4. A. Borglin and H. Keiding, *Existence of equilibrium actions of equilibrium, " A note on the 'new' existence theorems"*, J. Math. Economics 3 (1976), 313-316.
5. G. Debreu, *A social equilibrium existence theorem*, Proc. Nati. Acad. Sci. U.S.A. 38 (1952), 386-393.
6. X. P. Ding, W. K. Kim and K. K. Tan, *Equilibria of non-compact generalized games with $\mathcal{L}^*$-majorized preference correspondences* 164 (1992), 508-517.
7. J. Dugundji, *Topology*, Allyn and Bacon, Inc., Boston, 1966.
8. D. Gale and A. Mas-Colell, *An equilibrium existence theorem for a general model without ordered preferences*, J. Math. Economics 2 (1975), 9-15.
9. D. Gale and A. Mas-Colell, *On the role of complete, translative preferences in equilibrium theory*, Equilibrium and Disequilibrium in Economics Theory (G. Schwödiauer, ed.), Reidel, Dordrecht, 1978, pp. 7-14.
10. W. Hildenbrand, *Core and Equilibria of a Large Economy* (1974), Princeton University Press, Princeton, New Jersey.
11. C. J. Himmelberg, *Fixed points of compact multifunctions*, J. Math. Anal. Appl. 38 (1972), 205-207.
12. W. K. Kim, *Existence of maximal element and equilibrium for a nonparacompact N-person game*, Proc. Amer. Math. Soc. 116 (1992), 797-807.
13. E. Klein and A. C. Thompson, *Theory of Correspondences: including applications to mathematical economics*, John Wiley & Sons, 1984.
14. M. Lassonde, *Fixed point for Kakutani factorizable multifunctions*, J. Math. Anal. Appl. 152 (1990), 46-60.
15. A. Mas-Colell and W. R. Zame, *Equilibrium theory in infinite dimensional spaces*, Handbook of Mathematical Economics (W. Hildenbrand and H. Sonnenschein, eds.), vol. 4, North-Holland, 1991, pp. 1835-1898.
16. K. K. Tan and X. Z. Yuan, *A minimax inequality with applications to existence of equilibrium points*, to appear in Bull. Austral. Math. Soc. 47 (1993).
17. K. K. Tan and X. Z. Yuan, *Lower semicontinuity of multivalued mappings and equilibrium points*, to appear in the Proceedings of the First World Congress of Nonlinear Analysts, Walter de Gruyter 1993.
18. E. Tarafdar, *A fixed point theorem and equilibrium point of an abstract economy* J. Math. Econ. 20 (1991), 211-218.
19. S. Toussaint, *On the existence of equilibria in economies with infinitely many commodities and without ordered preferences*, J. Econ. Theory 33 (1984), 98-115.
20. C. I. Tulcea, *On the approximation of upper-semicontinuous correspondences and the equilibriums of generalized games*, J. Math. Anal. Appl. 136 (1988), 267-289.
21. N. C. Yannelis and N. D. Prabhakar, *Existence of maximal elements and equilibria in linear topological spaces*, J. Math. Econ. 12 (1983), 233-245. Erratum 13 (1984), 305.

Department of Mathematics, Statistics and Computing Science,
Dalhousie University, Halifax, Nova Scotia. Canada, B3H 3J5.
E-mail addresses: yuan@cs.dal.ca

Received July 21, 1993

C.R. Math. Rep. Acad. Sci. Canada - Vol. XV, No. 6, December 1993 décembre

On real polynomial forms and inequalities related to triangles

M. T. McGregor and A. C. Thompson

Presented by P.A. Fillmore, F.R.S.C.

Abstract

This note establishes the following inequalities. If $x, y, z \geq 0$ and if $x + y + z = 1$ then

$$2p(1 - 2p^2)^{1/2} - p^2 \leq xy + yz + zx \leq (1 + 9p^2)/4$$

where $p = (xyz)^{1/2}$.

AMS Subject Classification: 26D05 (51M16).

1 Introduction

The purpose of this note is to establish certain inequalities for the expression

$$\sum yz := yz + zx + xy$$

subject to the condition that $\sum x := x+y+z = 1$. Here x, y and z are non-negative real numbers and the bounds involve the product xyz. In what follows we make use of the convention just outlined that $\sum$ means that we sum over each of the three variables.

The prototypes for such inequalities are

$$\sum yz \geq \sqrt{3}(xyz)^{\frac{1}{2}} \tag{1}$$

and

$$\sum yz \leq (2 + 9xyz)/7. \tag{2}$$

The first, in its homogeneous form valid for all real x, y and z

$$(yz + zx + xy)^2 \geq 3(xyz)(x + y + z). \tag{3}$$

is well-known and is equivalent to the Finsler-Hadwiger inequality [5], [1, 10.3]

$$4\Delta_1^2 \geq \sqrt{3}\Delta,$$

where Δ denotes the area of triangle ABC with sides $a = y + z$, $b = z + x$, $c = x + y$ and Δ_1 is the area of a triangle with sides $\sqrt{a}$, $\sqrt{b}$, $\sqrt{c}$. Using Heron's formula it is immediate that $\Delta^2 = xyz(x + y + z)$ and straightforward to check that $4\Delta_1^2 = xy + yz + zx$. There are a number of inequalities related to triangles which are equivalent to (3), see [7, p.114]. In fact, J.F.Rigby [8] has shown how any inequality involving three non-negative numbers x, y, z may be transformed into 6 related inequalities for triangles by a sequence of substitutions beginning with the one above. In dealing with inequalities for triangles it is customary to set the semi-perimeter $s = (a+b+c)/2 = x+y+z$ equal to 1 as was indicated initially. With this condition the arithmetic-geometric mean (AM-GM) inequality implies that

$$xyz \leq 1/27. \tag{4}$$

It is known (and easily verified) that inequality (2) follows from

$$\sum(1 - x)^{-1} \geq 9/2 \tag{5}$$

and (5) follows from the arithmetic-harmonic mean inequality applied to $1 - x$, $1 - y$, $1 - z$.

To prove inequality (3) and hence (1) we use a simple "sums of squares of real polynomials" argument, namely:

$$\left(\sum yz\right)^2 - 3xyz\left(\sum x\right) = 2^{-1}\sum x^2(y - z)^2 \geq 0.$$

It was D. Hilbert and E. Artin, see [6, pp.57–60] who made significant contributions to the study of real forms $F(x_1, x_2, \ldots, x_m)$ of degree $2n$ in the m real variables $x_1, x_2, \ldots, x_m$ with real coefficients. Hilbert completely solved the problem: "Is it true that if $F(x_1, x_2, \ldots, x_m) \geq 0$ for all real $x_1, x_2, \ldots, x_m$ then $F = \sum_i P_i^2$, where each $P_i = P_i(x_1, x_2, \ldots, x_m)$ is a homogeneous real polynomial in $x_1, x_2, \ldots, x_m$?". He showed that the answer is affirmative in just three cases: (i) $m = 2$, F of arbitrary even degree, (ii) m arbitrary, F of degree 2, (iii) $m = 3$, F of degree 4. Furthermore, he showed that in all other cases the answer is negative since there are real forms of degree $2n$ in m variables which are non-negative and yet which do not admit such a representation. Hence it is unlikely that the inequalities discussed below can be proved in the same straightforward way as (3). For a good exposition of Hilbert's result, extensions of it, and concrete examples in the crucial negative cases ($m = 3$ $n = 3$, $m = 4$ $n = 2$) see Choi and Lam [2].

J.F.Rigby [8] has given a complete analysis of homogeneous cubic polynomial inequalities in three variables. He shows that necessary and sufficient conditions for the inequality

$$\lambda\sum x^3+\mu\sum x^2(y+z)+\nu 3xyz\geq 0$$

to hold for all $x,y,z\geq 0$ are $\lambda\geq 0$, $\lambda+\mu\geq 0$, $\lambda+2\mu+\nu\geq 0$. Consequently, the homogeneous cubic inequalities which we use below are all included in the preceding statement. However, we give independent proofs. In a subsequent work [9], Rigby has also analysed the situation with homogeneous sextic polynomials in x,y,z. Our results are related to but different from his. The paper of Choi, Lam and Reznick [3] is a thorough analysis of sextic polynomials in 3 variables. The inequalities (a), (b) and (14) below all appear there.

In this paper we shall prove the following sharper upper and lower bounds for $\sum yz$:

$$\sum yz \leq (1+9xyz)/4 \tag{6}$$

$$\sum yz \geq (xyz)^{1/2}(2(1-2xyz)^{1/2}-(xyz)^{1/2}). \tag{7}$$

It is easily checked that $(1+9xyz)/4\leq(2+9xyz)/7$ and $2(1-2xyz)^{1/2}-(xyz)^{1/2}\geq\sqrt{3}$ are both equivalent to (4) so that (6) and (7) are indeed improvements on (2) and (1) respectively.

The inequalities (6), (7) and (11) (see below) were originally established using the Lagrange multiplier method. The proofs we present are more elementary in that they rely only on sums of squares of polynomial forms and the AM-GM inequality.

2 The Proofs of Some Sharper Inequalities for Triangles

(i) <u>Inequality (6)</u>

Since $(x+y+z)^2=1$ implies $\sum x^2=1-2\sum xy$ it is clear that (6) is equivalent to

$$\sum x^2\geq(1-9xyz)/2.$$

Consider the non-negative real numbers ξ,η and ζ. Since $\xi+\eta\geq 2\sqrt{\xi\eta}$ and similarly for the other terms, we have

$$(\xi+\eta)(\eta+\zeta)(\zeta+\xi)\geq 8\xi\eta\zeta; \tag{8}$$

i.e. a product is increased by concentrating the terms closer to the mean (keeping the sum constant). Now replace ξ by $(x+y-z)$, η by $(y+z-x)$ and ζ by $(z+x-y)$. Supposing (for the moment) that all three are non-negative, then

$$xyz \geq (x+y-z)(y+z-x)(z+x-y). \tag{9}$$

However, since at most one of the terms on the right can be negative and in that case (9) is trivial, the inequality is established for all non-negative x, y and z (i.e. a product is decreased by dispersing the terms away from the mean). Reformulating inequality (9) yields

$$2(\sum x^2)(\sum x) + 9xyz \geq (\sum x)^3$$

which, with $\sum x = 1$, becomes

$$2(\sum x^2) \geq 1 - 9xyz$$

as required. Inequality (9) (with strict inequality when x, y, z are not all equal) is referred to by Coxeter [4] as the Lehmus inequality. The article [4] gives a detailed account of the inequality, its history and its geometrical interpretations.

(ii) Inequality (7)

In our search for a sharper inequality than (1) we first discovered the following homogeneous sextic inequality:

$$2(\sum yz)^2(\sum x)^2 + 7(\sum yz)(\sum x)(xyz) - 9x^2y^2z^2 \geq 8xyz(\sum x)^3, \tag{10}$$

which, when $\sum x = 1$, can be rewritten as

$$2(\sum x^{-1})^2 + 7(\sum x^{-1}) - 9 \geq 8/xyz. \tag{11}$$

These inequalities can be established by the same methods as those used below but since (12) is an improvement of (11) we omit the derivations.

However, a careful examination of inequality (11) resulted in the sharper inequality

$$(\sum x^{-1})^2 + 2(\sum x^{-1}) + 9 \geq 4/xyz. \tag{12}$$

In homogeneous form we have the following equivalent sextic inequality

$$(\sum yz)^2(\sum x)^2 + 2(\sum yz)(\sum x)xyz + 9x^2y^2z^2 \geq 4xyz(\sum x)^3, \tag{13}$$

which, when expanded and rearranged, becomes

$$\sum(x^4y^2+y^4x^2)+2\sum x^3y^3+6x^2y^2z^2 \geq 2xyz(\sum x^3)+2xyz\sum(x^2y+y^2x). \qquad (14)$$

We now prove (14) by summing the following two inequalities:

$$(a) \quad 2\sum x^3y^3+6x^2y^2z^2 \geq 2xyz\sum(x^2y+y^2x),$$

$$(b) \quad \sum(x^4y^2+y^4x^2) \geq 2xyz\sum x^3.$$

To obtain (a) we begin with (9):

$$\alpha\beta\gamma \geq (\alpha+\beta-\gamma)(\beta+\gamma-\alpha)(\gamma+\alpha-\beta)$$

for non-negative real numbers α, β and γ. Expand and rearrange to obtain

$$\sum(\alpha^2\beta+\beta^2\alpha) \leq 3\alpha\beta\gamma+\sum\alpha^3.$$

Now set $\alpha = xy$, $\beta = yz$ and $\gamma = zx$ to get

$$xyz\sum(x^2y+y^2x) \leq 3x^2y^2z^2+\sum x^3y^3$$

which establishes (a). To establish (b) we observe that

$$x^4(y^2+z^2) \geq 2x^4yz.$$

Adding this to two similar terms yields

$$\sum x^4(y^2+z^2) \geq 2xyz\sum x^3$$

and (b) follows. The proof of (14), (13) and (12) is now complete.

Finally, with $E = \sum x^{-1}$ inequality (12) becomes, on completing the square,

$$(E+1)^2+8 \geq 4/xyz;$$

i.e. $(E+1)^2 \geq 4(1-2xyz)/xyz$, so that $(E+1) \geq 2(1-2xyz)^{1/2}(xyz)^{-1/2}$ and hence

$$E = \sum x^{-1} \geq 2(1-2xyz)^{1/2}(xyz)^{-1/2}-1.$$

Multiplication of both sides by xyz completes the proof of (7).

We are grateful to the referee for pointing out references [2], [3] and [4] which we regret not having been familiar with before.

References

[1] O. Bottema, R. Ž, Djordjevič, R. R. Janič, D. Š. Mitrinovič, P.M. Vasič, *Geometric Inequalities*, Gottingen, 1969.

[2] Choi, M-D. and Lam. T-Y., An old question of Hilbert, in *Conference on Quadratic Forms - 1976* (Ed. G.Orzech) Queen's Papers in Pure and Applied Mathematics 46 (1977) 385-405.

[3] Choi, M-D., Lam,T-Y., and Reznick,B., Positive sextics and Schur's inequalities, *J.Algebra* 141 (1991) 36-77.

[4] Coxeter,H.S.M., The Lehmus inequality, *Aequationes Math.* 28 (1985) 4-12.

[5] P. Finsler, H. Hadwiger, Einige Relationen im Dreieck, *Comm. Math. Helv.* 10 (1937/38) 316-326.

[6] G. H. Hardy, J. E. Littlewood, G. Polya, *Inequalities*, London, 1952.

[7] M. S. Klamkin, Sums of squares representations for triangle inequalities, *Univ. Beograd Publ. Elektrotehn. Fak. Ser. Mat. Fiz.* Nos 412-460 (1973) 113-116.

[8] J.F.Rigby, A method of obtaining related triangle inequalities, with applications, *Univ. Beograd Publ. Elektrotehn. Fak. Ser. Mat. Fiz.* Nos 412-460 (1973) 217-226.

[9] J.F.Rigby, Sextic inequalities for the sides of a triangle, *Univ. Beograd Publ. Elektrotehn. Fak. Ser. Mat. Fiz.* Nos 498-541 (1975) 51-58.

Department of Mathematics
University College of Swansea
Swansea
Wales SA2 8PP

Department of Math., Stats. & C.S.
Dalhousie University
Halifax, NS
Canada B3H 3J5

Received September 20, 1993
in revised form November 12, 1993

C.R. Math. Rep. Acad. Sci. Canada - Vol. XV, No. 6, December 1993 décembre

Lattice Dicing

R. M. Erdahl and S. S. Ryshkov

Presented by P. Ribenboim, F.R.S.C.

Abstract

A lattice dicing is an arrangement of hyperplanes with sufficient regularity so that the vertices of the resulting partition form a lattice. In this note we introduce the notion of lattice dicing and consider applications to geometry of numbers and integer programming. We classify the lattice dicings for $n \leq 5$.

A *D-family* $\mathcal{G}$ is an infinite family of equi-spaced parallel hyperplanes that partitions $\mathbf{R}^n$ into translationally equivalent slabs. A *dicing* $\mathcal{D} = \{\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_r\}$ is a finite set of such D-families that *dices* $\mathbf{R}^n$ into convex sets. In the special case where $r = n$, and the normal vectors are linearly independent, these convex sets are translationally equivalent parallelepipeds, and the vertices of the dicing form an n- dimensional lattice Γ. Gauss gave such a dual description of a lattice in his 1831 commentary on the thesis of Seeber, which marks the first application of lattices in a mathematical argument. We will therefore refer to these dicings as *Gaussian dicings.* When $r > n$ more interesting dicings are formed where the species of polytope is typically varied. If such a dicing has sufficient regularity so that the vertices form a lattice (as in the case of the Gaussian dicings), we will refer to it as a *lattice dicing.*

The purpose of this note is to introduce the notion of *lattice dicing*, and to describe briefly the possible lattice dicings in $\mathbf{R}^n$, when $n \leq 5$. As a secondary purpose, we point out how the theory of lattice dicings relates to geometry of numbers and integer programming. Further details and references can be found in [ER].

1. Maximal lattice dicings. $\mathcal{D} = \{\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_r\}$ *is a lattice dicing if it is nondegenerate and vertex regular, where these terms are defined as follows.*

1. *Among the D-families there are n with linearly independent normal vectors.*

2. *Through each vertex of the dicing there is one hyperplane from each of the D-families of* $\mathcal{D}$.

The nondegeneracy condition insures that the partition formed by $\mathcal{D}$ includes only (finite) polytopes. The consequences of vertex regularity are given by the following Theorem.

Theorem 1 *Let* $\mathcal{D}$ *be a nondegenerate dicing in* $\mathbf{R}^n$. *If* $\mathcal{D}$ *is vertex regular, the vertices* Γ *of* $\mathcal{D}$ *form an n-dimensional lattice.*

If $\mathcal{D}, \mathcal{D}'$ are two lattice dicings and $\mathcal{D}' \subset \mathcal{D}$, then the partition determined by $\mathcal{D}$ is a refinement of that determined by $\mathcal{D}'$. It is easy to show that both $\mathcal{D}, \mathcal{D}'$ have a common vertex set Γ. More generally, the lattice dicings can be ordered by inclusion. Each lattice dicing is contained in a chain that starts with a Gaussian dicing and ends with a *maximal lattice dicing*. A maximal lattice dicing has the property that a D-family cannot be added without violating the regularity condition. The dicings of a chain are obtained by removing a succession of D-families from the maximal lattice dicing, and all have a common vertex set.

The central problem in the theory of lattice dicings is to give, for each value of n, a complete description of the possible lattice dicings in $\mathbf{R}^n$, *up to affine equivalence*. By the above comments, this reduces to the problem of classifying the maximal lattice dicings.

Consider the $\binom{n+1}{2}$ integer vectors $\mathbf{d}_{01} = \mathbf{e}_1$, $\mathbf{d}_{02} = \mathbf{e}, \ldots, \mathbf{d}_{0n} = \mathbf{e}_n$, $\mathbf{d}_{12} = \mathbf{e}_2 - \mathbf{e}_1$, $\mathbf{d}_{13} = \mathbf{e}_3 - \mathbf{e}_1, \ldots, \mathbf{d}_{n-1n} = \mathbf{e}_n - \mathbf{e}_{n-1}$ where $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ is the standard basis for $\mathbf{R}^n$. For each vector $\mathbf{d}_{ij}$ let $\mathcal{G}_{ij}$ be the D-family of parallel hyperplanes given by the equations $\mathbf{d}_{ij} \cdot \mathbf{x} = z$, $z \in \mathbf{Z}$, and define $\mathcal{D}_1(n) = \{\mathcal{G}_{01}, \mathcal{G}_{02}, \ldots, \mathcal{G}_{n-1n}\}$.

Theorem 2 *For $n \geq 2$, $\mathcal{D}_1(n)$ is a maximal lattice dicing with lattice $\mathbf{Z}^n$. Moreover, any lattice dicing in $\mathbf{R}^n$ with $\binom{n+1}{2}$ D-families of parallel hyperplanes is affinely equivalent to $\mathcal{D}_1(n)$, and there are no lattice dicings with a greater number of D-families.*

Theorem 3 *For $n = 2, 3$ any maximal lattice dicing is affinely equivalent to $\mathcal{D}_1(n)$. For $n = 4$ there are two affine classes of maximal lattice dicings: $\mathcal{D}_1(4)$ with 10 D-families and $\mathcal{D}_2(4)$ with 9 D- families. For $n = 5$ there are four affine classes: $\mathcal{D}_1(5)$ with 15 D-families, $\mathcal{D}_2^1(5)$, $\mathcal{D}_2^2(5)$ with 12 D-families and $\mathcal{D}_3^1(5)$ with 10 D-families.*

A complete description of the dicings $\mathcal{D}_2(4)$, $\mathcal{D}_2^1(5)$, $\mathcal{D}_2^2(5)$, $\mathcal{D}_3^1(5)$ can be found in [ER].

2. Affine equivalence. In studying lattice dicings it is convenient to invoke affine equivalence and assume that the vertices of the dicing are given by $\mathbf{Z}^n$. Then the normal vectors to the D-families $\mathcal{G}_i$ can be taken to be primitive integer vectors $\mathbf{d}_i$, and the dicing $\mathcal{D}$ can be represented by an integer matrix

$$\mathcal{D} = [\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_r]$$

where the columns are the *dicing vectors* for $\mathcal{D}$. The D-families $\mathcal{G}_i$ are then given by $\mathbf{d}_i \cdot \mathbf{x} = z$, $z \in \mathbf{Z}$, as in the case of the dicing $\mathcal{D}_1(n)$. A dicing matrix satisfies the following three conditions:

1. *There must be n linearly independent vectors among the dicing vectors;*
2. *The nth order minors of $\mathcal{D}$ have modulus 0 or 1;*
3. *Each pair of columns of $\mathcal{D}$ is linearly independent.*

The first two conditions are equivalent to requiring that the dicing be non-degenerate and vertex regular. The third insures that each D-family is represented by a single dicing vector. The matrix representation of a dicing is not unique, since arbitrary permutations of the dicing vectors, or replacing one or more by their negatives produces additional representations of the same dicing. The matrix of a maximal dicing has the property that a column cannot be added without violating the second or third of these conditions.

3. The L-types of lattices. The *L-polytopes* of a lattice Γ form a facet to facet partition of $\mathbf{R}^n$, called an *L-partition*, and are defined as follows: *a polytope with vertices in* Γ *is an L-polytope if it can be circumscribed by an empty sphere*. By an empty sphere we mean a sphere with no elements of Γ in its interior. In his 1909 memoir on *nouvelles applications des paramètres continus à la théorie des formes quadratiques* [Vor], Voronoi established a fundamental relationship between the affine structure of L- partitions of lattices and the arithmetic theory of quadratic forms. He showed that the cone of positive quadratic forms $\mathcal{P}(n)$ can be partitioned into non-overlapping, relatively open polyhedral cones which he called *L-type domains*. The domains with full dimension $\binom{n+1}{2}$ are *general* and fit together facet to facet. The other L-type domains are *special*, and are the relatively open faces of varying dimension of the general domains.

These L-type domains have the following properties:

1. *The affine structure of the L-partitions of lattices on an L-type domain is constant.*

2. *The affine structure of the L-partitions of lattices on two distinct L-type domains agree if and only if the domains are arithmetically equivalent.*

3. *For each dimension n there is a finite number of arithmetically inequivalent L-type domains.*

Lattices are defined on positive forms in the usual way, by interpreting a form ϕ as the metrical form for a lattice Γ_ϕ. The L-partitions of lattices on a general L- type domain are simplicial, whereas those on a special L-type domain are not.

Let $\mathcal{D} = [\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_r]$ be a lattice dicing with lattice $\mathbf{Z}^n$. For each $\mathbf{d} \in \mathcal{D}$ define the form $\phi_d = (\mathbf{d} \cdot \mathbf{x})^2$.

Definition *The domain* $\Phi(\mathcal{D})$ *of the dicing* $\mathcal{D}$ *is the collection of positive forms*

$$\sum_{d \in \mathcal{D}} \lambda_d \phi_d$$

where $\lambda_d > 0$.

Theorem 4 *Every dicing domain is an L-type domain, and is simplicial. An L-type domain is a dicing domain if and only if all the vertex forms are rank one forms.*

The bound for the number of D-families in Theorem 2 is a direct consequence of this Theorem. Since any dicing domain is simplicial, and since the dimension of the space of quadratic forms is $\binom{n+1}{2}$, the number of vertex forms (hence the number of D-families) cannot exceed this value.

Most L-type domains have vertex forms that are not rank one forms, so are not dicing domains. In fact, there is an example of a general L-type domain, with lattices in $\mathbf{R}^8$, where none of the vertex forms are rank one [ER].

Theorem 5 *Let $\Phi(\mathcal{D})$ be a dicing domain. Then the L-partition of a lattice Γ_ϕ, $\phi \in \Phi(\mathcal{D})$ is affinely equivalent to the partition determined by the dicing $\mathcal{D}$.*

One can easily deduce from this Theorem that two dicings $\mathcal{D}$, $\mathcal{D}'$ with the same lattice $\mathbf{Z}^n$, are affinely equivalent if and only if the corresponding dicing domains are arithmetically equivalent.

4. Totally unimodular matrices. Let $\mathcal{D}$ be a lattice dicing with lattice $\mathbf{Z}^n$. Then any polytope determined by hyperplanes from the D-families of $\mathcal{D}$ has vertices in $\mathbf{Z}^n$, so the theory of lattices dicings has applications to integer programming.

Let $\mathcal{D} = [\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_r]$ be a dicing matrix. If $\mathbf{U}$ is an integer $n \times n$ unimodular matrix, $\mathbf{P}$ an $r \times r$ permutation matrix, $\mathbf{D}$ an $r \times r$ ± 1 diagonal matrix, then $\mathbf{U}\mathcal{D}\mathbf{P}\mathbf{D}$ is also a dicing matrix. Post multiplication by $\mathbf{PD}$ merely permutes columns, and changes the signs of the columns, so does not alter the dicing. It is convenient to refer to the class determined by the formula $\mathbf{U}\mathcal{D}\mathbf{P}\mathbf{D}$ as the *arithmetic class* of $\mathcal{D}$.

Theorem 6 Let $\mathcal{D}, \mathcal{D}'$ be two dicing matrices. Then the corresponding dicings are affinely equivalent if and only if $\mathcal{D}$ is arithmetically equivalent to $\mathcal{D}'$.

Each dicing matrix $\mathcal{D}$ contains at least one $n \times n$ unimodular submatrix, say $\mathbf{B}$. The arithmetically equivalent dicing matrix $\mathbf{B}^{-1}\mathcal{D}$ is totally unimodular since it contains the identity as an $n \times n$ submatrix, and satisfies the conditions for a dicing matrix. Hence each arithmetic class of dicing matrices contains one or more totally unimodular matrix, and we refer to this collection as an *arithmetic class* of totally unimodular matrices.

We will consider a totally unimodular matrix to be maximal if addition of a column necessarily results either in a matrix with a pair of linearly dependent columns, or a matrix which is not totally unimodular. Theorem 3 can be reformulated in terms of totally unimodular matrices as follows.

Theorem 7 *The number of arithmetic classes of maximal $n \times r$ totally unimodular matrices for* $n = 2,3,4,5$ *is given by* $1,1,2,4$.

References

[ER] R. M. Erdahl and S. S. Ryshkov, *On lattice dicing*, to appear in the European Journal of Combinatorics.

[Ga] C. F. Gauss, J. Reine Angew. Math. **20**, 312-320 (1840).

[Vor] G. F. Voronoi, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques*, J. Reine Angew. math. **133**, 79-178 (1908); **134**, 198-287 (1908); **136**, 67-178 (1909).

Queen's University
Canada

Steklov Institute
Moscow

Received October 20, 1993

Ladder Operators For q^{-1}-Hermite Polynomials

Mourad E. H. Ismail

Presented by L. A. Lorch F.R.S.C.

Abstract. We compute raising and lowering operators and derive Rodrigues type formulas for the q^{-1}-Hermite polynomials and show that these polynomials are solutions of q-Sturm-Liouville problems. We also give two different Rodrigues formulas and exhibit two distinct q-Sturm-Liouville equations satisfied by the q^{-1}-Hermite polynomials.

1991 Mathematics Subject Classification: Primary 33D45.

Key words and phrases. Rodrigues formulas, finite difference operators, raising and lowering operators, q^{-1}-Hermite polynomials, q-Sturm-Liouville problems, weight functions.

1. Introduction. The q^{-1}-Hermite polynomials $\{h_n(x|q)\}_0^\infty$ are generated by

$$h_0(x|q) = 1, h_1(x|q) = 2x \tag{1.1}$$

and

$$h_{n+1}(x|q) = 2xh_n(x|q) - q^{-n}(1-q^n)h_{n-1}(x|q), \quad n > 0. \tag{1.2}$$

They are renormalized continuous q-Hermite polynomials with q replaced by $1/q$, [2], [5]. This terminology is in [7] but the q^{-1}-Hermite polynomials were first considered by Askey in [1]. The moment problem associated with the q^{-1}-Hermite polynomials in indeterminate when $0 < q < 1$, [10]. Ismail and Masson [6], [7] characterized the solutions of this moment problem by identifying the Stieltjes transforms of the measures that solve the q^{-1}-Hermite moment problem.

The h_n's have the generating function, [1]

$$\sum_{n=0}^{\infty} \frac{h_n(x|q)}{(q;q)_n} q^{n(n-1)/2} t^n = (-te^{\xi}, te^{-\xi}; q)_\infty, \tag{1.3}$$

where we used the notation [5]

$$(a;q)_0 := 1, \quad (a;q)_n := \prod_{k=1}^{n}(1-aq^{k-1}), \quad n = 1, 2, \cdots, \text{ or } \infty, \tag{1.4}$$

for the q-shifted factorial and [5]

$$(1.5)\qquad (a_1,\ldots,a_k;q)_n=\prod_{j=1}^{k}\prod_{r=1}^{n}(1-a_jq^{r-1}),\quad n=0,1,2,\ldots,\text{ or }\infty.$$

for the q-multishifted factorial. Analogous to the Askey-Wilson divided difference operator in [3] we define a divided difference operator $\mathcal{D}_q$ on functions defined on $(-\infty,\infty)$ by

$$(1.6)\qquad (\mathcal{D}_qf)(x):=\frac{\breve{f}(q^{1/2}e^{\xi})-\breve{f}(q^{-1/2}e^{\xi})}{(q^{1/2}-q^{-1/2})\cosh\xi},\quad x=\sinh\xi,$$

and is $\breve{f}$ given by

$$(1.7)\qquad \breve{f}(z):=f((z-1/z)/2).$$

The operator $\mathcal{D}_q$ is a lowering operator on $\{h_n(x|q)\}_0^\infty$ in the sense

$$(1.8)\qquad \mathcal{D}_qh_n(x|q)=2\frac{q^{-n/2}-g^{n/2}}{q^{-1/2}-q^{1/2}}\,h_{n-1}(x|q).$$

In this work we show how the adjoint $\mathcal{D}_q^*$ of $\mathcal{D}_q$ with respect to the inner product

$$(1.9)\qquad <f,g>:=\int_{-\infty}^{\infty}f(x)\overline{g(x)}\,\frac{dx}{\sqrt{1+x^2}}$$

gives rise to raising operators for $\{h_n(x|q)\}_0^\infty$. An operator L is a raising operator on $\{h_n(x|q)\}_0^\infty$ if there is a sequence of non zero numbers c_n such that

$$(1.10)\qquad Lh_n(x|q)=c_nh_{n+1}(x|q).$$

Each raising operator gives rise to a Rodrigues formula for $h_n(x|q)$ and to a q-Sturm-Liouville equation satisfied by the q^{-1}-Hermite polynomilas. Our main results are contained in Section 2 where we give two distinct raising operators for $h_n(x|q)$ but we believe there are infinitely many linearly independent raising operators. It is clear that every linear combination of raising operators is another raising operator. In Section 2 we also use the raising operators to show that the h_n's are solutions of q-Sturm-Liouville problems and use this fact to establish the orthogonality of the h_n's with respect to the weight functions in Askey [1] and [7], thus providing new proofs of a main result of [1] and a result of [7]. The novelty of our results lie in our demonstration that orthogonal polynomials whose moment problems do not have a unique solution may satisfy several

Rodrigues type formulas, several Sturm-Liouville type equations and may posses infinitely many raising operators.

2. Main Results. This section deals with adjoints and raising and lowering operators. The analog of integration by parts is, [4]

$$< \mathcal{D}_q f, g > = - < f, \sqrt{1-x^2}\,\mathcal{D}_q((1-x^2)^{-1/2} g(x) > . \tag{2.1}$$

Thus, [4]

$$\mathcal{D}_q^* f(x) = -\sqrt{1-x^2}\,\mathcal{D}_q\left[(1-x^2)^{-1/2} f(x)\right].$$

Let

$$w_1(x) = \frac{(1+x^2)^{-1/2}}{(-qe^{2\xi}, -qe^{-2\xi}; q)_\infty} \tag{2.2}$$

and

$$w_2(x;a) := 1/\left(ae^{\xi}, -ae^{-\xi}, \bar{a}e^{\xi}, -\bar{a}e^{-\xi}, -qe^{\xi}/a, qe^{-\xi}/a, -qe^{\xi}/\bar{a}, qe^{-\xi}/\bar{a}; q\right)_\infty, \quad \Im a \neq 0. \tag{2.3}$$

Askey [1] proved that the q^{-1}-Hermite polynomials are orthogonal with respect to $w_1(x)$ while Ismail and Masson [7] proved their orthogonality with respect to $w_2(x,a)$ for nonreal a. For other proofs see [8].

Theorem 2.1 *A raising operator for* $\{h_n(x|q)\}$ *is*

$$h_{n+1}(x|q) = \frac{(q-1)q^{-1-n/2}}{2\,w_1(x)}\mathcal{D}_q\left[w_1(x) h_n(x|q)\right] \tag{2.4}$$

Proof. A calculation using (1.3) gives

$$\frac{1}{w_1(x)}\mathcal{D}_q\left(w_1(x)\sum_{n=0}^{\infty}\frac{h_n(x|q)}{(q;q)_n}q^{n(n-1)/2}t^n\right)$$

$$= \frac{2q^{3/2}}{q-1}\,(-tq^{1/2}e^{\xi}, tq^{1/2}e^{-\xi}; q)_\infty\,(2q^{-1/2}\sinh\xi - q^{-1}t).$$

Therefore

$$\frac{t}{w_1(x)}\mathcal{D}_q\left(w_1(x)\sum_{n=0}^{\infty}\frac{h_n(x|q)}{(q;q)_n}q^{n(n-1)/2}t^n\right)$$

$$= \frac{2q^{3/2}}{q-1}\,(-tq^{1/2}e^{\xi}, tq^{1/2}e^{-\xi}; q)_\infty\,[(1+tq^{-1/2}e^{\xi})(1-tq^{-1/2}e^{-\xi})-1]$$

$$= \frac{2q^{3/2}}{q-1}\left[\sum_{n=0}^{\infty}\frac{h_n(x|q)}{(q;q)_n}q^{n(n-1)/2}t^n(q^{-n/1}-q^{n/2})\right].$$

Now (2.3) follows from the above identity by equating powers of t and the proof is complete.

Theorem 2.2 *The polynomials $\{h_n(x|q)\}$ satisfy the Rodrigues type formula*

$$h_n(x|q) = \left(\frac{q-1}{2}\right)^n q^{-n(n+3)/4}\,\frac{1}{w_1(x)}\mathcal{D}_q^n w_1(x). \tag{2.5}$$

Proof. Iterate (2.4).

We now combine (1.8) and (2.4) to establish our next result

Theorem 2.3 *The q^{-1}-Hermite polynomials are satisfy the q-Sturm-Liouville equation*

$$\mathcal{D}_q(w_1(x)\mathcal{D}_q h_n(x|q)) + 4q\,\frac{1-q^n}{(1-q)^2}\,w_1(x)h_n(x|q) = 0. \tag{2.6}$$

Theorem 2.4 *The q^{-1}-Hermite polynomials are orthogonal with respect to $w_1(x)$.*

Proof. Let $\lambda_n = -4q(1-q^n)(1-q)^{-2}$. Clearly the λ_n's are distinct. Therefore (2.6) implies

$$(\lambda_n-\lambda_m)\int_{-\infty}^{\infty} h_n(x|q)h_m(x|q)w_1(x)dx$$

$$= \int_{-\infty}^{\infty}[h_m(x|q)\mathcal{D}_q(w_1(x)\mathcal{D}_q h_n(x|q)) - h_n(x|q)\mathcal{D}_q(w_1(x)\mathcal{D}_q h_m(x|q))]dx$$

$$= < \mathcal{D}_q(w_1(x)\mathcal{D}_q h_n(x|q)), \sqrt{1-x^2}h_m(x|q) > - < \mathcal{D}_q(w_1(x)\mathcal{D}_q h_m(x|q)), \sqrt{1-x^2}h_n(x|q) >$$

$$= - < (w_1(x)\mathcal{D}_q h_n(x|q), \sqrt{1-x^2}\mathcal{D}_q h_m(x|q) > + < (w_1(x)\mathcal{D}_q h_m(x|q), \sqrt{1-x^2}\mathcal{D}_q h_n(x|q) >$$

$$= 0,$$

where we used (2.1).

As in the case of the classical orthogonal polynomials of Jacobi, Hermite and Laguerre, one can use the Rodrigues formula (2.5) to prove the orthogonality of $h_n(x|q)$ with respect to $w_1(x)$ and also compute their L^2 norms $\int_{-\infty}^{\infty} h_n^2(x|q)\,w_1(x)\,dx$ up to a normalization constant which is $\int_{-\infty}^{\infty} w_1(x)$.

We similarly treat the weight function $w_2(x;a)$ of (2.3).

Theorem 2.5 *The following alternate raising operator, Rodrigues formula and functional relationship hold for the q^{-1}-Hermite polynomials when $\Im a \neq 0$*

$$h_n(x|q) = a\bar{a}\left(\frac{q-1}{2}\right)\frac{q^{-2-n/2}}{w_2(x;a)}\mathcal{D}_q\left(w_2(x;aq^{-1/2})h_{n-1}(x|q)\right), \tag{2.7}$$

$$h_n(x|q) = (a\bar{a}(q-1)/2)^n \frac{q^{-n(n+9)/4}}{w_2(x;a)}\mathcal{D}_q^n\, w_2(x;aq^{-n/2}), \tag{2.8}$$

$$\mathcal{D}_q\left(w_2(x;aq^{-1/2})\mathcal{D}_q\, h_n(x|q)\right) = -\frac{4q^2(1-q^n)}{a\bar{a}(1-q)^2}w_2(x;a)h_n(x|q). \tag{2.9}$$

Proof. From the generating function (1.3) and the form of $w_1(x;a)$ in (2.3) we obtain

$$\sum_{n=0}^{\infty}\frac{q^{n(n-1)/2}t^n}{(q;q)_n}\mathcal{D}_q\left(w_2(x;aq^{-1/2})h_n(x|q)\right) = \mathcal{D}_q\left(w_2(x;aq^{-1/2})(-te^{\xi},te^{-\xi};q)_\infty\right).$$

Now a calculation gives

$$t\sum_{n=0}^{\infty}\frac{q^{n(n-1)/2}t^n}{(q;q)_n}\mathcal{D}_q\left(w_2(x;aq^{-1/2})h_n(x|q)\right) = \frac{2q^3\,(-t\sqrt{q}e^{\xi},t\sqrt{q}e^{-\xi};q)_\infty}{a\bar{a}(1-q)w_2(x;a)}(tq^{-1/2}\sinh\xi - t^2/q)$$

$$= -\frac{2q^3}{a\bar{a}(1-q)w_2(x;a)}\left[(-tq^{-1/2}e^{\xi},tq^{-1/2}e^{-\xi};q)_\infty - (-tq^{1/2}e^{\xi},tq^{1/2}e^{-\xi};q)_\infty\right].$$

Now (2.7) follows from the generating function (1.3). An iteration of (2.7) leads to (2.8). Finally (2.9) follows from the ladder operators (1.8) and (2.7).

Corollary 2.6 *The h_n's are orthogonal with respect to $w_2(x;a)$.*

For completeness we state the orthogonality relations of the q^{-1}-Hermite polynomials with respect to $w_1(x)$ and $w_2(x;a)$. They are

$$\int_{-\infty}^{\infty} w_1(x)h_m(x|q)h_n(x|q)dx = (\ln q^{-1})\,q^{-n(n+1)/2}(q;q)_n(q;q)_\infty\delta_{m,n}, \tag{2.10}$$

$$\int_{-\infty}^{\infty} w_2(x;a)h_m(x|q)h_n(x|q) = \frac{q^{-n(n+1)/2}\,\pi\, e^{-2\eta_1}(q;q)_n}{\sin\eta_2\,\cosh\eta_1\,(q,-qe^{2\eta_1},-qe^{-2\eta_1},qe^{2i\eta_2},qe^{-2i\eta_2};q)_\infty}\delta_{m,n}, \tag{2.11}$$

where $a = e^{\eta_1+i\eta_2}$, $\pi > \eta_2 > 0$.

Acknowledgements. This research partially supported by NSF grant DMS 9203659 and done during a sabbatical leave from the University of South Florida. Part of this work was done while the author was visiting the University of Wales College at Cardiff and he gratefully acknowledge the partial SERC support and the hospitality of B. M. Brown and D. W. Evans.

References

[1] R. A. Askey, *Continuous q-Hermite polynomials when $q > 1$*, in "q-Series and Partitions", ed. D. Stanton, IMA volumes in Mathematics and Its Applications, Springer-Verlag, New York, 1989, pp. 151-158.

[2] R. A. Askey and M. E. H. Ismail, *A generalization of ultraspherical polynomials*, in "Studies in Pure Mathematics", ed. P. Erdős, Birkhauser, Basel, 1983, pp. 55-78.

[3] R. A. Askey and J. A. Wilson, *Some basic hypergeometric orthogonal polynomials that generalize Jacobi polynomials*, Memoirs Amer. Math. Soc. **319** (1985).

[4] B. M. Brown, W. D. Evans and M. E. H. Ismail, in preparation.

[5] G. Gasper and M. Rahman, Basic Hypergeometric Series, Cambridge University Press, Cambridge, 1990.

[6] M. E. H. Ismail and D. R. Masson, *Extremal measures for q-Hermite polynomials when $q > 1$*, C. R. Math. Rep. Acad. Sc. Canada, 15 (1993), 7-12

[7] M. E. H. Ismail and D. R. Masson, *Q-Hermite polynomials, biorthogonal Rational Functions and q-beta integrals*, to appear.

[8] M. E. H. Ismail and M. Rahman, *Some basic bilateral sums and integrals*, Pac. J. Math., submitted.

[9] E. D. Rainville, Special Functions, Chelsea, Bronx 1971.

[10] J. Shohat and J. D. Tamarkin, The Problem of Moments, revised edition, American Mathematical Society, Providence, 1963.

Department of Mathematics, University of South Florida, Tampa, Florida 33620-5700.

Received November 8, 1993

C.R. Math. Rep. Acad. Sci. Canada - Vol. XV, No. 6, December 1993 décembre

The Theorem of Korkine and Zolotarev on the First Perfect Form

R. M. Erdahl

Presented by P. Ribenboim, F.R.S.C.

Abstract A new and compact proof is given of a theorem of Korkine and Zolotarev on the first perfect form. The proof uses elements of Voronoi's theory of L-types of lattices and the theory of lattice dicings which is briefly described.

1. Introduction. In their 1877 memoire *sur les formes quadratiques positives* [KZ], Korkine and Zolotarev considered integer $n \times r$ matrices that satisfy the following three conditions.

1. *Among the columns there are n that are linearly independent;*

2. *The nth order mirrors have modulus 0 or 1;*

3. *No two columns are linearly dependent.*

Because of their relationship to lattice dicings, described below, I will refer to matrices satisfying these conditions as **dicing matrices**. Using an elementary, but rather lengthy argument, Korkine and Zolotarev established the following important result.

Theorem 1 *For each value of $n \geq 2$ there is a unique arithmetic class of dicing matrices with $\binom{n+1}{2}$ columns. Moreover, there are no dicing matrices with a greater number of columns.*

The three properties that an $n \times r$ dicing matrix must satisfy are preserved by premultiplication by an integer $n \times n$ unimodular matrix $\mathbf{U}$, by postmultiplication by an $r \times r$ ± 1 diagonal matrix $\mathbf{D}$, and by postmultiplication by an $r \times r$ permutation matrix $\mathbf{P}$. The **arithmetic class** of a dicing matrix $\mathcal{D}$ is the class of matrices given by $\mathbf{U}\mathcal{D}\mathbf{PD}$.

Consider the $\binom{n+1}{2}$ (0,1)-vectors $\mathbf{d}_{ij} = [0^{j-i}1^i0^{n-j}]$, where $1 \leq i \leq j \leq n$.

Theorem 2 *For $n \geq 2$ the matrix $\mathcal{D}_1(n) = [\mathbf{d}_{11}, \mathbf{d}_{12}, \ldots, \mathbf{d}_{nn}]$ is a dicing matrix.*

Since $\mathcal{D}_1(n)$ has $\binom{n+1}{2}$ columns it determines the unique maximal class of Korkine and Zolotarev.

The integer vectors $\mathbf{d}_{ij}$ are the minimal vectors of the first perfect form ϕ_1 with the Cartan matrix $\mathbf{A}_n$ as coefficient matrix (the non-zero coefficients are given by $A_{ii} = 2$, $A_{i+1i} = A_{ii+1} = -1$). The form ϕ_1 is called perfect because its coefficients are completely determined by the $\binom{n+1}{2}$ equations $\phi_1(\mathbf{d}_{ij}) = 2$. Theorem 1 was used by Korkine and Zolotarev to characterize the arithmetic class of the first perfect form, and they referred to the matrix $\mathcal{D}_1(n)$ as the characteristic matrix for ϕ_1.

The Korkine and Zolotarev Theorem was rediscovered in 1957 by Heller [Hel] in quite a different context. Since that time Heller's arguments have been improved by several other authors (references and further comments can be found in [Sch, p.299]). All were motivated by the promise of totally unimodular matrices, and all were unaware of the Korkine and Zolotarev Theorem.

The purpose of this note is to describe a new, compact proof of the Korkine and Zolotarev Theorem, the bound being achieved by a one line argument. The proof makes use of Voronoi's theory of L-types of lattices and the theory of lattice dicings described below. Further details and references can be found in [ER], [Er].

2. The Korkine and Zolotarev bound. The L-polytopes (or Delaunay Cells) of a lattice form a facet to facet partition of $\mathbf{R}^n$, called an **L-partition**. In his deuxième mèmoire on *nouvelles applications des paramétres continus á la thèorie des formes quadratiques* [Vor], Voronoi established a fundamental relationship between the affine structure of L-partitions of lattices and the arithmetic theory of quadratic forms. He showed that the cone of positive quadratic forms $\mathcal{P}(n)$ can be partitioned into non-overlapping, relatively open polyhedral cones of varying dimension which he called **L-type domains**. These L-type domains have the following properties.

1. *The affine structure of the L-partitions of lattices on an L-type domain is constant;*

2. *The affine structure of the L-partitions of lattices on two distinct L-type domains agree if and only if the domains are arithmetically equivalent.*

3. *For each dimension n there are a finite number of arithmetically inequivalent L-type domains.*

Lattices, hence the L-partitions of lattices, are defined on subsets of quadratic forms in the usual way. Any positive quadratic form can be written as $\phi(\mathbf{x}) = \| \mathbf{B}\mathbf{x} \|^2$, where $\mathbf{B}$ is a square $n \times n$ matrix determined by ϕ up to an orthogonal transformation. The columns of $\mathbf{B}$ are then taken as a basis for the lattice Γ_ϕ. The matrix $\mathbf{B}$ is frequently referred to as the generating matrix for the lattice Γ_ϕ.

The L-type domains with full dimension $\binom{n+1}{2}$ are *general* and fit together facet to facet. The corresponding L-partitions are simplicial. The other L-type domains are *special*, and the L-partitions include non-simplicial L-polytopes. These domains appear as the relatively open faces, of varying dimensions, of the general L-type domains.

Dicing matrices are intimately related to Voronoi's theory of L- types. Associate with each column of a dicing matrix $\mathcal{D} = [\mathbf{d}_1, \mathbf{d}_2, \ldots \mathbf{d}_r]$ the quadratic form $\phi_i(\mathbf{x}) = (\mathbf{d}_i \cdot \mathbf{x})^2$. *The domain $\Phi(\mathcal{D})$ of this dicing matrix is the open polyhedral cone of positive quadratic forms given by*

$$\Sigma_{i=1}^{r} \lambda_i \phi_i(\mathbf{x})$$

where $\lambda_i > 0$.

Theorem 3 *Every dicing domain is an L-type domain, and is simplicial. An L-type domain is a dicing domain if and only if all the vertex forms are rank one forms.*

Since the dimension of the space of quadratic forms is $\binom{n+1}{2}$, the Korkine and Zolotarev bound is an immediate consequence of this theorem.

Corollary *The number of vertex forms of a dicing domain, hence the number of columns of a dicing matrix, cannot exceed* $\binom{n+1}{2}$.

A second consequence of the statement that a dicing domain is a simplicial cone is the following.

Corollary *A dicing domain is a general L- type domain if and only if the corresponding dicing matrix has* $\binom{n+1}{2}$ *columns, in which case the L-partitions of lattices on this domain are simplicial.*

3. Lattice Dicings. Consider an arbitrary dicing matrix $\mathcal{D} = [\mathbf{d}_1, \mathbf{d}_2, \ldots \mathbf{d}_r]$. Take each column $\mathbf{d}_i$ to be the normal vector to a **D-family** $\mathcal{G}_i$ of equi-spaced parallel hyperplanes with equations given by $\mathbf{d}_i \cdot \mathbf{x} = z, z \in \mathbf{Z}$. Taken together, the set of D-families $\{\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_r\}$ is the **lattice dicing** $\mathcal{D}$. It is convenient to use the same symbol $\mathcal{D}$ for both the dicing and the dicing matrix, and to think of the dicing matrix as a convenient way to represent the dicing. The hyperplanes of the dicing partition $\mathbf{R}^n$ into convex sets which fit together facet to facet. The conditions on the dicing matrix relate to geometric details of the lattice dicing in the following way. Condition 1 insures that the cells of the dicing are finite polytopes; these are the **D-polytopes** of the dicing. By condition 2, the vertices of the dicing form the lattice $\mathbf{Z}^n$, and it is from this result that the term *lattice dicing* is derived. Condition 3 insures that distinct columns of the dicing matrix correspond to distinct D-families. The notion of lattice dicing was introduced in [ER], and a complete description of the elementary properties of lattice dicings can be found there.

Theorem 4 *Let $\phi(\mathcal{D})$ be a dicing domain, and let $\Phi(\mathbf{x}) = \| \mathbf{B}\mathbf{x} \|^2 \in \Phi(\mathcal{D})$. Then the partition determined by the corresponding lattice dicing is mapped by* $\mathbf{B}$ *onto the L-partition of* Γ_ϕ.

From this theorem we again see that the affine structure of L- decomposition of lattices on a dicing domain is constant (see Theorem 3). The matrix $\mathbf{B}$ maps the D-polytopes of the dicing onto the L-polytopes of the lattice Γ_ϕ. The vertices of the D-polytopes are the coordinates of the vertices of the corresponding L-polytope.

By the second corollary to Theorem 3, and by Theorem 4, the D- polytopes of a lattice dicing with $\binom{n+1}{2}$ D-families are all simplexes. In fact, more can be said.

Theorem 5 *Any maximal lattice dicign with* $\binom{n+1}{2}$ *distinct D-families is arithmetically equivalent to a dicing that can be represented by a (0,1)-dicing matrix, which has among its columns the vectors* $\mathbf{e}_1, \mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$*. Moreover the D-polytopes of such a dicing are all simplexes, and include the standard simplex with vertices* $\mathbf{o}, \mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$*.*

In the statement of this theorem we have referred to arithmetically equivalent dicings, and this means that the corresonding dicing matrices are arithmetically equivalent. The vectors $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ are the standard basis vectors for $\mathbf{R}^n$. The (0,1)-dicing matrix $\mathcal{D}_1(n)$ has the properties described in the statement of this theorem, and the corresponding dicing has only simplicial D-polytopes, one of which is the standard simplex.

Lattice dicings have the following natural property. The intersection of a lattice dicing with any hyperplane of the dicing is affinely equivalent to a lattice dicing in $\mathbf{R}^{n-1}$. The intersection of a lattice dicing with k linearly independent hyperplanes from the dicing is affinely equivalent to a lattice dicing in $\mathbf{R}^{n-k}$.

Theorem 6 *The intersection of a maximal lattice dicing with* $\binom{n+1}{2}$ *D-families, with k linearly independent hyperplances from the dicing, is affinely equivalent to a maximal lattice dicing in* $\mathbf{R}^{n-k}$ *with* $\binom{n-k+1}{2}$ *D- families.*

The plane $\mathbf{e}_1 \cdot \mathbf{x} = 0$ belongs to the dicing $\mathcal{D}_1(n)$. The normal vector to the D-families in this plane, which are the intersection of the dicing $\mathcal{D}_1(n)$ with this plane, are obtained by setting the first row of the dicing matrix equal to zero. This set of normal vectors is clearly linearly equivalent to the set obtained by simply deleting these first components. By removing repeated columns, and the zero column, the dicing matrix $\mathcal{D}_1(n-1)$ is obtained (after possibly permuting columns). This shows that the intersection of the dicing $\mathcal{D}_1(n)$ with the hyperplane $\mathbf{e}_1 \cdot \mathbf{x} = 0$ is affinely equivalent to $\mathcal{D}_1(n-1)$. Moreover, by using a slightly more involved argument it can be shown that *the intersection of the dicing* $\mathcal{D}_1(n)$ *with any hyperplane of the dicing, is affinely equivalent to* $\mathcal{D}_1(n-1)$.

The fact that this last statement can be reversed supplies the essential step in the proof of the uniqueness of the Korkine and Zolotarev Theorem.

Theorem 7 *Suppose that $\mathcal{D}$ is a maximal lattice dicing with* $\binom{n+1}{2}$ *D-families of parallel hyperplanes. If the intersection of $\mathcal{D}$ with each of its hyperplanes is affinely equivalent to the lattice dicing $\mathcal{D}_1(n-1)$, then $\mathcal{D}$ is arithmetically equivalent to $\mathcal{D}_1(n)$.*

It is easy to establish that when $n = 2$, up to arithmetic equivalence, there is a unique lattice dicing with 3 D-families. Induction, along with Theorems 6 and 7, are used to establish the final result.

Theorem 8 *A lattice dicing with* $\binom{n+1}{2}$ *D-families of parallel hyperplanes is necessarily arithmetically equivalent to $\mathcal{D}_1(n)$.*

References

[Er] R. M. Erdahl, *Recipes for Lattice Dicing*, To appear in the Proceedings of the 2nd Gauss Symposium held in Munchen, Germany, August 1993.

[ER] R. M. Erdahl and S. S. Ryshkov, *On Lattice Dicing*, to appear in the European Journal of Combinatorics.

[Hel] J. Heller, *On linear systems with integral valued solutions*, Pacific Journal of Mathematics 7, 1351- 1364 (1957).

[KZ] A Korkine and G. Zolotarev, Sur les formes quadratiques positives, Math. Ann. 11, 242-292 (1877).

[Sch] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley-Interscience Series in Discrete Mathematics, 1986.

[Vor] G. F. Voronoi, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Premier mémoire*, J. Reine Angew. Math. **133**, 79-178 (1908); *Deuxiéme mémoire* **134**, 198- 287 (1908), **136**, 67-178 (1909).

Queen's University
Canada

Received November 18, 1993

An Asymptotic Formula by a Method of Selberg*

M. Ram Murty, F.R.S.C. and N. Saradha

1. Introduction. In [1], Landau showed that the number of integers $n \leq x$ which can be expressed as a sum of two squares i.e. $n = a^2 + b^2$ with a, b rational integers, is asymptotic to $cx/\sqrt{\log x}$ where $c > 0$ is a constant. For this, he considered $\psi(x)$ which denotes the number of odd integers n with $1 \leq n \leq x$ which do not have any prime factor of the form $4m+3$. He showed by analytic methods that

$$\psi(x) \sim cx/\sqrt{\log x}\,. \tag{1}$$

Since any n which can be expressed as a sum of two squares should have prime factors of the form $4m+3$ to an even power, the result on sums of two squares follows. Serre [3] used the method of Landau to prove many density theorems. In [2, p. 183–185], Selberg gave an elementary and simple proof of (1). Our aim in this paper is to show that the method of Selberg can be utilised to prove an asymptotic result in a wider context.

2. Preliminaries. Let N be a set of natural numbers and P be a proper subset of the set of primes. By (P) we denote the semigroup generated by the elements of P. Any integer $n \geq 1$ can be written as

$$n = n_P \cdot m,\ n_P \in (P) \text{ and } (m,p) = 1 \text{ for all } p \in P\,.$$

We notice that for any n_1, n_2 we have $(n_1 n_2)_P = (n_1)_P (n_2)_P$. An easy observation shows that

$$\sum_{\substack{d \in (P)\\ d|n}} \mu(d) = \begin{cases} 1 & \text{if } n_P = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

We define

$$\Lambda_P(d) = \begin{cases} \log p & \text{if } d = p^a,\ p \in P \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

We observe then that

$$\log n_P = \sum_{d|n} \Lambda_P(d)\,. \tag{4}$$

---

* Research partially supported by NSERC and FCAR grants.

On applying Möbius inversion to (4), we get

(5) $$\Lambda_P(n) = \sum_{d|n} \mu(d)\log(n/d)_P = -\sum_{\substack{d\in(P)\\ d|n}} \mu(d)\log d \quad \text{for } n_P > 1 .$$

Further, we define

(6) $$N_P = \{n \in N,\ (n,p) = 1 \text{ for all } p \in P\} = \{n \in N,\ n_p = 1\}$$

and

(7) $$N_P(x) = \text{the number of integers } n \text{ in } N_P \text{ with } 1 \le n \le x.$$

We make the following assumptions.

(A.1) Suppose for $d \in (P)$, $N(x,d)$ denotes the number of n in N with $1 \le n \le x$ and $d \mid n$. Then, there exists $\delta > 0$ such that

$$N(x,d) = \delta x/d + R(x,d)$$

with $R(x,d)$ satisfying

$$\sum_{\substack{d\in(P)\\ d\le x}} |R(x,d)| \log(x/d) = O(x) .$$

Note 1. *The condition on $R(x,d)$ is clearly satisfied if $R(x,d)$ is bounded.*

(A.2) For any $n \in N$, if $n_p > 1$ then n_p has at least two prime factors counted with multiplicity.

(A.3) (i) There exists a set $M \supseteq N$ and if M_P and $M_P(x)$ are defined as for N in (6) and (7) then

$$M_P = N_P .$$

(ii) For any $p \in P$ and $m \in M$, we have $pm \in M$.

Note 2. We call two sets M and N as *P-sieve equivalent* if (i) of (A.3) is satisfied.

(A.4) There exist numbers μ, ν such that $\mu > 0$

$$\sum_{\substack{m\in M\\ m\le x}} \frac{1}{m} = \mu \log x + \nu + O\left(\frac{1}{x}\right) .$$

We show

Theorem. *Under (A.1)-(A.4), there exists a constant c_1 depending on N, M and P such that*

$$N_P(x) \sim c_1 x/(\log x)^{1-(\delta/\mu)} .$$

3. Applications. In the following, while applying the theorem, we prefer to use the same c_1 though it changes with each example.

(i) As a first application, we recover (1) in the introduction. For this we take $N = \{n,\ n \equiv 1 (\bmod 4)\}$, $M = \{n,\ n \equiv 1 (\bmod 2)\}$, $P = \{p,\ p -$ prime and $p \equiv 3 (\bmod 4)\}$. Then

$$N_P = \{n \in N,\ (n,p) = 1 \text{ for } p \in P\} = \{n, \text{ if } p \mid n \text{ then } p \equiv 1 (\bmod 4)\} .$$

Thus $N_P(x) = \psi(x)$. Further, we notice that $M \supseteq N$ and M and N are P-sieve equivalent. Also $N(x,d) = (x/4d) + O(1)$ and $\sum_{\substack{n \in M \\ n \leq x}} 1/n = \frac{1}{2} \log x + \nu + O(1/x)$ where $\nu = \frac{\gamma - \log 2}{2}$ with γ-Euler's constant. $R(x,d)$ of axiom (1) is bounded. Thus axioms (A.1) to (A.4) are satisfied with $\delta = 1/4$ and $\mu = 1/2$. Hence (1) follows by the Theorem with $c = c_1$.

(ii) We generalise the result by Landau to any modulus ℓ. Let $N = \{n,\ n \equiv 1 (\bmod \ell)\}$, $M = \{n,\ (n,\ell) = 1\}$, $P = \{p,\ p -$ prime, $p \not| \ell$, $p \not\equiv 1 (\bmod \ell)\}$. We then have

$$N_P = \{n,\ n \equiv 1 (\bmod \ell), \text{ if } p \mid n \text{ then } p \equiv 1 (\bmod \ell)\} .$$

Also $M \supseteq N$ and M and N are P-sieve equivalent. Further,

$$N(x,d) = (x/\ell d) + O(1) \text{ and } \sum_{\substack{n \in M \\ n \leq x}} 1/n = \frac{\varphi(\ell)}{\ell} \log x + \nu + O(1/x)$$

where φ is the Euler totient function. Axioms (A.1) to (A.4) are satisfied with $\delta = 1/\ell$ and $\mu = \varphi(\ell)/\ell$. Thus,

$$N_P(x) \sim c_1 x / (\log x)^{1 - \frac{1}{\varphi(\ell)}} .$$

$\ell = 4$ gives the result of Landau as in (i).

(iii) Let G be a multiplicative group $\bmod \ell$ for any fixed ℓ and H a subgroup of G. Let $N = \{n,\ n (\bmod \ell) \in H\}$, $M = \{n,\ (n,\ell) = 1\}$ and $P = \{p,\ p -$ prime, $p (\bmod \ell) \notin H\}$. Then

$$N_P^* = \{n,\ n (\bmod \ell) \in H \text{ and if } p \mid n \text{ then } p (\bmod \ell) \in H\} .$$

We notice that $M \supseteq N$ and M and N are P-sieve equivalent since H is a subgroup. Further, $N(x,d) = (|H| x/\ell d) + O(1)$ and $\sum_{\substack{n \in M \\ n \leq x}} 1/n = \frac{\varphi(\ell)}{\ell} \log x + \nu + O(1/x)$ where $|H|$ denotes the order of group H. Axioms (A.1) and (A.4) are satisfied with $\delta = |H|/\ell$ and $\mu = \varphi(\ell)/\ell$. Thus

$$N_P(x) \sim c_1 x / (\log x)^{1 - \frac{|H|}{\varphi(\ell)}} .$$

Fixing $H = \{1\}$, we get the previous result. (ii).

4. Proof of the Theorem. In the sequel, c_2, c_3 and c_4 are effectively computable constants depending on N, M and P. We consider the expression

$$\sum_{\substack{n\in N\\ n\le x}} \sum_{\substack{d\in(P)\\ d|n}} \mu(d)\log(x/d) = \sum_{\substack{d\in(P)\\ d\le x}} \mu(d)\log(x/d) \sum_{\substack{n\in N\\ d|n\\ n\le x}} 1 . \tag{8}$$

We notice by (2), (3) and (5) that

$$\sum_{\substack{d\in(P)\\ d|n}} \mu(d)\log(x/d) = \begin{cases} \log x & \text{if } n\in N_P \\ \log p & \text{if } n \text{ is divisible by exactly one of } p \text{ from } P \\ 0 & \text{otherwise.}\end{cases} \tag{9}$$

Thus by (9) and (A.2), the left hand side of (8) equals

$$N_P(x)\log x + \sum_{\substack{p\in P\\ d\ge 2}} N_P(x/p^d)\log p = N_P(x)\log x + O(x) . \tag{10}$$

By (A.1) the right hand side of (8) equals

$$\sum_{\substack{d\in(P)\\ d\le x}} \mu(d)N(x,d)\log(x/d) = \delta \sum_{\substack{d\in(P)\\ d\le x}} \mu(d)(x/d)\log(x/d) + O(x) . \tag{11}$$

We now use (A.4) with x replaced by c_2x/d where $c_2 = e^{-(\nu/\mu)}$ on the right hand side of (11) to obtain

$$\sum \mu(d)N(x,d)\log(x/d) = (\delta x/\mu) \sum_{\substack{m\in M\\ d\in(P)\\ md\le c_2x}} \mu(d)/md + O(x) . \tag{12}$$

By (ii) of (A.3), (2) and (A.4) we get

(13)
$$\sum_{\substack{m\in M\\ d\in(P)\\ md\le c_2x}} \mu(d)/md = \sum_{\substack{n\in M\\ n\le c_2x}} (1/n) \sum_{\substack{d\in(P)\\ d|n}} \mu(d) = \sum_{\substack{n\in M\\ n\le c_2x\\ n_P=1}} (1/n) = \sum_{\substack{n\in M\\ n\le x\\ n_P=1}} (1/n) + \nu + O(1/x) .$$

Since N and M are P-sieve equivalent, (12) and (13) imply that

$$\begin{aligned}\sum \mu(d)N(x,d)\log(x/d) &= (\delta x/\mu) \sum_{\substack{n\in N\\ n\le x\\ n_P=1}} (1/n) + O(x) \\ &= (\delta x/\mu) \int_1^x \frac{dN_P(t)}{dt} + O(x) .\end{aligned} \tag{14}$$

From now on, we follow the proof of Selberg [2]. For the convenience of the reader we give below the details. We combine (8), (10) and (14) to obtain

$$N_P(x)\log x - (\delta x/\mu)\int_1^x N_P(t)/t^2 dt = O(x). \tag{15}$$

We set

$$V(x) = \int_1^x N_P(t)/t^2 dt. \tag{16}$$

Substituting (16) in (15) we get

$$x^2(\log x)V'(x) - (\delta x/\mu)V(x) = O(x)$$

which is equivalent to

$$\Big(\frac{V(x)}{(\log x)^{\delta/\mu}}\Big)' = O\Big(\frac{1}{x(\log x)^{1+\delta/\mu}}\Big)$$

where the dash indicates differentiation with respect to x. This yields

$$\frac{V(x)}{(\log x)^{\delta/\mu}} = c_3 + O\big(1/(\log x)^{\delta/\mu}\big). \tag{17}$$

From (15), (16) and (17) we get

$$N_P(x) = c_4 x/(\log x)^{1-(\delta/\mu)} + O(x/\log x). \qquad \square$$

In the above examples, it is not difficult to calculate c_1 explicitly. Finally, we note that $c_1 = 0$ can occur in the case that N is the set of non-primes, P is the set of primes, M is taken as the set of all natural numbers.

5. References.

[1] Landau, E. Über die Einteilung der postiven ganzen zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven zusammen-setzung erforderlichen Quadrate. *Arch. der Math. Und. Phys.*, (3) 13 (1908), pp. 305-312.

[2] Selberg, A.. *Collected Papers, Vol. II.* Springer-Verlag (1991).

[3] Serre, J.-P. Divisibilité de certaines fonctions arithmétiques. *L'enseignement Mathematique* (1976), pp. 227-260.

Department of Mathematics
McGill University

School of Mathematics
Tata Institute of Fundamental Research

Received January 13, 1994

C.R. Math. Rep. Acad. Sci. Canada - Vol. XV, No. 6, December 1993 décembre

ON BLOCH FUNCTIONS

Lou Zengjian

Abstract. In this paper, we give some new characterizations of Bloch functions, which extends a result of [5]

Key words and phrases. Bloch function, H^p space, $BMOA$, Hadamard product.

1. Introduction.

In the theory of one complex variable, Bloch functions play an important part, as they can be described in many ways, so their properties can be used in many branches of one complex variable. In this paper, we give some new characterizations of Bloch functions in term of Hadamard products.

2. Definition and notation.

Definetion 2.1. A function f analytic in D: $|z|<1$ is said to be of class $H^p(0<p<\infty)$ if

$$\| f \|_{H^p} = \lim_{r\to 1} M_p(r,f)$$

where

$$M_p(r,f) = \left(\frac{1}{2\pi}\int_0^{2\pi} |f(re^{i\theta})|^p d\theta\right)^{\frac{1}{p}} < \infty$$

H^∞ is the space of all bounded analytic functions (See [2] for more information on H^p)

Definition 2.2. The class $G^p(p>0)$ are defined by $f \in G^p$ if and only if

$$\| f \|_{G^p} = \left(\int_0^1 M_1^p(r,f')dr\right)^{\frac{1}{p}} < \infty$$

By [5], $G^1 \subset H^1$.

Definition 2.3. The class of functions f, analytic in D, for which

$$\| f \|_B = |f(0)| + \sup_{z\in D}(1-|z|)|f'(z)| < \infty$$

will be denoted by B. These functions are called the Bloch functions. The little Bloch B_0 is the set of analytic functions f in D for which (see [1,6])

$$(1-|z|)|f'(z)| \to 0, \qquad |z| \to 1.$$

Definition 2.4. A function $f \in H^1$ is said to be in the space $BMOA$ if and only if ([3, P. 238 Lemma 3.2])

$$\| f \|_* = \sup_{\xi\in D}\iint_D |f'(z)|^2 \frac{(1-|z|^2)(1-|\xi|^2)}{|1-z\bar{\xi}|^2} dxdy < \infty$$

By $VMOA$ we denoted the space of analytic functions of vanishing mean oscillation (see, for example, [3]). The proper inclusions

$$H^\infty \subset BMOA \subset B, \qquad VMOA \subset B_0$$

are well known.

3. The result and its proof.

In this paper, we use the "Hadamard products" to discribe the Bloch functions and obtain the following

Theorem. If g is analyic in D. Then the following are equivalent

① $g \in B$ ② $f * g \in H^\infty$ *for all* $f \in G^1$

③ $f * g \in BMOA$ *for all* $f \in G^1$ ④ $f * g \in B$ *for all* $f \in G^1$

⑤ $f * g \in BMOA$ *for all* $f \in H^1$ ⑥ $f * g \in B$ *for all* $f \in H^1$

⑦ $f * g \in VMOA$ *for all* $f \in G^1$ ⑧ $f * g \in B_0$ *for all* $f \in G^1$

⑨ $f * g \in VMOA$ *for all* $f \in H^1$ ⑩ $f * g \in B_0$ *for all* $f \in H^1$

Remark. This theorem extends Theorm 3.6 of [5].

Proof. ①→②. Suppose $g(z) = \sum_{n=0}^{\infty} x_n z^n \in B$, let $f(z) = \sum_{n=0}^{\infty} a_n z^n \in G^1$, then by a simple calculation, we have

$$\int_0^{2\pi} g'(re^{it}) f'(rze^{-it})dt = \sum_{n=0}^{\infty} (n+1)^2 r^{2n} a_n x_n z^n$$

from $\int_0^1 r^{2n+1} log \frac{1}{r} dr = \frac{1}{4(n+1)^2}$, we get

$$4\int_0^1 r log \frac{1}{r} \int_0^{2\pi} g'(re^{it}) f'(rze^{-it})dtdr = \sum_{n=0}^{\infty} a_n x_n z^n = f * g(z)$$

where $f * g(z) = \sum_{n=0}^{\infty} a_n x_n z^n$ is the Hadamard product of

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \qquad and \qquad g(z) = \sum_{n=0}^{\infty} x_n z^n.$$

By the inequality $r \log \frac{1}{r} \leqslant 1 - r, 0 < r \leqslant 1$, we have

$$\begin{aligned} |f * g(z)| &\leqslant 4\int_0^1 \int_0^{2\pi} |g'(re^{it})|(1-r)|f'(rze^{-it})|dtdr \\ &\leqslant 4\|g\|_B \int_0^1 M_1(r, f')dr \\ &\leqslant 4\|g\|_B \|f\|_{G^1} \end{aligned}$$

So $f * g \in H^\infty$ for all $f \in G^1$.

②→③→④. Since $H^\infty \subset BMOA \subset B$, their proofs are obvious.

④→①. If $f \in G^1$, we defined $T_g(f) = f * g$, T_g is clearly closed, so T_g is a bounded linear operator from G^1 to B. Let

$$f_r(z) = \frac{(1-r)rz}{(1-rz)^2} \tag{1}$$

Since T_g is bounded, there is a constant C independent of r such that

$$\|f_r * g\|_B \leqslant C\|f_r\|_{G^1} = O(1)$$

Since

$$(f_r * g)'(z) = \sum_{n=0}^{\infty} (1-r)r^n n^2 x_n z^{n-1}$$

we have

$$|\sum_{n=0}^{\infty} n^2 x_n r^n z^n|(1-r)(1-|z|) = O(1)$$

Taking $r = |z|$, we have

$$|\sum_{n=0}^{\infty} n^2 x_n z^n| = O(1-r)^{-2}$$

So $g \in B$.

①→⑨. Suppose that $g \in B$, $f \in H^1$ and $h = f * g$. Then we have

$$|D^2 h(r^2 e^{it})| = \left| \frac{1}{2\pi}\int_0^{2\pi} D^1 f(re^{i\theta}) D^1 g(re^{i(t-\theta)}) d\theta \right|$$
$$\leqslant C M_1(r, D^1 f)(1-r)^{-1} \| g \|_B$$

where $D^\alpha f(z) = \sum_{n=0}^{\infty} (n+1)^\alpha a_n z^n$ is the fractional derivative of $f(z) = \sum_{n=0}^{\infty} a_n z^n$.

By a result of [4], we conclude that

$$\int_0^1 (1-r)^3 M_\infty^2 (r^2, D^2 h) dr$$
$$\leqslant \int_0^1 (1-r) M_1^2 (r, D^1 f) dr \| g \|_B$$
$$\leqslant C \| f \|_{H^1} \| g \|_B$$

We use [2] to show that

$$\int_0^1 (1-r) M_\infty^2 (r, h') dr \leqslant C \| f \|_{H^1} \| g \|_B \tag{2}$$

By (2) and the fact that

$$\int_0^{2\pi} \frac{d\theta}{|1 - \xi r e^{i\theta}|^2} = \frac{2\pi}{1 - |\xi r|^2}$$

we have

$$\| h \|_* \leqslant \sup_{\xi \in D} 2\pi (1 - |\xi|^2) \int_0^1 \frac{1-r^2}{1 - |\xi r|^2} M_\infty^2 (r, h') dr$$
$$\leqslant C \int_0^1 (1-r^2) M_\infty^2 (r, h')$$
$$\leqslant C \| f \|_{H^1} \| g \|_B$$

That is

$$\| F * g \|_* \leqslant C \| F \|_{H^1} \| g \|_B, \qquad F \in H^1 \tag{3}$$

where the constant C does not depend on F. If we substitute $F = f_r - f$ *in* (3). we get

$$\| f * g_r - f * g \|_* \leqslant C \| f_r - f \|_{H^1} \| g \|_B$$

Since ([2, Th. 2.6])

$$\| f_r - f \|_{H^1} \to 0, \qquad r \to 1$$

from [3, P. 250 Th. 5.1] we have $f * g \in VMOA$.

⑨→⑦→⑧→④, ⑨→⑤→⑥→④, ⑨→⑩→⑥. Since $VMOA \subset BMOA \subset B$, $G^1 \subset H^1$, $VMOA \subset B_0 \subset B$, their proofs are obvious. This completes the proof of the theorem.

References

[1] J. M. Anderson, J. Clunie and Ch. Pommerenke, *On Bloch functions and normal functions*, J. Reine Angew Math., 270(1974), 12—37.

[2] P. L. Duren, *Theory of H^p spaces*, (1970), Academic Press.

[3] J. Garnett, *Bounded analytic functions*, 1981, Acadamic Press.

[4] G. H. Hardy and J. E. Littlewood, *Notes on the theory of series (XX) generalizations of a theorem of Paley*, Quart. J. Math. Oxford Ser., 8(1937), 161—171.

[5] S. B. Lee and Y. C. Kim, *Multipliers of G^p and Bloch functions*, Math. Japon., 32 (1987), 421—426.

[6] Z. J. Lou, *Characterizations of Bloch functions on the unit ball in C^n*, Kodai Math. J., 16 (1993), 74—78.

Department of Mathematics
Qufu Normal University

Received June 16, 1993
in revised form October 19, 1993

C.R. Math. Rep. Acad. Sci. Canada - Vol. XV, No. 6, December 1993 décembre

THE GELFAND THEOREM IN FLOW GEOMETRY

J.C. González-Dávila, M.C. González-Dávila and L. Vanhecke

Presented by P.C. Greiner, F.R.S.C.

We extend the Gelfand-like characterization of simply connected φ-symmetric spaces to the broader class of simply connected contact Killing-transversally symmetric spaces.

1. INTRODUCTION

Symmetric spaces have been studied extensively and they have some remarkable properties. In particular, it is well-known that for a symmetric space $M = G/H$, where G denotes the connected component of the identity of the full isometry group $\mathcal{I}(M)$ and H the isotropy group at $o \in M$, the algebra $\mathcal{D}(G/H)$ of G-invariant differential operators is commutative. This property is known as the Gelfand theorem. It is now also well-known that the converse theorem is not true in general. There are a lot of non-symmetric Riemannian manifolds where this algebra is commutative. However, it is shown in [8] that the Hermitian symmetric spaces can be characterized as the homogeneous Kähler manifolds with commutative algebra $\mathcal{D}(G/H)$, where G denotes the connected component of the identity of the group of holomorphic isometries. Further, the φ-symmetric spaces introduced by T. Takahashi in [11] (see also [1]) play a similar role in Sasakian geometry as that played by the Hermitian symmetric spaces in Kähler geometry. In [9] it is proved that a simply connected homogeneous Sasakian manifold G/H is globally φ-symmetric space if and only if the algebra $\mathcal{D}(G/H)$ is commutative modulo ξ. Here G denotes the connected component of the identity of the full automorphism group of the Sasakian structure and ξ is the characteristic vector field.

The class of (locally or globally) φ-symmetric spaces is a subclass of a broader class of Riemannian spaces, namely the class of (locally or globally) Killing transversally symmetric spaces (briefly, KTS-spaces) which have been introduced and studied in [2] - [6], [12] in the framework of the study of the geometry of Riemannian manifolds equipped with a unit Killing vector field ξ, that is, equipped with a special isometric flow $\mathcal{F}_\xi$. The main purpose of this note is to extend the Gelfand-like characterization of simply connected φ-symmetric spaces to the simply connected KTS-spaces of contact type (see Section 2 for details) inside the broader class of homogeneous Riemannian manifolds G/H equipped with such a contact flow $\mathcal{F}_\xi$, where G denotes the identity component of the group of ξ-preserving isometries.

2. PRELIMINARIES

We start by giving some of the basic definitions and results which will be needed to prove the characterization. We refer to [2] - [6] for more detailed information.

Let (M,g) be an n-dimensional, smooth, connected Riemannian manifold with Levi Civita connection ∇ and Riemannian curvature tensor R. A tangentially oriented foliation of dimension one on (M,g) is called a flow. It is said to be an isometric flow if it is generated by a non-singular Killing vector field. In what follows we shall denote by $\mathcal{F}_\xi$ an isometric flow generated by a unit Killing vector field ξ. It is well-known that such a Riemannian foliation is locally a Riemannian submersion $\pi : U \to \tilde{U} = U/\xi$ where U is a small open neighborhood on which ξ is regular. We denote by $\tilde{g}$ the induced metric on $\tilde{U}$ and by $\tilde{\nabla}$ the corresponding Levi Civita connection with associated Riemannian curvature tensor $\tilde{R}$. Further, H denotes the skew-symmetric tensor field of type $(1,1)$ defined by $HX = -\nabla_X\xi$ for all tangent vectors X of M and η is the dual one-form of ξ. Then, the flow $\mathcal{F}_\xi$ is said to be normal if and only if for all horizontal vectors X,Y,Z (i.e., orthogonal to ξ) we have $R(X,Y,Z,\xi) = 0$, and $\mathcal{F}_\xi$ is said to be a contact flow if H is of maximal rank or, equivalently, η is a contact form. In this case n is necessarily odd.

Further, $(M,g,\mathcal{F}_\xi)$ is called a locally Killing-transversally symmetric space (or briefly, a locally KTS-space) if and only if the local reflections [13] with respect to all flow lines are isometries. Moreover, $(M,g,\mathcal{F}_\xi)$ is said to be a (globally) KTS-space if ξ is a complete vector field and if the local reflections can be extended the global ones. Any simply connected, complete locally KTS-space is a globally KTS-space [5]. Further, for any locally KTS-space $(M,g,\mathcal{F}_\xi)$ the flow $\mathcal{F}_\xi$ is normal [3].

Locally and globally φ-symmetric spaces provide nice examples of locally and globally KTS-spaces of contact type [3] but there are a lot of examples of KTS-spaces which are of contact type and which are not Sasakian manifolds. We refer to [3], [5], [6] for explicit examples which are constructed by using the theory of infinitesimal models and principal bundles. However, in the simply connected case, those of contact type play a fundamental role as can be seen from the following result [5] :

Proposition 1. Let $(M,g,\mathcal{F}_\xi)$ be a simply connected KTS-space. Then (M,g) is irreducible if and only if it is of contact type. In the other case (M,g) is a direct product of an irreducible KTS-space $(M',g',\mathcal{F}_\xi)$ and a symmetric space (M'',g'').

Moreover, we have [3]

Proposition 2. Any locally KTS-space is locally homogeneous and is equipped with a naturally reductive homogeneous structure. Further, a simply connected, complete locally KTS-space is a naturally reductive homogeneous space.

Next, we have [3]

Proposition 3. The flow $\mathcal{F}_\xi$ is normal if and only if $\tilde\nabla\tilde H = 0$ where $\tilde H\tilde X = \pi_*(H\tilde X^*)$ for all vectors $\tilde X$ tangent to $\tilde U$. (Here $\tilde X^*$ denotes the horizontal lift of $\tilde X$ with respect to π.) In this case we have $\tilde R_{\tilde H\tilde X\tilde Y} = -\tilde R_{\tilde X\tilde H\tilde Y}$ for all $\tilde X, \tilde Y$ tangent to $\tilde U$.

Note that an (M,g) equipped with a normal contact flow $\mathcal{F}_\xi$ is automatically irreducible [3].

Finally, we have [3], [4]

Proposition 4. A Riemannian manifold (M,g) equipped with a normal flow $\mathcal{F}_\xi$ is a locally KTS-space if and only if each base space $(\tilde U, \tilde g)$ is locally symmetric. Moreover, for normal contact flows this is equivalent with $(\tilde\nabla_{\tilde X}\tilde R)(\tilde X, \tilde H\tilde X, \tilde X, \tilde H\tilde X) = 0$ for all $\tilde U$ and all $\tilde X$ tangent to $\tilde U$.

Because of Proposition 2 we shall now focus on a special class of isometric flows.

3. HOMOGENEOUS FLOWS AND THE MAIN THEOREM

Let (M,g) be a Riemannian manifold equipped with an isometric flow $\mathcal{F}_\xi$ and suppose that the group $A(M)$ of ξ-preserving isometries acts transitively on M. In this case $\mathcal{F}_\xi$ is called a homogeneous flow. Since M is connected, also the identity component $G = A_o(M)$ of $A(M)$ acts transitively and (M,g) can be identified with the coset space G/H where H is the isotropy subgroup of G at $o \in M$. The orbit space $\tilde M = M/\xi$ of such a space $(M,g,\mathcal{F}_\xi)$ admits a unique structure of a differentiable manifold such that the natural projection $\pi : M \to \tilde M$ is a submersion. In fact, let G^1 be the one-parameter subgroup of global isometries generated by ξ. Then G^1 is a Lie subgroup of G which belongs to its center. $\tilde M$ may be identified in a natural way with $G/H \cdot G^1$ and $\pi : G/H \to G/H \cdot G^1$ is a submersion. Following [10, Theorem XIV. p. 28] ξ is strictly regular. Moreover, since η is G^1-invariant, $(M,g,\mathcal{F}_\xi)$ is a principal G^1-bundle over $\tilde M$ and η is a connection form on M. Finally, define $\tilde g$ on $\tilde M$ by $\tilde g(\tilde X, \tilde Y) = g(\tilde X^*, \tilde Y^*)$ for all $\tilde X, \tilde Y$ tangent to $\tilde M$. Then π becomes a Riemannian submersion.

Next, let $A(\tilde M)$ be the group of $\tilde H$-preserving isometries of $(\tilde M, \tilde g)$ and $A_o(\tilde M)$ its identity component. The canonical projection $\pi : M \to \tilde M$ induces a map $\phi : A(M) \to A(\tilde M)$ given by $a \in A(M) \mapsto \phi(a) = \tilde a$ where $\tilde a(\pi(m)) = \pi(a(m))$ for all $m \in M$. ϕ is a homomorphism of Lie groups with kernel G^1. Then $\tilde G = G/G^1$ with its natural group structure is a Lie group isomorphic to a subgroup of $A(\tilde{M})$. We identify $\tilde{G}$ with the subgroup $\phi(G/G^1)$ of $A(\tilde{M})$. Then $\tilde{G}$ acts transitively on $\tilde{M}$ with the action given by $\tilde{G} \times \tilde{M} \to \tilde{M} : (\tilde{a}, \pi(m)) \mapsto \pi(a(m)), a \in G, m \in M$ and $\tilde{a} = \phi(a)$. Hence $\tilde{M}$ can be written as $\tilde{M} = \tilde{G}/\tilde{H}$ where $\tilde{H}$ is the isotropy subgroup at $\pi(o)$. The projection $G \to \tilde{G}$ induces an isomorphism H onto $\tilde{H}$ because $H \cap G^1 = \{e\}$ and $\phi(H) = \tilde{H}$.

Then we have

Proposition 5. The orbit space $(\tilde{M}, \tilde{g})$ of an (M, g) equipped with a normal contact homogeneous flow $\mathcal{F}_\xi$ is locally symmetric if and only if the algebra of $A_o(\tilde{M})$-invariant differential operators is commutative.

Proof. The result follows as in [8, Theorem 1] by using Proposition 3 and Proposition 4.

Now, in a similar way as in [9, Theorem 9] and by using Proposition 5 we get

Theorem 6. Let $(M, g, \mathcal{F}_\xi)$ be a simply connected manifold equipped with a normal contact homogeneous flow $\mathcal{F}_\xi$. Then $(M, g, \mathcal{F}_\xi)$ is a globally KTS-space if and only if the algebra $\mathcal{D}(G/H)$ is commutative modulo ξ.

Note that ξ can be interpreted in a natural way as an element of $\mathcal{D}(G/H)$.

Using Proposition 1 and following the same reasoning as in [7, Proposition 4] we get

Theorem 7. Let $(M, g, \mathcal{F}_\xi)$ be a simply connected globally KTS-space G/H. Then the algebra $\mathcal{D}(G/H)$ of invariant differential operators is commutative modulo ξ.

REFERENCES

[1] D.E. Blair and L. Vanhecke, Symmetries and φ-symmetric spaces, Tôhoku Math. J. 39 (1987), 373-383.

[2] M.C. González-Dávila, Espacios transversalmente simétricos de tipo Killing, doctoral dissertation, Universidad de La Laguna, 1992.

[3] J.C. González-Dávila, M.C. González-Dávila and L. Vanhecke, Reflections and isometric flows, to appear.

[4] J.C. González-Dávila and L. Vanhecke, Geodesic spheres and isometric flows, to appear.

[5] J.C. González-Dávila, M.C. González-Dávila and L. Vanhecke, Classification of Killing-transversally symmetric spaces, preprint.

[6] J.C. González-Dávila, M.C. González-Dávila and L. Vanhecke, Normal flow forms and their classification, preprint.

[7] O. Kowalski and L. Vanhecke, Classification of four-dimensional commutative spaces, Quart. J. Math. Oxford (2) 35 (1984), 281-291.

[8] O. Kowalski and L. Vanhecke, The Gelfand theorem and its converse for Kähler manifolds, Proc. Amer. Math. Soc. 102 (1988), 150-152.

[9] O. Kowalski and L. Vanhecke, The Gelfand theorem and its converse in Sasakian geometry, Kodai Math. J. 11 (1988), 70-77.

[10] R.S. Palais, A global formulation of the Lie theory of transformation groups, Mem. Amer. Math. Soc. 22, 1957.
[11] T. Takahashi, Sasakian φ-symmetric spaces, Tôhoku Math. J. 29 (1977), 91-113.
[12] Ph. Tondeur and L. Vanhecke, Transversally symmetric Riemannian foliations, Tôhoku Math. J. 42 (1990), 307-317.
[13] L. Vanhecke, Geometry in normal and tubular neighborhoods, Proc. Workshop on Differential Geometry and Topology, Cala Gonone (Sardinia) 1988, Rend. Sem. Fac. Sci. Univ. Cagliari, Supplemento al vol. 58 (1988), 73-176.

- Departamento de Mathemática Fundamental, Sección de Geometría y Topología, Universidad de La Laguna, La Laguna, Spain
- Department of Mathematics, Katholieke Universiteit Leuven, Celestijnenlaan 200B, B-3001 Leuven, Belgium

Received December 17, 1993

C.R. Math. Rep. Acad. Sci. Canada - Vol. XV, No. 6, December 1993 décembre

The equation $x^4 - y^4 = z^p$

Henri Darmon

Presented by M.R. Murty, F.R.S.C

Let p be an odd prime. We consider the equation

$$x^4 - y^4 = z^p, \qquad \gcd(x,y) = 1. \tag{1}$$

When $p = 2$, this equation was considered by Fermat, who used it to prove his celebrated "last theorem" for exponent 4.

In [Po], Powell proved that this equation has no integer solutions with $p \nmid xyz$ (analogous to the "first case" of Fermat's Last theorem) and proved a similar (slightly weaker) result for the equation $x^4 + y^4 = z^p$.

Terai and Osada [TO] and Cao [Ca] have extended this analysis to the equations $x^4 + dy^4 = z^p$ and $cx^4 + dy^4 = z^p$ respectively, proving that there are no first case solutions under certain assumptions.

The methods used by these authors involve factoring the left hand side of the equations over the appropriate quadratic field, and are close in spirit to the descent ideas which form the basis of Kummer's work on Fermat's Last Theorem.

Recently, it has been observed that Fermat's equation can be tackled by different methods based on elliptic curves and the Galois representations attached to them. Following work of Frey [Fr] and Serre [Sr2], Ribet [Ri] showed that the celebrated conjecture of Shimura and Taniyama that every elliptic curve is modular implies Fermat's last theorem. Thanks to the revolutionary work of Wiles, the Shimura Taniyama conjecture, previously thought to be inaccessible, now seems within reach.

Our main result is:

Theorem I: *Suppose the Shimura-Taniyama conjecture is true, and let $p \geq 11$ be a prime. Then:*

1. *Equation (1) has no non-trivial solution if $p = 1 \bmod 4$.*

2. *Equation (1) has no non-trivial solution with z even.*

Proof: Let $p \geq 11$ be prime, and let

$$a^4 - b^4 = c^p$$

be a solution to equation (1). If c is odd, assume without loss of generality that a is odd and b is even (otherwise, interchange a and b and replace c by $-c$). Factorizing the left hand side of $a^4 - b^4 = c^p$, the assumption $\gcd(a, b) = 1$ forces the three factors

$$a + b, \quad a - b, \quad a^2 + b^2$$

to be pth powers up to powers of 2. Hence, so are the integers

$$\begin{aligned} A = (a+b)^2 &= a^2 + 2ab + b^2, \\ B = (a-b)^2 &= a^2 - 2ab + b^2, \\ C &= a^2 + b^2, \end{aligned}$$

which also satisfy the equation

$$A + B - 2C = 0.$$

This equation gives three integers that are "almost" p-th powers and sum up to 0, and suggests considering the Frey curve

$$E : y^2 = x(x + A)(x - B).$$

Expanding the right hand side, the equation for E becomes:

$$y^2 = x^3 + 4abx^2 - (a^2 - b^2)^2 x.$$

The j-invariant and discriminant of E are:

$$j = 2^6 \frac{(a^2 + 3b^2)^3(3a^2 + b^2)^3}{c^{2p}(a^2 - b^2)^2}, \quad \Delta = 2^6 c^{2p}(a^2 - b^2)^2.$$

The conductor N of E can be computed using Tate's Algorithm [Ta]; let N_l denote the conductor of E at l, so that $N = \prod N_l$. The calculation is divided into two cases:

1. $l \neq 2$: Then E has good or semistable reduction at l; the conductor $N_l = 1$ if l does not divide c, and $N_l = l$ if l divides c. In any case, $\mathrm{ord}_l(\Delta) \equiv 0 \pmod{p}$, since $a^2 - b^2$ is a pth power up to powers of 2.
2. $l = 2$: If 2 divides c, then E is semi-stable and $N_2 = 2$; if 2 does not divide c, then $N_2 = 2^5$.

Let $\rho : \mathrm{Gal}(\bar{Q}/Q) \longrightarrow \mathrm{Aut}(E_p)$ be the Galois representation associated to the p-division points of E. By a result of Mazur [Mz], the representation ρ is irreducible. By using the Tate curve to analyze the local behaviour of ρ at the primes l of bad reduction for E ($l \neq 2, p$) one sees that ρ is unramified outside of 2 and p, and is finite at p (cf. [Sr2]). Hence, the conductor $N(\rho)$ is a power of 2 which satisfies:

$$N(\rho) = 2 \quad \text{if } 2|c,$$

$$N(\rho)|2^5 \quad \text{otherwise.}$$

Assuming the Shimura Taniyama conjecture, the elliptic curve E corresponds to a cusp form of weight 2 and level N. The "lowering the level" result of Ribet [Ri] shows that ρ corresponds to a cusp form of weight 2 and level $N(\rho)$ mod p. But:

1. If c is even, such a cusp form cannot exist, because there are no modular forms of weight 2 and level 2: the curve $X_0(2)$ has genus 0. This proves the second part of theorem I.

2. If c is odd, then ρ corresponds to a modular form of weight 2 and level dividing 32. There is a unique such form, of level 32, which corresponds to the elliptic curve $A = X_0(32)$, with complex multiplication by $Q(i)$. By Chebotarev's density theorem, it follows that

$$E_p \simeq A_p \quad \text{as Galois modules.}$$

In particular, by the theory of complex multiplication, the Galois representation ρ maps to the normalizer of a Cartan subgroup of $GL_2(F_p)$, and the restriction of ρ to $\mathrm{Gal}(\bar{Q}/Q(i))$ has abelian image. Furthermore, when $p = 1$

(mod 4), then ρ maps to the normalizer of a split Cartan subgroup; hence E has a rational subgroup of order p defined over $\mathbf{Q}(i)$; moreover all of its points of order 2 are defined over $\mathbf{Q}(i)$. It follows from work of Mazur [Mz] and Kamienny [Ka] (cf. cor. 1.7 of [Da]) that the denominator of $j(E)$ is divisible only by 2 or 3. Hence $a^4 - b^4$ is a power of 3, and so is $a^2 + b^2$. This can occur only if $ab = 0$, i.e., (a, b, c) is a trivial solution. This proves the first statement in theorem I.

Remarks:

1. Observe that in the proof we could not rule out the existence of the curve E, and had to obtain a contradiction in a more indirect manner. There is a good reason for this: the curve $A = X_0(32)$ is precisely the curve that arises from the trivial solution $(1,0,1)$ to the equation $x^4 - y^4 = z^p$.
2. When $p = -1$ mod 4, the image of ρ is the normalizer of a non-split Cartan subgroup. This case seems more difficult to rule out using the "Eisenstein descent" methods of Mazur and Kamienny, although one also expects it cannot occur when p is large. More precisely, one expects that the image of the Galois representation coming from a non-CM elliptic curve should be the full $\mathbf{GL}_2(\mathbf{F}_p)$ when p is large enough ($p > 19$, perhaps?) A similar issue arises in [Da] in the study of the equations $x^p + y^p = z^2$ and $x^p + y^p = z^3$.
3. A natural question is to analyze the equation $x^4 + y^4 = z^p$ (or even more general variants such as $x^4 + cy^4 = z^p$). This equation is quite different from the previous one: $x^4 + y^4$ is irreducible over $\mathbf{Q}$ and only splits after adjoining primitive 8th roots of unity. A promising approach in this case is to consider the Galois representations arising from certain $\mathbf{Q}$-curves, that are defined over $\mathbf{Q}(i)$ and are 2-isogenous to their Galois conjugates. The methods used in that case are more involved and will be treated in a separate paper.

References

[Ca] Cao, Zhen Fu, *The Diophantine equation $cx^4 + dy^4 = z^p$*, C.R. Math. Rep. Acad. Sci. Canada 14 (1992), no. 5, pp. 231-234.

[DG] Darmon, H., Granville, A., *On the equations $Ax^p + By^q = Cz^r$ and $z^m = F(x, y)$*, to appear.

[Da] Darmon, H. *The equations* $x^n + y^n = z^2$ *and* $x^n + y^n = z^3$, Intern. Math. Res. Not. no 10, 1993, pp. 263-273.

[Fr] Frey G., *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Saraviensis, 1 (1986), 1–40.

[Ka] Kamienny, S., *Points on Shimura curves over fields of even degree*, Math. Ann. 286, 731-734 (1990).

[Mz] Mazur, B., *Rational isogenies of prime degree*, Inv. Math. 44, 129-162 (1978)

[Po] Powell, B. *Sur l'équation Diophantienne* $x^4 \pm y^4 = z^p$, Bull. Sc. Math., 107 (1983), 219-223.

[Ri] Ribet, K., *On modular representations of* $Gal(\bar{Q}/Q)$ *arising from modular forms*, Invent. Math. 100, 431-476 (1990).

[Sr1] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. 15, 259-331 (1972).

[Sr2] Serre, J.-P., *Sur les représentations modulaires de degré* 2 *de* $Gal(\bar{Q}/Q)$, Duke Math. J. Vol. 54, no. 1, 179-230 (1987).

[Ta] Tate, J., *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in Modular Functions of One Variable, SLN 476, pp. 33–52.

[TO] Terai, N. and Osada, H. *The Diophantine equation* $x^4 + dy^4 = z^p$, C.R. Math. Rep. Acad. Sci. Canada 14 (1992), No. 1, pp. 55-58.

Department of Mathematics
Princeton University

Received January 17, 1994

Mailing Addresses

H.S.M.Coxeter	Department of Mathematics University of Toronto Toronto, Ontario M5S 1A1 Canada
H. Darmon	Department of Mathematics Princeton University Box 37, Fine Hall, Princeton, NJ 08544-1000 U.S.A.
R.M. Erdahl	Department of Mathematics and Statistics Queen's University Kingston, Ontario K7L 3N6 Canada
J.C. González- Dávila	Departamento de Mathemática Fundamental Sección de Geometria y Topologia Universidad de La Laguna La Laguna, Spain
M.C. González- Dávila	Departamento de Mathemática Fundamental Sección de Geometria y Topologia Universidad de La Laguna La Laguna, Spain
M.E.H. Ismail	Department of Mathematics University of South Florida Tampa, FL 33620-5700 U.S.A.
Z. Lou	Department of Mathematics Qufu Normal University Qufu, Shandong 273165 P.R. China
M.T. McGregor	Department of Mathematics University College of Swansea Swansea, Wales SA2 8PP, U.K.
M.R. Murty	Department of Mathematics McGill University Montreal, Quebec H3A 2K6 Canada
S.S. Ryshkov	Steklov Institute Moscow, Russia
N. Saradha	School of Mathematics Tata Institute of Fundamental Research Homi Bhabha Road, Bombay 400005, India
A.C. Thompson	Department of Mathematics, Statistics and Computer Science Dalhousie University Halifax, Nova Scotia B3H 3J5 Canada
L. Vanhecke	Department of Mathematics Katholieke Universiteit Leuven Celestijnenlaan 200B, B-3001 Leuven, Belgium
X.-Z. Yuan	Department of Mathematics, Statistics and Computer Science Dalhousie University Halifax, Nova Scotia B3H 3J5 Canada

Articles Index – Volume XV

Paging of Vol. XV

(1) 1–60 (2) 61–84 (3) 85–120
(4) 121–180 (5) 181–236 (6) 237–296