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

Vol. VIII, No. 3 June 1986 juin

CONTENTS

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 3, June 1986 juin

EUCLID AND MINKOWSKI JUXTAPOSED

J. L. Synge F.R.S.C.

Part I

In 1905 Einstein invented the special theory of relativity. In 1909 Minkowski invented four-dimensional space-time as an alternative way of looking at Einstein's theory. In 1915 Einstein invented the general theory of relativity by turning Minkowski's flat space-time into a curved one. This general theory deals with gravitation. Since there is much of physics in which gravity is unimportant, Minkowskian space-time is the basic theatre of operations in most modern physics, just as Euclidean space and absolute time were prior to 1905.

The first difficulty in thinking about Minkowskian space-time is its four-dimensionality. In most approaches this difficulty is overcome by taking plane slices of space-time, and this serves very well in obtaining those spectacular results of which even the general public has learned with amazement - the contraction of a moving rod and the slowing down of a moving clock. But if we view these matters in geometrical terms, they are merely deductions from Minkowskian geometry, with which even the well-educated public, conversant with Euclidean geometry, seems to have remained ignorant. The purpose of the present note is not to give a systematic account of Minkowskian geometry, but rather to stimulate interest in it by contrasting triangles in the Minkowskian plane with Euclidean triangles.

Let us start with the Euclidean plane E_2. In it we have points, vectors joining points, and the usual scalar product of vectors, commutative and distributive. Take a basis (or axes)

consisting of two orthogonal unit vectors $\underline{e}_1$, $\underline{e}_2$, so that

$$\underline{e}_1.\underline{e}_1 = 1, \qquad \underline{e}_2.\underline{e}_2 = 1, \qquad \underline{e}_1.\underline{e}_2 = 0. \tag{1}$$

Let $\underline{a}$, $\underline{b}$, $\underline{c}$ be the directed sides of a triangle. They satisfy the condition of closure

$$\underline{a} + \underline{b} + \underline{c} = 0, \tag{2}$$

and so

$$(\underline{a} + \underline{b}).(\underline{a} + \underline{b}) = \underline{c}.\underline{c}. \tag{3}$$

Define

$$x = \underline{a}.\underline{a}, \qquad y = \underline{b}.\underline{b}, \qquad z = \underline{c}.\underline{c}, \tag{4}$$

these being the squares on the sides. Then (3) gives

$$x + y - z = -2\underline{a}.\underline{b}. \tag{5}$$

Resolve $\underline{a}$, $\underline{b}$, $\underline{c}$ on the basis:

$$\underline{a} = a_1\underline{e}_1 + a_2\underline{e}_2, \quad \underline{b} = b_1\underline{e}_1 + b_2\underline{e}_2, \quad \underline{c} = c_1\underline{e}_1 + c_2\underline{e}_2. \tag{6}$$

Then by (1)

$$\underline{a}.\underline{b} = a_1b_1 + a_2b_2, \tag{7}$$

for substitution in (5). But first we note that

$$x = \underline{a}.\underline{a} = a_1^2 + a_2^2, \qquad y = \underline{b}.\underline{b} = b_1^2 + b_2^2, \tag{8}$$

and so (5) gives

$$\begin{aligned}(x + y - z)^2 - 4xy &= 4\{(a_1b_1 + a_2b_2)^2 - (a_1^2 + a_2^2)(b_1^2 + b_2^2)\} \\ &= -4(a_1b_2 - a_2b_1)^2,\end{aligned} \tag{9}$$

which is negative. Define

$$F(x,y,z) = x^2 + y^2 + z^2 - 2yz - 2zx - 2xy, \tag{10}$$

which is merely the left hand side of (9) in symmetric form. We conclude that F is negative for every Euclidean triangle.

Now for a triangle in the Minkowskian plane M_2, we have points, vectors joining points and a scalar product, commutative and distributive. But when we take a basis consisting of two

orthogonal unit vectors $\underline{m}_1$, $\underline{m}_2$, they satisfy

$$\underline{m}_1 \cdot \underline{m}_1 = 1, \qquad \underline{m}_2 \cdot \underline{m}_2 = -1, \qquad \underline{m}_1 \cdot \underline{m}_2 = 0, \tag{11}$$

differing from (1) by the minus sign. The physicist would say that $\underline{m}_1$ is spacelike and $\underline{m}_2$ timelike. The whole difference between E_2 and M_2 lies in that minus sign.

Again we take $\underline{a}$, $\underline{b}$, $\underline{c}$ to be the directed sides of a triangle, and the argument from (2) to (5) inclusive holds in M_2. But we must change (6) by putting $\underline{m}$ for $\underline{e}$, and so, by (11), (7) is changed to

$$\underline{a} \cdot \underline{b} = a_1 b_1 - a_2 b_2, \tag{12}$$

while instead of (8) we have

$$x = \underline{a} \cdot \underline{a} = a_1^2 - a_2^2, \qquad y = \underline{b} \cdot \underline{b} = b_1^2 - b_2^2. \tag{13}$$

Then by simple algebra we get from (5)

$$(x + y - z)^2 - 4xy = 4(a_1 b_2 - a_2 b_1)^2, \tag{14}$$

formally similar to (9), but with the sign reversed.

Conclusion: The algebraic expression $F(x,y,z)$ as in (10) is negative for all triangles in the Euclidean plane and positive for all triangles in the Minkowskian plane, where x, y, z are the self-products of the directed sides as in (4) and (13).

To exploit this juxtaposition of Euclid and Minkowski, let us make a picture in ordinary space E_3 using x, y, z as rectangular cartesians. To any triangle in either plane there corresponds a point in E_3. $F = 0$ is a quadric cone of revolution separating Euclid from Minkowski. If we move out along any ray from the origin of (x,y,z) we merely magnify the triangle without changing its shape. Thus, if we are content to think only of the shapes of triangles, it is convenient to consider only the

points in E_3 where the rays cut the unit sphere

$$x^2 + y^2 + z^2 = 1. \tag{15}$$

Now

$$F(x,y,z) = 2(x^2 + y^2 + z^2) - (x + y + z)^2, \tag{16}$$

and so, on the unit sphere, the representative points of E_2, which make F negative, occupy the "arctic cap"

$$E_2: \quad x + y + z > 2^{\frac{1}{2}}, \tag{17}$$

for we must remember that, in E_2, we have x, y, z positive. As for the representative points of M_2, they occupy the "tropics", viz.

$$M_2: \quad (x + y + z)^2 < 2. \tag{18}$$

That leaves an unoccupied "antarctic cap",

$$Q_2: \quad x + y + z < -2^{\frac{1}{2}}. \tag{19}$$

This last is a queer region: the scalar products $\underline{a}.\underline{a}$, $\underline{b}.\underline{b}$, $\underline{c}.\underline{c}$ are negative, a sort of perverted E_2.

The axis of the cone F = 0 is equally inclined to the (x,y,z) axes, and this is unsatisfactory for diagrammatic purposes. It is better to view the sphere obliquely so that the plane x + y + z = 0 appears as a straight line. Then we have a diagram as in Fig. 1.

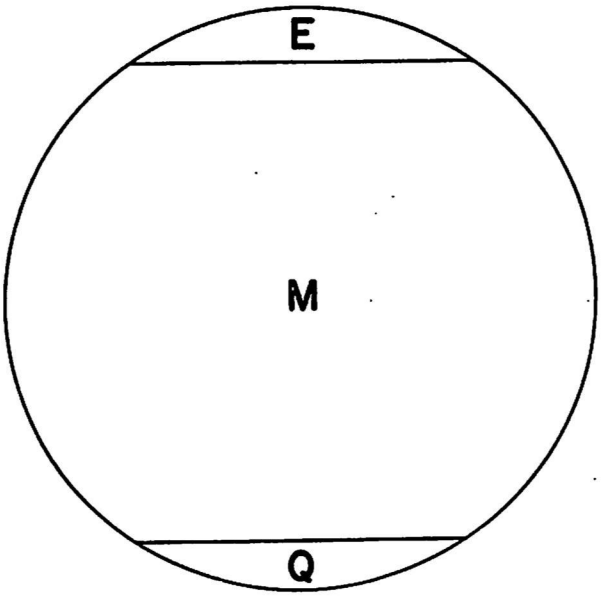

Fig. 1: The unit sphere on which are represented the shapes of all triangles in E_2, M_2 and Q_2, with the separating planes $x + y + z = \pm 2^{\frac{1}{2}}$.

J. L. Synge

Part II

THE NINE-POINT CIRCLE IN THE MINKOWSKIAN PLANE

When treated vectorially using scalar products, the formal geometry of the Minkowskian plane is similar to that of the Euclidean plane. If V and V' are two Minkowskian vectors with components (V_1, V_2) and (V_1', V_2') respectively, their scalar product is

$$V.V' = V_1V_1' - V_2V_2' , \qquad (20)$$

this expression being invariant under Lorentz transformations. But, as far as this note is concerned, the minus sign is of little importance. What is important is that Euclidean diagrams must be used with great caution, merely as a mental aid in identifying the symbols.

Fig. 2 shows a triangle in the Euclidean plane. The dictionary reads:

A, B, C are the vertices,

A', B', C' are the feet of the perpendiculars,

H is the orthocentre,

A", B", C" are the middle points of the sides,

A‴ , B‴ , C‴ are the middle points of the lines joining the vertices to H.

The Euclidean nine-point circle passes through the points with one, two or three primes. All the symbols may be regarded as position vectors relative to an arbitrary origin in the plane.

I dedicate this note to the memory of Louis Brand (1885-1971); but for his concise and elegant treatment of the Euclidean nine-point circle, I would not have succeeded in passing to the Minkowskian plane.

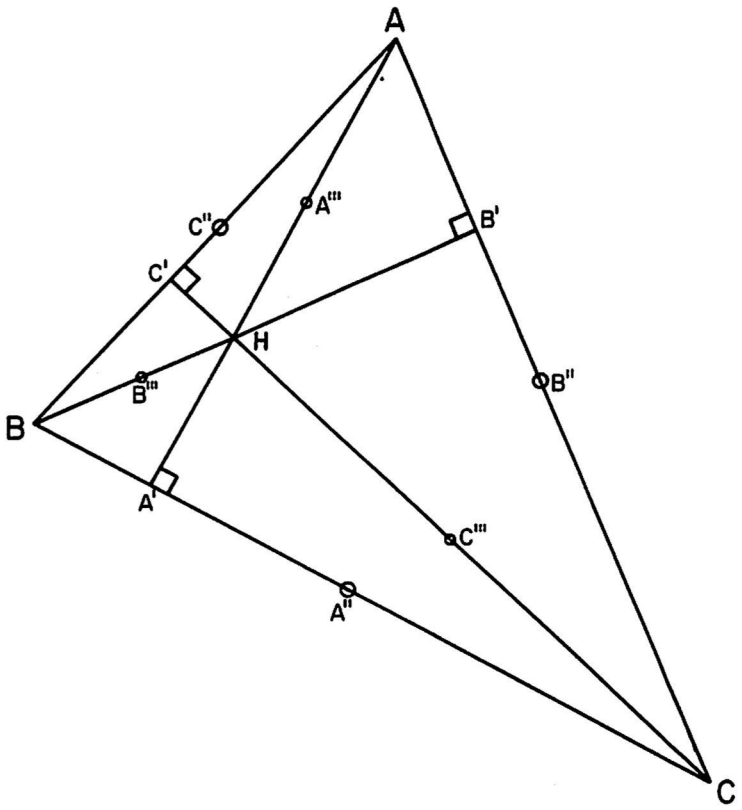

Fig. 2: The nine points for a Euclidean triangle. The diagram identifies schematically the nine points in a Minkowskian triangle.

Let us now use this dictionary for a triangle in the Minkowskian plane, interpreting the symbols as position vectors. We start with the vertices A, B, C. As we seek a general argument, singular cases will not be considered, thus A, B, C are taken to be linearly independent and no side is a null line.

But what are the feet of the perpendiculars? Does H exist? Here I follow Brand formally. We are not to waste time seeking explicit formulae, instead, it is best to define certain vectors by their properties. Consider the identity

$$(A - B).(H - C) + (B - C).(H - A) + (C - A).(H - B) = 0. \tag{21}$$

If H is such that it makes two of these terms zero, then the third is zero. But $(A - B).(H - C) = 0$ is, for free H, the locus of points on the line through C perpendicular to the side A - B. Hence the three perpendiculars intersect at an orthocentre H, and A', B', C' are defined by drawing the lines from A, B, C through H. To obtain an explicit formula for H would only complicate the argument unnecessarily: all we need is the fact that H satisfies the three equations

$$(A - B).(H - C) = (B - C).(H - A) = (C - A).(H - B) = 0. \tag{22}$$

The other points are easy:

$$A'' = \tfrac{1}{2}(B + C), \text{ etc.} \qquad A''' = \tfrac{1}{2}(H + A) \text{ etc.} \tag{23}$$

where etc. means cyclical permutation of A, B, C.

Our dictionary has now been made Minkowskian. The next step is to define four vectors as follows:

$$P = (1/4)(H + A - B - C)$$
$$Q = (1/4)(H - A + B - C)$$
$$R = (1/4)(H - A - B + C) \qquad (24)$$
$$N = (1/4)(H + A + B + C).$$

It follows from (22) that

$$P.P = Q.Q = R.R = S, \text{ say.} \qquad (25)$$

Theorem: The Minkowskian circle with equation

$$(X - N).(X - N) = S \qquad (26)$$

passes through the nine points A', B', C', A", B", C", A"', B"', C"', N as in (24) is the nine-point centre, and S is given by (25).

Proof: We are to verify (26) by substituting for X each of the nine points.

Now

$$N - A" = (1/4)(H + A - B - C) = P,$$
$$(N - A").(N - A") = P.P = S, \qquad (27)$$

as required, with of course the same for B" and C". Further

$$A"' - N = (1/4)(H + A - B - C) = P,$$
$$(A"' - N).(A"' - N) = P.P = S, \qquad (28)$$

as required, with of course the same for B"' and C"'. As for A', it follows from the above equations that

$$N = \tfrac{1}{2}(A" + A"'). \qquad (29)$$

Thus

$$N - A" = A"' - N,$$

and

$$A" - A' = (N - A') - (N - A") \qquad (30)$$
$$A"' - A' = (N - A') - (N - A"') = (N - A') + (N - A")$$
$$(A" - A').(A"' - A') = (N - A').(N - A') - (N - A").(N - A"').$$

The left hand side vanishes by the orthogonality at A' (cf. Fig. 1) and the final scalar product in (11) is S by (8); thus

$$(A' - N).(A' - N) = S, \tag{31}$$

with of course the same for B' and C'. This completes the proof of the nine-point theorem in the Minkowskian plane.

Reference

1. L. Brand, Vector and Tensor Analysis, Wiley, New York, 1947, p.33.

Dublin Institute for Advanced Studies
10, Burlington Road, DUBLIN 4, Ireland.

Received 18 March, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 3, June 1986 juin

CONTRACTIONS STRICTES ET COVARIANCES MARKOVIENNES

Bernard Aupetit et Jean-Claude Massé *

Presented by F.V. Atkinson F.R.S.C.

Résumé

On démontre qu'une covariance markovienne $\Gamma(t) = \exp(-At)$, $t>0$, est une contraction stricte si et seulement si (a) $A+A^*$ est une matrice hermitienne positive; (b) la partie réelle des éléments du spectre de A est strictement positive.

Summary

We prove that a Markov covariance $\Gamma(t) = \exp(-At)$, $t>0$, is a strict contraction if andonly if (a) $A+A^*$ is a positive hermitian matrix; (b) the real part of the elements of the spectrum of A is strictly positive.

1. INTRODUCTION.

La loi d'un processus aléatoire gaussien centré stationnaire est déterminée par sa fonction de covariance. Etant donné dans $\mathbb{C}^n$ un tel processus $(X_t, t>0)$ défini sur un espace probabilisé $(\Omega,\mathcal{F},P)$, la fonction de covariance est définie par

$$\Gamma(t-s) = E[X_s X_t'] = \int_\Omega X_s X_t' \, dP, \quad 0<s<t$$

où X_t' désigne le vecteur ligne conjugué de X_t. Si on exclut les cas dégénérés, on peut supposer par renormalisation que $\Gamma(0) = I$.

* Recherche subventionnée par le Conseil de Recherche en Sciences Naturelles et en Génie du Canada.

Les processus markoviens peuvent être caractérisés comme étant les processus associés aux fonctions de covariance qui sont solutions de l'équation de Cauchy

$$\Gamma(s+t) = \Gamma(s)\Gamma(t) \quad s>0 \ , \ t>0.$$

Il est bien connu que les solutions continues de cette équation sont de la forme $\Gamma(t) = \exp(-At)$ où A est une matrice complexe m×m.

En théorie de la prédiction le meilleur prédicteur linéaire de X_{s+t} au temps s est $\Gamma^*(t)X_s$ [2, p.289], où * désigne la transposée de la conjuguée. La matrice variance-covariance de l'erreur de prévision est alors

$$E[(X_{s+t}-\Gamma^*(t)X_s)(X_{s+t}-\Gamma^*(t)X_s)'] = I-\Gamma^*(t)\Gamma(t).$$

Pour qu'il ne subsiste pas de déterminisme dans le processus, on pourra exiger que $I-\Gamma^*(t)\Gamma(t)$ soit définie positive quel que soit $t>0$; cela équivaut à dire que $\|\Gamma(t)\|<1$, quel que soit $t>0$ ou encore que $\Gamma(t)$ est une contraction stricte. Dans la suite, nous caractériserons à l'aide de la matrice A l'ensemble des covariances markoviennes continues vérifiant cette condition de non-dégénérescence sur la prédiction.

2. CARACTÉRISATION

THÉORÈME. Soit $\Gamma(t) = \exp(-At)$, $t>0$, où A est une matrice complexe m×m. Alors pour que $\Gamma(t)$ soit une contraction stricte - c'est-à-dire pour que $I-\Gamma^*(t)\Gamma(t)$ soit définie positive dans $(0,\infty)$-il faut et il suffit que

(a) $A+A^*$ soit une matrice hermitienne positive, autrement dit $x'(A+A^*)x \geq 0$, quel que soit $x \in \mathbb{C}^m$;

(b) la partie réelle des éléments du spectre de A soit strictement positive.

Démonstration. Nécessité.

La condition (a) découle du théorème de Lumer-Phillips [1, p.30] ou [3, p.250]. En effet, celui-ci affirme que $\|\exp(-At)\| \leq 1$ si et seulement si pour tout $x \in \mathbb{C}^m$ la partie réelle de $x'Ax$ est ≥ 0. Il clair que cela équivaut à dire que $x'(A+A^*)x \geq 0$, que soit $x \in \mathbb{C}^m$.

D'autre part, la positivité de $I-\exp(-A^*t)\exp(-At)$, $t>0$, équivaut à dire que le spectre de $\exp(-A^*t)\exp(-At)$ est contenu dans $(0,1)$, quel que soit $t>0$. Désignons par $\rho(M)$ le rayon spectral d'une matrice M. Comme

$$\rho(\exp(-At)) \leq \|\exp(-At)\| = \sup_{\substack{|x|=1 \\ x \in \mathbb{C}^m}} (x'\exp(-A^*t)\exp(-At)x)^{1/2} < 1 ,$$

on a $|e^{-tz}| = e^{-t\mathrm{Re}z} < 1$ pour z dans le spectre de A, d'où la validité de (b).

Suffisance.

En vertu de ce qui précède, il nous suffira de vérifier que les conditions impliquent que $\psi(t) = \|\exp(-At)\| < 1$, pour $t>0$. Soit $x \in \mathbb{C}^m$ tel que $|x|=1$. Alors pour tout $t>0$

$$x'.x - x'\exp(-A^*t)\exp(-At)x = \int_0^t x'\exp(-A^*s)(A^*+A)\exp(-As)x\,ds \geq 0$$

en vertu de (a), d'où $\|\exp(-At)\| \leq 1$, $t>0$. Comme ψ est évidemment décroissante, on obtiendra le résultat cherché en montrant que ψ ne peut être égale à 1 dans un intervalle de la forme $[0,u]$, $u>0$. Si c'était le cas, on pourrait en effet prendre ci-dessus x tel que $|\exp(-Au)x| = 1$, de sorte qu'on aurait

$$x'\exp(-A^*s)(A^*+A)\exp(-As)x = 0 \qquad 0 \leq s \leq u.$$

Or, d'après le principe d'identité, la fonction analytique

$$z \to x'\exp(-A^*z)(A^*+A)\exp(-Az)x$$

vaut 0 sur un intervalle non trivial seulement si elle vaut 0 dans tout le plan

complexe. Il en résulte que $\|\exp(-At)\| = 1$, $t>0$. Or cela entraîne que

$$\rho(\exp(-At)) = \lim_{n\to\infty} \|\exp(-Atn)\|^{1/n} = 1 ,$$

ce qui vient en contradiction avec la condition (b) et termine la démonstration.

Ce résultat peut se généraliser au cas des opérateurs linéaires bornés de l'espace de Hilbert en utilisant les états purs et en modifiant l'argument.

Bibliographie

[1] D.R. BRILLINGER, *Time Series Data Analysis and Theory* (Holt, Rinehart and Winston, 1975).

[2] F. F. BONSALL et J. DUNCAN, *Numerical Ranges of Operators on Normed Spaces and Elements of Normed Algebras* (Cambridge University Press, 1971).

[3] K. YOSIDA, *Functional Analysis, 2nd ed.* (Springer-Verlag, 1968).

Received 21 October, 1985

Département de mathématiques,
statistiques et actuariat
Université Laval
Québec G1K 7P4
CANADA

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 3, June 1986 juin

PERIODICITE DES PUISSANCES D'UNE MATRICE DONT LES COEFFICIENTS APPARTIENNENT A UN CORPS FINI. APPLICATIONS.

Yves HELLEGOUARCH

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

Our aim is to determine the period of the sequence $m \longmapsto A^m$, A being an $n \times n$ matrix with entries in the finite field $\mathbb{F}_q$. As an application, an upper bound is given for the orders of the elements of $GL_n(\mathbb{F}_q)$.

1) Un résultat en caractéristique p.

On suppose que A est une matrice $n \times n$ à coefficients dans un corps k de caractéristique p. On désigne par $\bar{k}$ une clôture algébrique de k. On sait que A peut être mis sous forme de Jordan dans l'anneau $M_n(\bar{k})$, c'est-à-dire qu'il existe une matrice $P \in GL_n(\bar{k})$ telle que :

$$A = P \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_r \end{pmatrix} P^{-1} \tag{1}$$

où J_i est une matrice $n_i \times n_i$ du type $\begin{pmatrix} \lambda_i & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i \end{pmatrix}$, $\lambda_i \in \bar{k}$.

On pose : $\nu(A) = \sup \{n_1, \ldots, n_r\}$.

Théorème 1.-

On suppose que A a été mise sous forme de Jordan comme dans (1). Alors si $h \in \mathbb{N}$ est tel que $p^h \geq \nu(A)$, $P^{-1} A^{p^h} P$ est une matrice diagonale Δ.

Preuve :

1) On sait (produit par blocs) que :

$$A^{p^h} = P \begin{pmatrix} J_1^{p^h} & & \\ & \ddots & \\ & & J_r^{p^h} \end{pmatrix} P^{-1}$$

2) Maintenant pour tout i, $J = J_i$ est de la forme :

$$J = \lambda I + N$$

où N est une matrice nilpotente, et on a :

$$N^{\nu(A)} = 0, \qquad N^{\nu(A)-1} \neq 0$$

3) On en déduit que :

$$J^{p^h} = \lambda^{p^h} I + \sum_{i=1}^{p^h} \binom{p^h}{i} \lambda^{p^h - i} N^i = \lambda^{p^h} I$$

car $\binom{p^h}{i} = 0$ si $1 \leqslant i \leqslant p^h - 1$ et $N^{p^h} = 0$.

Remarque.-

Si $p^h < \nu(A)$ et si p ne divise pas e, A^{ep^h} n'est pas diagonale car $\binom{ep^h}{p^h} \equiv e \pmod{p}$.

2) Cas d'un corps fini.

On suppose que $k = \mathbf{F}_q$ avec $q = p^\alpha$, p premier, $\alpha \geqslant 1$. Si $\lambda_1, \ldots, \lambda_r$ sont les valeurs propres de A dans $\overline{k}$, on désigne par e_o le plus petit entier $e \geqslant 1$ tel que $\lambda_i^e \in \{0,1\}$ pour tout i.

Par ailleurs on désigne par h_o le plus petit entier h tel que $p^h \geqslant \nu(A)$.

Théorème 2.-

Avec les notations ci-dessus on a :

$$P^{-1} A^{e_o p^{h_o}} P = \mathcal{H}$$

où $\mathcal{H}$ est une matrice diagonale idempotente.

Corollaire 1.-

1) La suite (A^m) est périodique à partir de $m \geqslant e_o p^{h_o}$ et sa période est du type $e_o p^h$ avec $h \leqslant h_o$.

2) Si $A \in GL_n(\mathbf{F}_q)$, la suite (A^m) est purement périodique de période $e_o p^{h_o}$.

Preuve :

1) Il est clair que :

$$A^{2e_o p^{h_o}} = P\,\textcircled{H}^2\,P^{-1} = P\,\textcircled{H}P^{-1} = A^{e_o p^{h_o}}, \text{ etc.}$$

2) La période de (A^m) divise $e_o p^{h_o}$; elle est donc du type ep^h où e divise e_o et $h \leq h_o$. On doit avoir :

$$P^{-1} A^{ep^h} P\,\textcircled{H} = \textcircled{H}$$

on en déduit que $\lambda_i^e = 1$ pour tout i, donc $e = e_o$.

3) Si $A \in GL_n(\mathbb{F}_q)$, $\textcircled{H} = I$ et la remarque du paragraphe 1 entraîne que $h = h_o$.

3) Application à $GL_n(\mathbb{F}_q)$

On va montrer que le corollaire 1 donne des informations sur le groupe $GL_n(\mathbb{F}_q)$.

Soit $A \in GL_n(\mathbb{F}_q)$, on désigne par χ_A le polynôme caractéristique de A.

En décomposant χ_A en facteurs premiers on a :

$$\chi_A = P_1^{\alpha_1} \ldots P_s^{\alpha_s}$$

Posons $\deg P_i = d_i'$ et désignons par $[d_1,\ldots,d_s]$ le plus petit commun multiple de $d_1,\ldots,d_s$.

Corollaire 2.-

Soit $A \in GL_n(\mathbb{F}_q)$.

1) L'ordre de A dans le groupe $GL_n(\mathbb{F}_q)$ est l'égal à $e_o p^{h_o}$.

2) e_o divise $q^{[d_1,\ldots,d_s]} - 1$.

Définition.-

Soit $n \in \mathbb{N}$, on pose :

$$\theta(n) = \sup\{[n_1,\ldots,n_t],\ 1 \leq t \leq n,\ n_1+\ldots+n_t = n\}$$

Corollaire 3.-

Les ordres des éléments de $GL_n(\mathbb{F}_q)$ sont bornés supérieurement par

$[q^{\theta(n)}-1]p^{h(n)}$, $h(n)$ désignant le plus petit entier h tel que $p^h > n$.

4) Application à $\mathbb{F}_q[X]/(N)$.

A partir de résultats classique sur le groupe $(\mathbb{F}_q[X]/(N))^*$ on va obtenir des informations sur une application linéaire remarquable f.

N étant un polynôme de $\mathbb{F}_q[X]$ on pose : $|N| = q^{\text{degré}(N)}$.

Si N est unitaire sa décomposition en facteurs premiers s'écrit :

$$N = P_1^{\alpha_s} \dots P_s^{\alpha_s}$$

où les polynômes irréductibles P_i sont unitaires et distincts.

Si $\varphi(N)$ désigne l'ordre du groupe $(\mathbb{F}_q[X]/N))^*$ des éléments inversibles de $\mathbb{F}_q[X]/(N)$ on a :

$$\begin{cases} \varphi(N) = \varphi(P_1^{\alpha_1}) \dots \varphi(P_s^{\alpha_s}) \\ \varphi(P^\alpha) = |P|^{\alpha-1}(|P|-1). \end{cases}$$

Cette définition permet d'énoncer le théorème d'Euler :

Si $B \in \mathbb{F}_q[X]$ et $(B,N) = 1$, on a :

$$B^{\varphi(N)} \equiv 1 \pmod N$$

ou encore

$$B^{\varphi(N)+1} \equiv B \pmod N \tag{2}$$

Avant d'aller plus loin, rappelons le résultat suivant :

Théorème 3.-

1) Si N est irréductible, $(\mathbb{F}_q[X]/(N))^*$ est cyclique.

2) Si $q>2$ et si $(\mathbb{F}_q[X]/(N))^*$ est cyclique, N est irréductible.

Preuve :

1) est classique et 2) résulte de ce que si ℓ est un diviseur premier de $q-1$, $(\mathbb{F}[X]/(N))^*$ contient un sous-groupe isomorphe à $(\mathbb{Z}/\ell\mathbb{Z})^s$.

Considérons maintenant l'automorphisme de Frobenius : $B \xrightarrow{f} B^q \pmod N$ qui est en fait une application $\mathbb{F}_q$-linéaire de $\mathbb{F}_q[X]/(N)$ dans lui-même.

Si B désigne un vecteur propre de f associé à la valeur propre $\lambda=0$, on a :

$$B^q \equiv 0 \pmod{N}$$

et si N est sans facteur carrés on en déduit que

$$B \equiv 0 \pmod{N}$$

ce qui est absurde.

Il en résulte que si N est sans facteurs carrés, alors $f \in GL_n(\mathbb{F}_q)$, $n = \text{degré}(N)$.

Théorème 4.-

Soient e_o et h_o comme dans le théorème 2 et soit pour $1 \leq i \leq s$, $d_i = \deg(P_i)$.

1) On a toujours

$$f^{2e_o p^{h_o}} = f^{e_o p^{h_o}}$$

et $[d_1,\ldots,d_s]$ divise $e_o p^{h_o}$.

2) Si $[d_1,\ldots,d_s]$ n'est pas divisible par p on a :

$$[d_1,\ldots,d_s] = e_o.$$

3) Si N n'a pas de facteurs carrés on a :

$$f^{e_o p^{h_o}} = I, \quad I = \text{identité},$$

et

$$[d_1,\ldots,d_s] = e_o p^{h_o}.$$

Preuve :

Il s'agit de démontrer les assertions relatives à $[d_1,\ldots,d_s]$.

1) On utilise l'homomorphisme surjectif :

$$(\mathbb{F}_q[X]/(N))^* \xrightarrow{\varphi} (\mathbb{F}_q[X]/(P_1))^* \times \ldots \times (\mathbb{F}_q[X]/P_s))^*.$$

2) On remarque que ce dernier groupe est d'exposant $q^{[d_1,\ldots,d_s]}-1$ et que $\operatorname{Ker}\varphi$ est un p-groupe.

3) On choisit $B \in (\mathbb{F}_q[X]/(N))^*$ tel que $\varphi(B)$ soit d'ordre $q^{[d_1,\ldots,d_s]}-1$.

4) On spécialise la suite (f^m) en $(f^m(B))$ et on utilise les résultats du

paragraphe 2 en remarquant que pour m assez grand le comportement de $(f^m(B))$ représente celui de (f^m). On utilise le corollaire 1.

Remarques :

1) Si N est irréductible, $e_o p^{h_o} = n$.

2) Si N est un "polynôme de Carmichael" c'est-à-dire si N est réductible et si $B^{|N|-1} \equiv 1 \pmod N$ pour tout B premier à N, alors N est sans facteurs carrés et $e_o p^{h_o}$ divise n.

3) Si N est un polynôme de Carmichael tel que $e_o p^{h_o} = n$, on dira que N est un "polynôme de Carmichael fort".

Il existe une infinité de polynômes de Carmichael forts dans $\mathbb{F}_q[X]$, ils ont au moins trois facteurs irréductibles.

Exemple : $(d_1, d_2, d_3) = (d, 2d, 3d)$, $d \in \mathbb{N}$.

4) Si N est sans facteurs carrés, le rang de $f-I$ est égal à $n-s$ [1].

REFERENCE

[1] D.E. KNUTH, The Art of Computer programming, vol. 2, 1981, Addison-Wesley, p. 423.

Université de Caen, France.

Received 7 November, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 3, June 1986 juin

ESSENTIALLY MINIMAL TC-CLONES ON THREE-ELEMENT BASE SET

J. Demetrovics and I.A. Malcev

Presented by G.A. Grätzer F.R.S.C.

Let A be a finite set and f an n-ary operation on A. The operation f is said to satisfy the term condition, if for any i, $1 \leq i \leq n$, and for any x,y,

$$a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n,b_1,\ldots,b_{i-1},b_{i+1},\ldots,b_n \in A$$

$$f(a_1,\ldots,a_{i-1},x,a_{i+1},\ldots,a_n)=f(b_1,\ldots,b_{i-1},x,b_{i+1},\ldots b_n)$$

implies

$$f(a_1,\ldots,a_{i-1},y,a_{i+1},\ldots,a_n)=f(b_1,\ldots,b_{i-1},y,b_{i+1},\ldots,b_n).$$

In short, such operations will be called TC-operations.

We denote the set of all finitary operations over A by O_A. The operations in Post's preiterative algebra $\gamma^*_A = \langle O_A;\xi,\tau,\Delta,*\rangle$ of type (1,1,1,2) are defined by

$$(\xi f)(x_1,x_2,\ldots,x_n) = f(x_2,x_3,\ldots,x_n,x_1),$$

$$(\tau f)(x_1,x_2,\ldots,x_n) = f(x_2,x_1,x_3,\ldots,x_n),$$

$$(\Delta f)(x_1,x_2,\ldots,x_{n-1}) = f(x_1,x_1,x_2,\ldots,x_{n-1}),$$

$$(f*g)(x_1,x_2,\ldots,x_{n+m-1})=f(g(x_1,\ldots,x_m),x_{m+1},\ldots,x_{n+m-1});$$

for unary f: $\xi f = \tau f = \tau f = \Delta f$ (see [5]). Subalgebras of γ^*_A containing all projections e^i_n $(1 \leq i \leq n)$, defined by $e^i_n(x_1,\ldots,x_n)=x_i$, are called clones. The clone generated by the operations $f_1,\ldots,f_k$ will be denoted by $[f_1,\ldots,f_k]$.

A clone consisting of TC-operations is called a TC-clone. Every TC-clone on A is contained in a maximal TC-clone; on the two-element set there is a unique maximal TC-clone, on the three-element set - two, on the four-element set - 25 (see Berman and McKenzie [2]).

In the sequel we always take $A = \{0,1,2\}$. The two maximal TC-clones on A are L and B. Here L is the clone of linear operations, i.e. operations of the form

$$a_0 + a_1x_1 + a_2x_2 + \ldots + a_nx_n ,$$

where addition and multiplication is taken modulo 3. The lattice of subclones of L is finite, it was determined by Bagyinszki and Demetrovics.

The other maximal TC-clone, B, consists of the essentially unary operations on A and the operations of the form

$$f_0(f_1(x_1)+\ldots+f_n(x_n)),$$

where $f_0:\{0,1\}\to A$, $f_1,\ldots f_n:A\to\{0,1\}$ and the addition is modulo 2. This clone was first considered by Burle [3]. In the present paper we describe the lattice of subclones $L(Z)$ of the clone Z consisting of the projections and those members of Burle's clone which take values 0 and 1 only.

On the basis of this result we shall be able to determine all minimal and essentially minimal TC-clones on the three-element set (cf. Machida [4]).

We introduce the following notation for the eight unary functions taking values 0 and 1 only:

x	ϕ	ψ	γ	δ	$\bar{\phi}$	$\bar{\psi}$	c_0	c_1
0	0	0	0	1	1	1	0	1
1	1	1	0	1	0	0	0	1
2	0	1	1	0	1	0	0	1

Since $\delta(x)=1+\gamma(x)$, $\bar{\phi}(x)=1+\phi(x)$, $\bar{\psi}(x)=1+\psi(x)$, any operation in Z which is not a projection can be uniquely written in the form

$$h(x_1,\ldots,x_b)=c+\sum_{j=1}^{g}\gamma(x_{i_j})+\sum_{j=g+1}^{g+f}\phi(x_{i_j})+\sum_{j=g+f+1}^{g+f+p}\psi(x_{i_j})$$

where $c\in\{0,1\}$, $g,f,p\geq 0$ and the indices $1\leq i_1,\ldots,i_{g+f+p}\leq n$ are pairwise different. For short, we shall write $1+\gamma+\psi$ for $1+\gamma(x_1)+\phi(x_2)$, $\psi+\psi+\psi$ for $\psi(x_1)+\psi(x_2)+\psi(x_3)$, etc.

There is a regular pattern of infinitely many subclones of Z. Let we define the clones $J_{00}=E[e_2^1]$, $J_{10}=[c_0]$, $J_{01}=[c_1]$, $J_{m0}=[\sum_{i=1}^{m-1}\gamma(x_i)]$, $J_{0m}=[1+\sum_{i=1}^{m-1}\gamma(x_i)]$ $(m=2,3,\ldots)$, $J_{\infty 0}=\bigcup_{m=0}^{\infty}J_{m0}$, $J_o=\bigcup_{m=0}^{\infty}J_{0m}$, $J_{\ell m}=J_{\ell 0}\cup J_{0m}$ $(\ell,m=0,1,\ldots,\infty)$. We shall also write $W=J_{\infty\infty}$. Furthermore, let $E^{\phi}=[\phi]$, $E^{\psi}=[\psi]$, $J^{\phi}_{\ell m}=J_{\ell m}\cup E^{\phi}$, $J^{\psi}_{\ell m}=J_{\ell m}\cup E^{\psi}$, $J^{\phi\psi}_{\ell m}=J_{\ell m}\cup E^{\phi}\cup E^{\psi}$ $(\ell,m=0,1,\ldots,\infty)$. The lattice of subclones of $W_{\phi\psi}=J^{\phi\psi}_{\infty\infty}$ is shown on Fig.1.

Let $F^{\phi}_n=J_{nn}\cup[1+\phi]$. $F^{\psi}_n=J_{nn}\cup[1+\psi]$, $F^{\phi\psi}_n=J_{nn}\cup[1+\phi]\cup[1+\psi]$ $(n=0,1,\ldots,\infty)$. The lattice of subclones of $F^{\phi\psi}_{\infty}$ is shown on Fig. 2.

The remaining part of the lattice $L(Z)$ contains finitely many elements and has less regular structure. We have the clones $L_{\phi}=[\phi+\phi+\phi]$, $L_{\psi}=[\psi+\psi+\psi]$, $S_{\phi}=[\phi+\phi]$, $S'_{\psi}=[1+\psi+\psi]$, $L'_{\phi}=[1+\phi+\phi+\phi]$, $L'_{\psi}=[1+\psi+\psi+\psi]$, $S'_{\phi}=[1+\phi+\phi]$, $S_{\psi}=[\psi+\psi]$, $U_{\phi}=[\phi+\phi,\ 1+\phi+\phi]$, $U_{\psi}=[\psi+\psi,1+\psi+\psi]$, $L_{\phi+\gamma}=[\phi+\gamma]$, $L_{\phi\psi}=[\phi+\phi+\phi,\psi+\psi+\psi]$, $L_{\phi+\delta}=[1+\gamma+\phi]$, $L^1_{\phi\psi}=[1+\phi+\psi+\psi]$, $H_{\phi}=[\gamma+\phi,\ c_0]$, $H_{\psi}=[\gamma+\psi,\ c_1]$, $H_{\phi\psi}=[\gamma+\phi,c_0,c_1]$, $G=[\gamma+\phi,1+\phi,c_0]$, $S_{\phi\psi}=[\phi+\psi]$, $S'_{\phi\psi}=[1+\phi+\psi]$, $Z=[\phi+\psi,1+\phi]$.

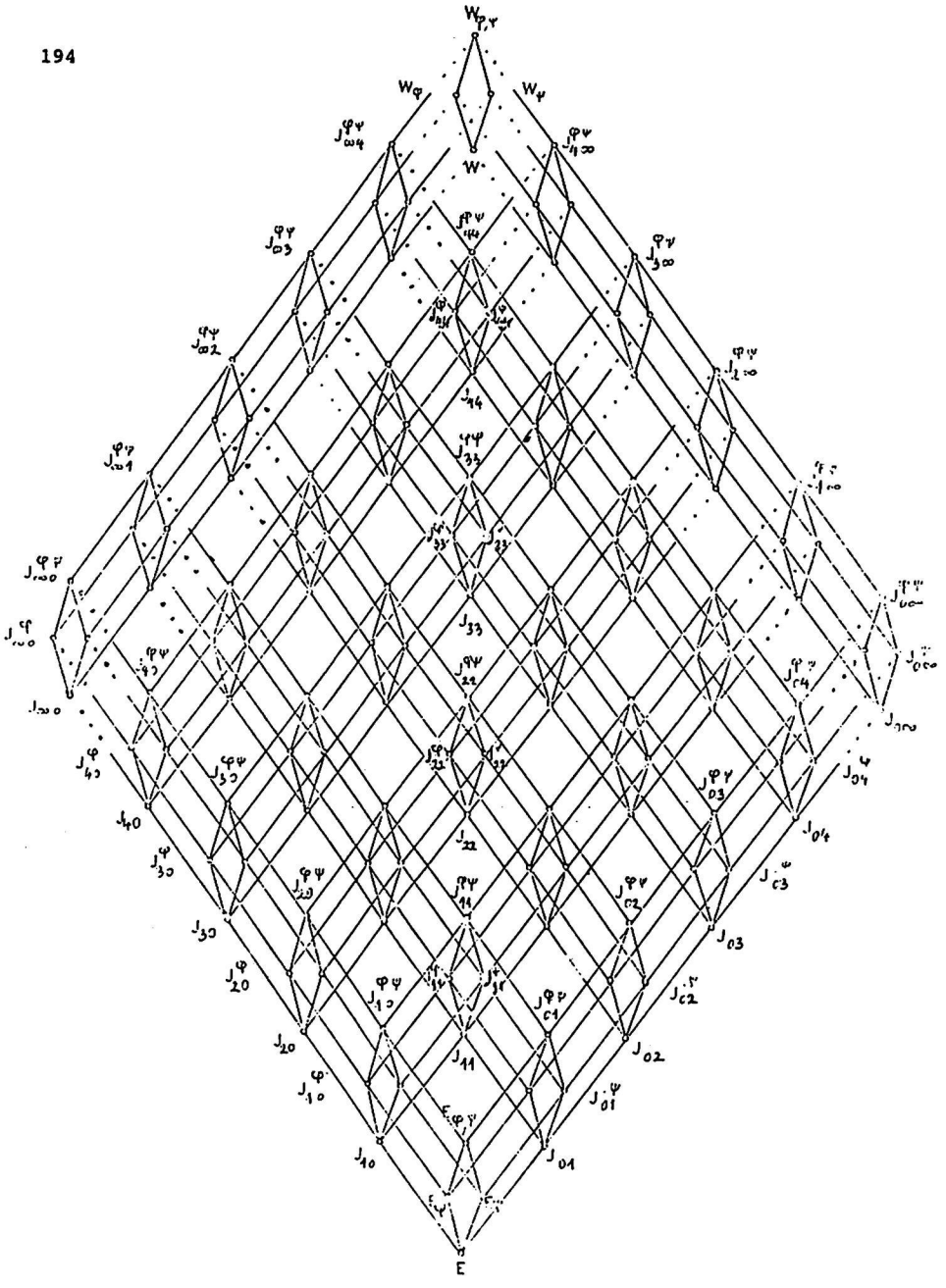

Figure 1.

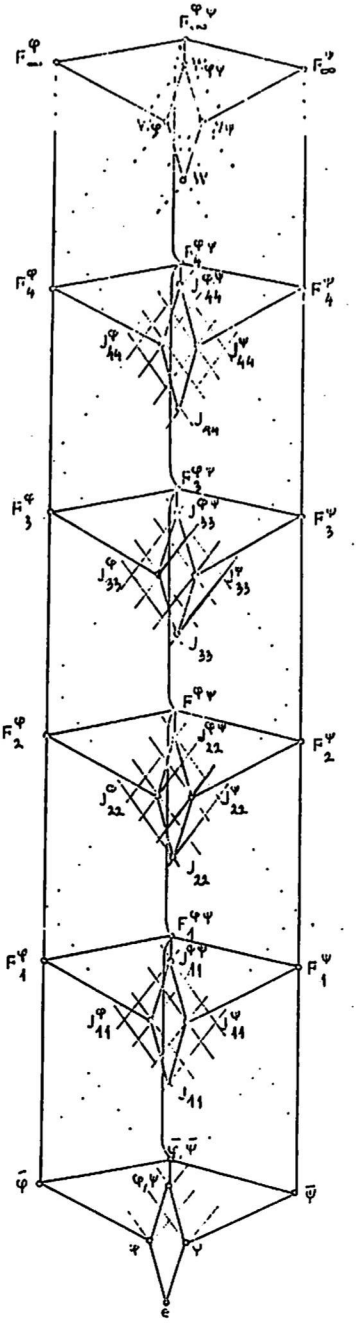

Figure 2.

As an application we can determine all minimal and essentially minimal TC-clones on $\{0,1,2\}$. For this we need some more notation. In the clone L of linear operations modulo 3 let $\xi(x)=2x, \pi(x)=x+1$, and $L'=[2x_1+2x_2]$.

Theorem. Up to permutations of the base set the minimal TC-clones on $\{0,1,2\}$ are $[\phi]$, $[c_0]$, $[\xi]$, $[\pi]$ and L'; the essentially minimal TC-clones are L_ϕ, $L_{\phi+\gamma}$, J_{30} and L'.

References

1 J. Bagyinszki and J. Demetrovics, The lattice or linear classes in prime-valued logics, in: Discrete Mathematics, Banach Center Publ., vol. 7, Warsaw (1982), 105-123.

2 J. Berman and R. McKenzie, Clones satisfying the term condition, Discrete Math. 52(1984), 7-29.

3 G.A. Burle, Classes is k-valued logic containing all one-variable functions (in Russian), Discret. Analiz 10(1967), 3-7.

4 H. Machida, Toward a classification of minimal closed sets in 3-valued logic, Proc. 12th Intl. Symp. on multiple-valued logic, Paris (1982), 313-317.

5 A.I. Malcev, Post's iterative algebras (in Russian), Novosibirsk, 1976.

I.A. Malcev
Math. Inst. Siberian Branch, Acad. Sci. USSR,
630090 Novosibirsk 90, USSR

J. Demetrovics
Computer and Automation Inst. Hungarian Acad. Sci.
H-1132 Budapest, Victor Hugo u. 18-22.

Received 5 December, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol.VIII, No.3, June 1986 juin

HIGHER ORDER POLYMORPHIC LAMBDA CALCULUS AND CATEGORIES II

R.A.G. Seely

Presented by J. Lambek F.R.S.C.

Abstract A definition of "polymorphic lambda calculus with subtypes" is given, together with a suitable categorical semantics. (Equality subtypes may be defined in this context.) A technique for constructing models of this theory is illustrated by application to the well-known model of closure operators in $P\omega$.

0. Introduction This note is a sequel to [5], in which the basic definitions of PL theory and PL category are given. Here we extend the notion of a PL theory to include equality as a type; the corresponding strengthening of the notion of a PL category has finite limits in the fibres. However, we must be a little careful, as a naive approach can yield inconsistency, as Girard showed [1]. We shall see the type theory we present is consistent by constructing a model. This construction is a quotient of a general construction on indexed categories, due to F. Lamarche [2] generalising the "Freyd cover" construction for toposes [3].

1. Discussion/Definition 1 We begin with a strengthening of the notion of PL theory [5], by adding the type formation rule for Σ, corresponding term formation rules, and corresponding equalities. (These may be found in [1], or deduced from the semantics below; note that as in [5] we must include equality rules for "expansions" (η rules), as well as for "reductions" (β rules).) A PLS theory has in addition subtypes, where (s, X) is a subtype of a type s if s is a type with, say, a free indeterminate α of

order A, and X is a function, which to each closed operator u of order A assigns a set X(u) of closed terms of type $s[u/\alpha]$, (s with u replacing α). Furthermore, a term of subtype (s,X) with free variable of subtype (t,Y) is an equivalence class of terms a of type s with a free variable x of type t satisfying: for each closed operator $u \in A$, for each closed term b of type $t[u/\alpha]$ in Y(u), $a[b/x]$ is in X(u). Note that variables are always such terms. Two such terms a_1 and a_2 are equivalent if for all $u \in A$, $b \in Y(u)$, $a_1[b] = a_2[b]$. In particular, given terms a_1, a_2 of type s or of subtype (s,X), with the same free variable of type t or of subtype (t,Y), we have an "equality type" $E(a_1,a_2)$, a subtype of t, consisting of those terms b for which $a_1[b] = a_2[b]$.

Remark Morally speaking, the addition of Σ to the type theory does not take us significantly beyond PL theories as defined in [5]; the corresponding categorical semantics would be simply PL categories for which κ has a left adjoint Σ. (Henceforth we shall use "PL theory/category" in this extended sense.) The category (G,K) of closure operators [5] is such a category. What is new is the notion of subtype, and the resulting inclusion of equality (sub)types; the categorical semantics must be modified to a greater degree, and some work is required to get a model out of (G,K), which is done by the construction of §3.

Definition 2 A PLS category (G,S) consists of:

(i) A category S with finite products, a distinguished object Ω, and exponentiation of the form Ω^A for A in S, and

(ii) an indexed category G over S satisfying

(a) for each A in S, $G(A)$ is "subrepresentable on objects by Ω": there is a full subcategory $\underline{Rep}_G(A) \subseteq G(A)$ so that $Obj(\underline{Rep}_G(A)) \cong Hom_S(A,\Omega)$, every object of $G(A)$ is a subobject of a representable object (ie one in $\underline{Rep}_G(A)$), and every morphism in $G(A)$ lifts to a moprhism in $\underline{Rep}_G(A)$ between the corresponding representable objects; furthermore, for each $f:A \to B$ of S, f^* acts as $Hom(f,\Omega)$ on $\underline{Rep}_G(A)$;

(b) for each A in S, $G(A)$ is catesian closed, has finite limits and this structure is preserved by all f^*;

(c) G is "complete and cocomplete": for each C in S, the canonical indexed functor $\kappa : G \to G^C$ has both adjoints $\Sigma \dashv \kappa \dashv \Pi$;

(d) as a subindexed category, $(\underline{Rep}_G, S)$ is a PL category.

2. Equivalences It is routine to extend the equivalences of categories in [5] to show PLS theories equivalent to PLS categories.

3. The construction of models Every PL category (with Σ) can be extended to a PLS category; we illustrate this by constructing a PLS category $(\tilde{G},K)$ from (G,K). Recall K is the category of closure operators in $P\omega$[4]. For $d \in K$, $T(d)$ is the set of fixed points of d, and $G(d)$ is the category $[T(d),K]$ of continuous functions $T(d) \to K$. For each $d \in K$, an object of $\tilde{G}(d)$ is a pair $\langle a,X \rangle$, $a:d \to V$ in K and X a function $T(d) \to PP\omega$ so that $X(t) \subseteq T(a(t))$ for all $t \in T(d)$. (Recall $T(V) = K$.) A morphism $f: \langle a,X \rangle \to \langle b,Y \rangle$ of $\tilde{G}(d)$ is (represented by) a morphism $f:a \to b$ of $G(d)$, so that $f(t)^{-1}X(t) : X(t) \to Y(t)$ for all $t \in T(d)$. (Two such morphisms f,g are equal if $f(t)^{-1}X(t) = g(t)^{-1}X(t)$ for all $t \in T(d)$.) For a morphism $g:d \to e$ in K, g^* is defined by composition, making

$(\tilde{G},K)$ an indexed category.

Proposition $(\tilde{G},K)$ is a PLS category.

Proof The representable objects are of the form $<a,T(a(\ ))>$. Equalisers are given by $E(f,g)$. $\Pi,\Sigma\colon \tilde{G}^c(d) \to \tilde{G}(d)$ are defined by $\Pi <a,X> = <\Pi(a), \Pi s \in T(c).X(<s,>)>$, and $\Sigma <a,X> = <\Sigma(a), \Sigma s \in T(c).X(<s,>)>$, where $\Pi(a)$ and $\Sigma(a)$ are defined as in (G,K) by composition with $\Pi_c,\Sigma_c\colon c \supset V \to V$, $\Pi_c = \lambda x\lambda y\lambda z \in c.x(z)(y(z))$ and $\Sigma_c = \lambda x\lambda <t \in c,y>.<t,x(t)(y)>$.

Remarks 1. By definition, every PLS category (G,S) induces a PL category $(\underline{Rep}_G,S)$: however this process is not inverse to the construction of §3. In fact, $(\underline{Rep}_{\tilde{G}},S)$ is a quotient of (G,S); one could say a PL theory was extensional if its PL category $(G,S) \cong (\underline{Rep}_{\tilde{G}},S)$.

2. In the closure operator model, $\tilde{G}(1)$ has a natural numbers object with standard numerals, viz $<N,X>$, where $N = \lambda x\lambda y \in V.y\cdot x(y)\cdot(y\times(y \supset y))$ (ie the interpretation of $\Pi\alpha.(\alpha\times(\alpha \supset \alpha)) \supset \alpha)$ and X is the set of "Church numerals" (iterations of evaluation): $\underline{0} =$ " $\Lambda\alpha\ \lambda<x,y>.x$", $S\underline{n} =$ " $\Lambda\alpha\ \lambda <x,y>.y(\underline{n}\{\alpha\}\ (x,y))$". So $(\tilde{G},K)$ models Girard's original system, and hence provides an example of a context in which the Dialectica interpretation can be defined, say, as a functor from the free topos with natural numbers object to the $\exists\forall$ category of a PLS category with a stable natural numbers object.

References

[1] Girard, J.-Y., "Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre superieur", Ph.D. Thesis, Université Paris VII (1972).

[2] Lamarche, F., Unpublished lecture notes, McGill University, September 1985.

[3] Lambek, J. and P.J. Scott, Introduction to Higher Order Categorical Logic, Cambridge Studies in Advanced Mathematics 7 (Cambridge University Press, 1986).

[4] Scott, D.S., Data types as lattices, SIAM J. Comput.5(1976) 522-587.

[5] Seely, R.A.G., Higher order polymorphic lambda calculus and categories, (this journal, 1986). Errata Add to Definition 1:
Operators: $T \in \Omega$ Terms: $* \in T$
Equalities: $t = *$ for all $t \in 1$; $a = *$ for all $a \in T$.

Department of Mathematics
John Abbott College
CP 2000
Ste. Anne de Bellevue
Quebec H9X 3L9

Received 23 January, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, June 1986 Juin

UNE PROPRIETE DES COURBES TRACEES SUR UNE SUFFACE DE DEGRE INFERIEUR OU EGAL A TROIS

J.D'ALMEIDA

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

Résumé

Soit X une courbe lisse irréductible de degré d tracée sur une surface de degré inférieur ou égal à trois de P^3. On note J_X l'idéal de X dans $\mathcal{O}_{P^3}$. Pour $n > d/2 - 1$, $H^1(P^3, J_X(n))$ est non nul si et seulement si X a une (n+2)-sécante.

Soit X une courbe lisse irréductible non dégénérée de degré d et de genre g de P^3 (espace projectif de dimension trois sur le corps des complexes). On note J_X le faisceau d'idéaux définissant X dans P^3. Dans [4] on montre que $H^1(J_X(n))$ est nul pour $n \geq d-2$ et que $H^1(J_X(d-3))$ est non nul si et seulement si X a une (d-1)-sécante (une k-sécante est une droite qui rencontre X en k points.). Dans ce même article on a la conjecture suivante:

Conjecture: Pour $n > 2d/3 - 1$, $H^1(J_X(n))$ est non nul si et seulement si X a une (n+2)-sécante.

Cette conjecture a été vérifiée dans [1] pour n = d-4. On se propose ici de démontrer le théorème suivant:

Théorème: Soit X une courbe lisse irréductible de degré d tracée sur une surface de degré inférieur ou égal à trois de P^3. Pour $n > d/2 - 1$, $H^1(J_X(n))$ est non nul si et seulement si X a une (n+2)-sécante.

Démonstration: Une courbe tracée sur un cône du second degré est suivant la parité de d intersection complète ou liée à une droite par le cône et une surface de degré d+1. Elle est donc arithmétiquement normale.

Pour une courbe tracée sur une quadrique lisse c'est à dire une section de $\mathcal{O}(p,q)$ $(p \leq q)$ on a $\max \{n / H^1(J_X(n)) \neq 0\}$ $= q-2$ si $p \leq q-2$. Les cas $p=q-1$ et $p=q$ correspondent aux courbes arithmétiquement normales. Il reste à considérer les cas suivants:

a) X est sur une surface cubique lisse

b) X est sur une surface cubique normale

c) X est sur une surface cubique réglée

a) X est sur une surface cubique lisse

On utilisera les notations suivantes (cf [5]). Soit S une surface cubique lisse de P^3. Le faisceau des formes de degré deux sur S est $\omega_S = \mathcal{O}_S(-1)$. Soit Δ un $\mathcal{O}_S$-module inversible tel que $(\Delta, \Delta) = 1$ et $(\Delta, \omega_S) = -3$. induit un morphisme $S \longrightarrow P^2$ qui est l'éclatement de 6 points en position générale. Si on note E_i $(1 \leq i \leq 6)$ les diviseurs exceptionnels. $(\Delta, -E_1, \quad , -E_6)$ est une base de Pic S. Pour tout module inversible L il existe Δ tel que les

coordonnées ($\delta, m_1, \ldots, m_6$) vérifient $\delta \geqslant m_1+m_2+m_3$ et $m_1 \geqslant m_2 \geqslant \ldots \geqslant m_6$. Si X est section d'un tel faisceau, on a $H^1(J_X(n)) = H^1(L^V(n))$. On peut trouver sur S une droite rencontrant X en $2\delta - m_2 - m_3 - \ldots - m_6$ points. Il suffit donc de montrer que $H^1(L^V(n)) = 0$ pour $n \geqslant 2\delta - m_2 - m_3 - \ldots - m_6 - 1$. Si on pose $A = L^V(2\delta - m_2 - \ldots - m_6)$, on vérifie qu'une section générale de A est une courbe lisse et connexe ([3] Ex 4.8) Il en résulte que $H^1(A(-1)) = (H^1(A^V))^V = 0$.

b) X est sur une surface cubique normale

On se ramène au cas précédent en utilisant l'argument de [5] théorème 2.11

c) X est sur une surface cubique réglée

On utilisera le résultat suivant démontré dans [1]:

Proposition [1] : Soit S une surface de P^3 dont la normalisée $\tilde{S}$ est lisse, J_Γ l'idéal de $\mathcal{O}_{P^3}$ image réciproque du conducteur $\mathrm{Hom}(\mathcal{O}_{\tilde{S}}, \mathcal{O}_S) \subset \mathcal{O}_S$, Γ la courbe de P^3 d'idéal J_Γ $\tilde{X}$ une courbe tracée sur $\tilde{S}$, section d'un $\mathcal{O}_{\tilde{S}}$-module inversible L: on note X l'image de $\tilde{X}$ dans P^3 et s le degré de S. Si $h^1(J_X(n)) > 0$ alors $h^1(L(s-n-4)) > 0$ ou $h^1(J_X \otimes \mathcal{O}_\Gamma(n)) > 0$

On utilise cette proposition dans le contexte suivant: Soient C une courbe lisse, E un $\mathcal{O}_C$-module localement libre de rang 2 et de degré s, $\tilde{S} = P(E)$, $\pi : \tilde{S} \to C$ la projection $\mathcal{O}_{\tilde{S}}(1)$ le quotient tautologique de π^*E. L'application

$(A,k) \longrightarrow \pi^*A \otimes \mathcal{O}_{\tilde{S}}(k)$ identifie $Pic(C) \oplus Z$ et $Pic(\tilde{S})$.

La matrice de la forme d'intersection est:

$$\begin{pmatrix} 0 & 1 \\ 1 & s \end{pmatrix}$$

Le $\mathcal{O}_{\tilde{S}}$-module $\omega_{\tilde{S}}$ est isomorphe à $\pi^*(\omega_C \otimes \wedge^2 E) \otimes \mathcal{O}_{\tilde{S}}(-2)$

$\tilde{X}$ est section de :

$$L = \pi^*(\wedge^2 E^v)^{\otimes k} \otimes \mathcal{O}_{\tilde{X}}(1) \otimes \mathcal{O}_{\tilde{S}}(k)$$

En utilisant la suite spectrale $H^p R^q \pi_* L(s-n-4) \Rightarrow H^n L(s-n-4)$ la proposition précédente admet le corollaire suivant:

Corollaire: Si $h^1(J_X(n)) > 0$, alors $h^1(J_X \otimes \mathcal{O}_\Gamma(n)) > 0$

ou $\quad h^0(((\wedge^2 E)^{\otimes k+1})^v \otimes \mathcal{O}_{\tilde{X}}(1) \otimes Sym_{n+2-k-s} E^v) > 0$

Revenons à la surface cubique réglée .On a $C = P^1$, $E = \mathcal{O}(1) \oplus \mathcal{O}(2)$, $J_\Gamma = \omega_{\tilde{S}}(1)$ .Le lieu double de S est la droite Γ . Γ est une (d-k)-sécante.Il suffit donc de montrer que $h^1(J_X(n)) = 0$ pour $n \geqslant d-k-1$.Pour cela on utilise le corollaire précédent:$J_X \otimes \mathcal{O}_\Gamma(n)$ est un $\mathcal{O}_{P^1}$ module inversible de degré n-d+k et $Sym_{n-k-1} E^v$ est une somme directe de modules inversibles de degré inférieur ou égal à k-n.

On a donc montré dans tous les cas que la condition $H^1(J_X(n))$ non nul pour un entier n entraine l'existence d'une droite ayant au moins (n+2) points d'intersection avec la courbe X.

Supposons maintenant qu'il existe une droite ayant au moins (n+2) points d'intersection avec la courbe X. D'après [3] on a $H^1(J_X(n)) \neq 0$ ou $H^1(\mathcal{O}_X(n-1)) \neq 0$. Mais $H^1(\mathcal{O}_X(t)) = 0$ pour $t > d/2 - 2$ ([2]) .

Références

[1] J.D'ALMEIDA, Courbes de l'espace projectif: Séries linéaires incomplètes et multisécantes: à paraître au "Journal fur die reine und angew. Mathematik"

[2] G.HALPHEN, Mémoire sur la classification des courbes gauches algébriques (Oeuvres complètes t III)

[3] R.HARTSHORNE, Algebraic Geometry, Springer Verlag

[4] L.GRUSON, C.PESKINE, R.LAZARSFELD, On a theorem of Castelnuovo and the equations defining space curves Inv Math n°72 1983

[5] L.GRUSON, C.PESKINE, Genre des courbes de l'espace projectif II Ann scient Ec.Norm.Sup 4è série t 15 1982

JEAN D'ALMEIDA

Département de Mathématiques

Université de CAEN

CAEN , FRANCE

Received 3 February, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 3, June 1986 juin

UN EXEMPLE D'ANNEAU CATENAIRE

G. NACHAR

Presented by J.G. Arthur F.R.S.C.

RESUME. — Dans cet article, on donne un exemple d'un anneau T non noethérien et non prüférien tel que :

1) T[[Z]] est caténaire ;
2) dim T[[Z]] = dim T + 1.

INTRODUCTION. — Soient D un anneau intègre, commutatif et unitaire, D[[X]] l'anneau des séries formelles en X sur D. Si I est un idéal de D, on note I[[X]] l'idéal de D[[X]] formé des éléments de D[[X]] dont les coefficients sont dans I. L'idéal de D[[X]] engendré par I se note ID[[X]]. Evidemment, ID[[X]] $\subseteq$ I[[X]]. On dit que I est un SFT-idéal (idéal strong finite type) s'il existe un entier positif k et un idéal de type fini J $\subseteq$ I tels que $x^k \in J$ pour tout élément x de I. L'anneau D sera dit un SFT-anneau si tous ses idéaux sont des SFT-idéaux. On rappelle que l'anneau D est dit caténaire si pour tout couple d'idéaux premiers (P,Q) de hauteurs finis, toutes les chaînes saturées d'idéaux premiers d'origine P et d'extrémité Q sont finies et ayant la même longueur.

Dans la littérature, plusieurs auteurs ont étudié la caténarité des anneaux de polynômes sur un anneau noethérien ou prüférien [5] et [10]. De plus, dans le cas des anneaux de séries formelles sur un anneau noethérien ou prüférien, on trouve des conditions nécessaires et suffisantes pour que D[[X]] soit caténaire [4], [6], [8], [9]. Le but essentiel de cet article est de montrer qu'il existe un anneau T qui n'est ni noethérien, ni prüférien tel que T[[X]] soit caténaire et dim T[[X]] = dim T + 1.

Soient $\mathbb{Z}_{(2)}[[X]]$ l'anneau des séries formelles en X sur $\mathbb{Z}_{(2)}$ et K son corps des fractions. On note $T = \mathbb{Z}_{(2)}[[X]] + YK[[Y]]$ le sous-anneau de K[[Y]] formé des séries dont les termes constants sont dans $\mathbb{Z}_{(2)}[[X]]$. On note dimT la dimension de Krull de T.

PROPOSITION 1. — *Dans l'anneau T, les propriétés suivantes sont vérifiées :*

1) *T est un anneau local.*

2) *T admet un seul idéal premier minimal non nul.*

3) *T est un SFT-anneau caténaire et* dim T = 3.

DEMONSTRATION. — Soit $\varphi : T \longrightarrow \frac{T}{YK[[Y]]} \simeq \mathbb{Z}_{(2)}[[X]]$ la surjection canonique, φ induit une bijection croissante entre le spectre premier de $\mathbb{Z}_{(2)}[[X]]$ et l'ensemble des idéaux premiers de T contenant $\text{Ker}\,\varphi = YK[[Y]] = P_1$. Puisque ht $P_1 = 1$, P_1 est un idéal premier minimal non nul de T. De plus, l'anneau $\mathbb{Z}_{(2)}[[X]]$ est local, régulier, de dimension de Krull deux dont l'idéal maximal est (2,X) ([8], lemme 1). De plus, si Q est un idéal premier de $\mathbb{Z}_{(2)}[[X]]$, ht Q = 1, alors Q est engendré par un élément irréductible de $\mathbb{Z}_{(2)}[[X]]$. D'autre part, il est évident que $f = a_o + Yg$ est un élément inversible de T si et seulement si a_o l'est dans $\mathbb{Z}_{(2)}[[X]]$. Soient P_2 un idéal premier non nul de T, $P_2 \neq P_1$, et $f = a_o + Yg$ un élément de $P_2 \setminus P_1$, alors $a_o \neq 0$ et $a_o = b_o f_1^{n_1} f_2^{n_2} \dots f_s^{n_s}$ où f_i est un élément irréductible de $\mathbb{Z}_{(2)}[[X]]$, $1 \leq i \leq s$, et b_o est un élément inversible de $\mathbb{Z}_{(2)}[[X]]$. Donc $\varphi(f) = \varphi(a_o) = b_o \bar{f}_1^{n_1} \bar{f}_2^{n_2} \dots \bar{f}_s^{n_s}$ est un élément de $\varphi(P_2) = \bar{P}_2$ qui est un idéal premier de $\frac{T}{P_1} \simeq \mathbb{Z}_{(2)}[[X]]$. On en déduit qu'il existe un entier positif k avec $1 \leq k \leq s$, tel que $(\bar{f}_k) = \bar{P}_2$ et par conséquent, $P_2 = (f_k, P_1) \supsetneq P_1$. Il s'en suit que P_1 est le seul idéal premier minimal non nul de T et T est un anneau local, caténaire de dimension de Krull trois : (dim T = dim $\mathbb{Z}_{(2)}[[X]]$ + 1 = 2 + 1 = 3).

Il nous reste à montrer que T est un SFT-anneau. Soit Y_g un élément de P_1, $(Yg)^2 = Y.Yg^2 \in YT \subsetneq P_1$. Donc P_1 est un SFT-idéal. De plus $Yg = f \cdot \frac{Yg}{f}$ pour tout élément irréductible f de $\mathbb{Z}_{(2)}[[X]]$. Donc, si P est un idéal premier de T de hauteur deux, P est prinicpal. Si ht P = 3, P = (X,t) est l'unique idéal maximal de T. Il en résulte que tous les idéaux premiers de T sont des SFT-idéaux et par conséquent T est un SFT-anneau ([2], prop. 2.2, page 2).

Il est clair que l'anneau T n'est ni noethérien, ni prüférien. On considère l'anneau $T[[Z]] = (\mathbb{Z}_{(2)}[[X]] + YK[[Y]])[[Z]]$.

PROPOSITION 2. — *Soit* P_1 *l'idéal premier minimal non nul de T alors*

$$T_{P_1}[[Z]]_{T_{P_1} \setminus \{0\}} = T[[Z]]_{T \setminus \{0\}} .$$

DEMONSTRATION. — Soit $f = \sum_{i=o}^{\infty} \frac{a_i}{b_i} Z^i$ un élément de $T_{P_1}[[Z]]$, alors $b_i \in T \setminus P_1$. Pour tout entier positif i, l'élément $Y \frac{a_i}{b_i} \in YK[[Y]] \subset T$. Par conséquent, $Yf \in T[[Z]]$ et $f = \frac{Yf}{Y} \in T[[Z]]_{T \setminus \{0\}}$. D'autre part, puisque $\operatorname{Frac} T \subset T[[Z]]_{T \setminus \{0\}}$, on a :

$$T_{P_1}[[Z]]_{T_{P_1} \setminus \{0\}} \subseteq T[[Z]]_{T \setminus \{0\}}.$$

L'inclusion inverse est évidente.

COROLLAIRE 1. — *Dans les conditions de la proposition précédente, il existe une bijection croissante entre l'ensemble des idéaux premiers Q de* $T[[Z]]$ *tels que* $Q \cap T = \{0\}$ *et l'ensemble des idéaux premiers Q' de* $T_{P_1}[[Z]]$ *tels que* $Q' \cap T_{P_1} = \{0\}$.

COROLLAIRE 2. — *Soit* $(0) \subsetneqq Q_1 \subsetneqq Q_2$ *une chaîne saturée d'idéaux premiers de* $T[[Z]]$ *telle que* $Q_1 \cap T = (0)$, *alors* $Q_2 \cap T \supsetneq (0)$.

DEMONSTRATION. — Il est clair que T_{P_1} est un suranneau de valuation discrète de T et d'après ([8], lemme 3), le corollaire est évident.

PROPOSITION 3. — *Dans l'anneau* $T[[Z]]$, $\operatorname{ht} P_1[[Z]]$ *vaut un*.

DEMONSTRATION. — Puisque T est un SFT-anneau, $P_1[[Z]] = \sqrt{P_1 T[[Z]]}$ ([1], théorème 1), donc $P_1[[Z]]$ est le plus petit idéal premier Q' de $T[[Z]]$ tel que $Q' \cap T = P_1$. Supposons qu'il existe un idéal premier Q de $T[[Z]]$ tel que $(0) \subsetneqq Q \subsetneqq P_1[[Z]]$, alors $Q \cap T = (0)$ et $Q \subsetneqq YT \subseteq P_1[[Z]]$. Soit $f = \sum_{i=o}^{\infty} a_i Z^i \in Q$, $f \in YT$ donc $f = Yg_1$. Or $Y \notin Q$ donc $g_1 \in Q$ et $g_1 = Yg_2$, $g_2 \in Q$ et $f = Yg_1 = Y^2 g_2 = \ldots = Y^n g_n$ pour tout entier positif n. D'autre part, $a_i \in P_1$ donc pour tout entier positif i, il existe n_i tel que $a_i = Y^{n_i} h_i$, $h_i \in K[[Y]]$. Soit $n_o = \inf(\{n_i\})$, alors $f = Y^{n_o+1} \sum_{i=o}^{\infty} \frac{a_i}{Y^{n_o+1}} Z^i$ et $\frac{a_{n_o}}{Y^{n_o+1}} = Y^{n_o} \frac{h_{n_o}}{Y^{n_o+1}} = \frac{h_{n_o}}{Y} \in P_1$. En particulier on peut supposer que $h_{n_o} = 1$ d'où $\frac{1}{Y} \in P_1$ ce qui est absurde car $Y \in P_1$.

THEOREME 1. — *L'anneau* $T[[Z]]$ *est caténaire et* $\dim T[[Z]] = 4$.

DEMONSTRATION. — Il est clair que $T[[Z]]$ est un anneau local d'idéal maximal (M,Z) où M est l'idéal maximal de T ([8], lemme 1). Soit

$(0) \subsetneq Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_s \subsetneq Q_{s+1} = (M,Z)$ une chaîne saturée d'idéaux premiers de $T[[Z]]$ telle que $Q_1 \cap T = (0)$. Alors $Q_2 \cap T = P \neq (0)$. Montrons que $P = P_1$.

Supposons que $Q_2 \cap T = M$. Puisque $M[[Z]] = \sqrt{MT[[Z]]}$, alors $M[[Z]] \subseteq Q_2 \subseteq (M,Z)$ et $Q_2 = M[[Z]]$ ou $Q_2 = (M,Z)$ $\left(\dim \frac{T[[Z]]}{M[[Z]]} = 1\right)$.

Supposons que $Q_2 = (M,Z)$ alors la chaîne $(0) \subsetneq Q_1 \subsetneq (M,Z)$ est saturée. Soit (W,Q_2') un suranneau de valuation de $T[[Z]]$ dont $(0) \subsetneq Q_1' \subsetneq Q_2'$ sont des idéaux premiers tels que $Q_1' \cap T[[Z]] = Q_1$ et $Q_2' \cap T[[Z]] = (M,Z)$ ([7], corollaire 19.7, p. 229). On peut supposer que $\mathrm{ht}\, \frac{Q_2'}{Q_1'} = 1$ (on prend $Q_2' = \sqrt{YW}$ et $Q_1' = \bigcap_{i=1}^{\infty} Y^i W$ ([7], théorème 17-1, p. 187). Soit $V = W \cap K$, V est un suranneau de valuation de $\mathbb{Z}_{(2)}[[X]]$ dont $(0) \subseteq S_1 \subsetneq S_2$ sont des idéaux premiers tels que $S_2 \cap \mathbb{Z}_{(2)}[[X]] = (2,X)$ et $S_1 \cap \mathbb{Z}_{(2)}[[X]] = (0)$. Evidemment, $\mathrm{ht}\, \frac{S_2}{S_1} = 1$. Montrons que $S_1 = (0)$. Soit $f \in V_{S_1}$, $f \in K$ et $f = \frac{g}{h}$; $g,h \in \mathbb{Z}_{(2)}[[X]]$. Puisque $S_1 \cap \mathbb{Z}_{(2)}[[X]] = (0)$, g et h sont deux éléments inversibles de V_{S_1}, f est donc inversible dans V_{S_1}, d'où la contradiction. Il en résulte que $S_1 = (0)$ et V est un suranneau de valuation de $\mathbb{Z}_{(2)}[[X]]$ de dimension un donc $V = \mathbb{Z}_{(2)}[[X]]_{P'}$, ou P' est un idéal premier de $\mathbb{Z}_{(2)}[[X]]$ de hauteur un. Il s'en suit que $S_2 \cap \mathbb{Z}_{(2)}[[X]] \subsetneq (2,X)$ d'où la contradiction . On en déduit que $Q_2 \subsetneq (M,Z)$. Le même argument invoqué ci-dessus montre que $Q_2 \neq M[[Z]]$ et $Q_2 \cap T = P \subsetneq M$.

Supposons que $\mathrm{ht}\, P = 2$, on construit de la même manière (W,Q_2') un suranneau de valuation de $T[[Z]]$ dont $(0) \subsetneq Q_1' \subsetneq Q_2'$ sont des idéaux premiers tels que $Q_i' \cap T[[Z]] = Q_i$, $1 \leq i \leq 2$ et on suppose que $\mathrm{ht}\, \frac{Q_2'}{Q_1'} = 1$ (voir ci-dessus). Soit $K' = \mathrm{Frac}\, T$, on note $V' = W \cap K'$, V' est un suranneau de valuation de T dont $(0) \subseteq N_1' \subsetneq N_2'$ sont des idéaux premiers tels que $N_i' = Q_i' \cap K'$, $1 \leq i \leq 2$. Il est clair que $V' = T_S = \mathbb{Z}_{(2)}[[X]]_S + YK[[Y]]$ pour un certain idéal premier S de T. Il en résulte que $N_1' \neq (0)$ d'où $Q_1' \cap T \neq (0)$, ce qui est en contradiction avec l'hypothèse que $Q_1' \cap T = (0)$. On en déduit que $P = P_1$.

D'autre part, soit $\psi : T[[Z]] \longrightarrow \frac{T[[Z]]}{P_1[[Z]]} \simeq \frac{T}{P_1}[[Z]] \simeq \mathbb{Z}_{(2)}[[X,Z]]$ la surjection canonique, ψ induit une bijection croissante entre le spectre premier de $\mathbb{Z}_{(2)}[[X,Z]]$ et l'ensemble des idéaux premiers de $T[[Z]]$ contenant $P_1[[Z]] = \mathrm{Ker}\, \psi$. De plus $\mathbb{Z}_{(2)}[[X,Z]]$ est un anneau caténaire ([5], théorème 12) et ([6], corollaire, p. 593).

Soit $(0) \subsetneq Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_s \subsetneq (M,Z)$ une chaîne saturée d'idéaux premiers de $T[[Z]]$.

1er CAS. — Si $Q_1 \cap T = P_1$, $P_1[[Z]] \subseteq Q_1$. Puisque $\text{ht}\, Q_1 = \text{ht}\, P_1[[Z]] = 1$, $Q_1 = P_1[[Z]]$ et la longueur de cette chaîne vaut quatre.

2ème CAS. — Si $Q_1 \cap T = (0)$, $Q_2 \cap T = P_1$, $P_1[[Z]] \subsetneq Q_2$ et $\text{ht}\, \frac{Q_2}{P_1[[Z]]} = 1$ et la longueur de cette chaîne vaut toujours quatre, d'où le résultat.

REFERENCES

[1] J.T. ARNOLD, "Krull dimension in power series rings", trans of the A.M.S., vol. 177, p. 299-304, (1973).

[2] J.T. ARNOLD, "Power series rings over Prüfer domains", Pac. J. of Math. Vol. 44, p. 1-11, (1973).

[3] J.T. ARNOLD, "Power series rings with finite Krull dimension", Indiana University Math. J., Vol. 31, n° 6, p. 897-911, (1982).

[4] J.T. ARNOLD, "The catenarian property of power series rings over a Prüfer domain", Proc. of the A.M.S., Vol. 94, n° 4, p. 577-580, (1985).

[5] A. BOUVIER and M. FONTANA, "The catenarian property of the polynomial rings over a Prüfer domain", Séminaire d'Algèbre P. DUBREIL et M.P. MALLIAVIN, Lecture Notes in Math. Springer, BERLIN - NEW YORK

[6] S. DOERING and Y. LEQUAIN, "Chain of primes ideals in formal power series rings", Proc. of the A.M.S., Vol. 88, n° 4, p. 591-594, (1983).

[7] R. GILMER, "Multiplicative ideal theory", Marcel DEKKER, NEW YORK, 1972.

[8] G. NACHAR, "Sur la caténarité des anneaux de séries formelles sur un anneau de valuation discrète". (Soumis à une publication).

[9] G. NACHAR, "Sur la caténarité des anneaux de séries formelles sur un anneau de Prüfer". (Soumis à une publication).

[10] L. RATTLIF, "On Quasi-unmixed local domains, the altitude formula, and the chain condition for prime ideal (I)", Ann. J. Math., Vol. 91, p. 508-528, (1969).

G. NACHAR
Université Claude Bernard - Lyon I
Département de Mathématiques
43, boulevard du 11 Novembre 1918
69622 VILLEURBANNE CEDEX - FRANCE.

Received 3 February, 1986

C.R. Math. Rep. Acad. Canada - Vol.VIII, No. 3, June 1986 juin

POWERFUL NUMBERS AND FERMAT'S LAST THEOREM

Andrew Granville

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

A powerful number n is a positive integer with the property that p^2 divides n whenever prime p divides n.

Mollin and Walsh conjectured [4] that there does not exist three consecutive powerful numbers and gave some strong numerical evidence.

Recently Adleman and Heath-Brown [1], using a result of Fouvry [3] on the Brun-Titchmarsh inequality, showed that the first case of Fermat's Last Theorem is true for infinitely many primes p.

We shall show that if the conjecture of Mollin and Walsh is true then the Adleman-Heath-Brown theorem follows immediately.

Lemma

If p is a prime such that p^2 divides 2^p-2 and m is a positive integer for which p divides 2^m-1 then p^2 divides 2^m-1.

Proof: Let r be the greatest common divisor of m

and $p-1$. Clearly p divides 2^r-1 .

Suppose $2^r = 1 + ap$.

Then $2^{p-1} = (2^r)^{(p-1)/r} = (1+ap)^{(p-1)/r}$

$$\equiv 1 + a \cdot \frac{p-1}{r} \cdot p \bmod p^2 \ .$$

But $2^{p-1} \equiv 1 \mod p^2$, so that p divides a .

Thus $2^r \equiv 1 \mod p^2$ and as r divides m ,

$2^m \equiv 1 \mod p^2$.

THEOREM

If the conjecture of Mollin and Walsh is true then there exists an infinite sequence of primes p for which p^2 does not divide 2^p-2 .

Proof: Suppose p^2 divides 2^p-2 for all primes $p > p_0$.

Let $t = \prod_{p \le p_0} p$, and $A = 2^{t\phi(t)}$ where $\phi(\cdot)$ is Euler's function. We claim that A^n-1 is powerful for any positive integer n .

For, if $2 < p \le p_0$, $p \cdot p-1 \mid t\phi(t)$ and so $A \equiv 1 \mod p^2$.

Thus $A^n \equiv 1 \mod p^2$ for each positive integer n .

If $p > p_0$ and $p|A^n-1$ then $p|2^{nt\phi(t)}-1$. By the lemma $p^2|2^{nt\phi(t)}-1$ that is p^2 divides A^n-1 .

Thus A^n-1 is powerful.

So $A-1$ and A^2-1 are both powerful.

But gcd $(A-1,A+1)$ = gcd $(2,A-1)$ = 1 as 2 divides A .

Thus, as $A^2-1 = A-1 \cdot A+1$, we know $A+1$ is also powerful. But then $A-1$, A , $A+1$ are three consecutive powerful numbers, which contradicts the conjecture of Mollin and Walsh,

Wieferich [5] showed the following:

If x , y and z are positive integers and p is a prime, for which

$$x^p + y^p = z^p \quad \text{with} \quad p \nmid xyz$$

then p^2 divides 2^p-2 .

(See a recent elegant proof by Agoh [2].)

So, by the theorem and Wieferich's criteria, we can immediately state the following.

Corollary

If the conjecture of Mollin and Walsh is true then there exists an infinite sequence of primes p for which the First

References

1. Adleman, L.M. and Heath-Brown, D.R., 'The First Case of Fermat's Last Theorem,' Invent. Math. 79, 409-415 (1985).

2. Agoh, T., 'On the Criteria of Wieferich and Mirimanoff,' C. R. Math. Rep. Acad. Sci. Canada, 8, 49-52 (1986).

3. Fouvry, E., 'Théorème de Brun-Titchmarsh. Application au Théorème de Fermat,' Invent. Math. 79, 383-407 (1985).

4. Mollin, R.A. and Walsh, P.G., 'A Note on Powerful Numbers, Quadratic Fields and the Pellian,' C. R. Math. Rep. Acad. Sci. Canada, 8, (1986), to appear.

5. Wieferich, A., 'Zum letzten Fermat'schen Theorem,' J. reine u. angew Math. 136, 293-302 (1909).

Received 12 February, 1986

Department of Mathematics
and Statistics
Queen's University
Kingston, Ontario
Canada, K7L 3N6

C.R. Math. Rep. Acad. Sci. Canada Vol. VIII, No. 3, June 1986 juin

ON CONTINUOUS MULTILINEAR MAPPINGS

Jürg Rätz

Presented by J. Aczél F.R.S.C.

Abstract. If X and Y are topological vector spaces and $h:X\longrightarrow Y$ a linear mapping, then it is a familiar fact that continuity of h at 0 implies uniform continuity of h. We show in this note that if $f:X_1\times\ldots\times X_n\longrightarrow Y$ is a multilinear mapping, then continuity of f at $(0,\ldots,0)$ implies that f is a Cauchy morphism.

1. For uniform spaces $(X,\mathcal{U})$, $(Y,\mathcal{V})$, a mapping $f:X\longrightarrow Y$ is called a Cauchy morphism or Cauchy-regular if it satisfies one and therefore all of the following equivalent conditions:

(I) f preserves Cauchy filterbases.

(II) f preserves Cauchy nets.

(III) If $(\tilde{X},\tilde{\mathcal{U}})$ is a uniform space, X a dense uniform subspace of $\tilde{X}$ and Y complete, then there exists a continuous extension $g:\tilde{X}\longrightarrow Y$ of f.

In (III), if Y is separated, then g is uniquely determined (cf. [1],p.91,Théorème 1; [4], [5], [7]). - It then follows

(*) f uniformly continuous $\Longleftrightarrow$ f Cauchy morphism $\Longleftrightarrow$ f continuous.

Examples of not necessarily uniformly continuous Cauchy morphisms in connection with topological groups may be found, e.g., in [2],§6, nos 5 and 6; [5], section 3.

Throughout the paper, K will denote a field equipped with a non-trivial valuation $|.|:K\longrightarrow R_+$, so that for all $\alpha,\beta\in K$ we have $|\alpha|=0$ if and only if $\alpha=0$, $|\alpha+\beta|\leq|\alpha|+|\beta|$, $|\alpha\beta|=|\alpha|\cdot|\beta|$, and that there exists $\alpha_0\in K\setminus\{0\}$ with $|\alpha_0|\neq 1$. The metric $|\alpha-\beta|$

then makes K into a separated topological field. The subfields of the complex number field C with its ordinary and those of the Hensel fields Q_p with their p-adic valuations are examples of the type required here.

A topological vector space over such a $(K,|.|)$ will briefly be called a topological $(K,|.|)$-vector space. If $X_1,\ldots,X_n$ are topological $(K,|.|)$-vector spaces, it is understood that $X_1\times\ldots\times X_n$ be furnished with the algebraic and topological product structure, making it into a topological $(K,|.|)$-vector space. Of course, all uniform notions in connection with a topological $(K,|.|)$-vector space refer to the natural uniformity of its additive group.

2. It has been pointed out by many authors that multilinear mappings which are continuous at $(0,\ldots,0)$ are continuous everywhere (for a general version cf. [3],p.I.8, Proposition 5; the proof of our Theorem 1 is partially inspired by that procedure). In contrast to the situation for linear mappings, uniform continuity cannot be expected in case that $n \geq 2$, for there are as well-known counterexamples as inner products are, but (see (*)) the following weaker result holds:

Theorem 1. Let K be a field, $|.|:K\longrightarrow R_+$ a nontrivial valuation, $n\in N$, $n \geq 2$, and $X_1,\ldots,X_n,Y$ topological $(K,|.|)$-vector spaces. If the multilinear mapping $f:X_1\times\ldots\times X_n\longrightarrow Y$ is continuous at $(0,\ldots,0)$, it is a Cauchy morphism ([6], Theorem 2).

Proof. Let $(x_\delta)_{\delta\in D}$, more briefly (x_δ), be a Cauchy net of elements of $X_1\times\ldots\times X_n$. Since $X_1\times\ldots\times X_n$ is a uniform product space, (*) and (II) imply that

(1) $(\mathrm{pr}_i x_\delta)$ is a Cauchy net on X_i $(i = 1,\ldots,n)$.

Let W be an arbitrary neighborhood of 0 in Y. We have to show that for sufficiently "large" $\delta,\delta' \in D$ we get $f(x_{\delta'})-f(x_\delta) \in W$. Continuity of addition in Y ensures the existence of a neighborhood W_1 of 0 in Y such that

(2) the $n.2^{n-1}$-fold sum $W_1+\ldots+W_1$ is contained in W.

From continuity of f at $(0,\ldots,0)$ and $f(0,\ldots,0) = 0$ we obtain a neighborhood $U_1\times\ldots\times U_n$ of $(0,\ldots,0)$ in $X_1\times\ldots\times X_n$ with

(3) $\qquad f(U_1\times\ldots\times U_n) \subset W_1.$

Without loss of generality we may assume that

(4) $U_1,\ldots,U_n$ are circled and absorbing sets.

([3],p.I.7, Proposition 4). By (1) there exists $\delta_i \in D$ such that $\delta,\delta' \in D$, $\delta_i \leq \delta$, $\delta_i \leq \delta'$ imply $pr_i x_{\delta'}-pr_i x_\delta \in U_i$. Directedness of $(D,\leq)$ implies the existence of $\gamma \in D$ with $\delta_i \leq \gamma$ $(i=1,\ldots,n)$, so

(5) $\delta,\delta' \in D$, $\gamma \leq \delta$, $\gamma \leq \delta'$, $i \in \{1,..,n\} \Longrightarrow pr_i x_{\delta'}-pr_i x_\delta \in U_i$.

We define the auxiliary element $w \in X_1\times\ldots\times X_n$ by

(6) $\qquad w := x_\gamma$, $w = (w_1,\ldots,w_n)$.

By (4) there exist $\rho_i \in K$ with $0 < |\rho_i| \leq 1$ and $\rho_i w_i \in U_i$ $(i=1,\ldots,n)$. Let be $\rho \in K$ such that $|\rho| > 1$, $|\rho| \geq |\rho_i|^{-1}$ $(i=1,..,n)$.

(7) $V_i := \rho^{-n}U_i$ is a neighborhood of 0 in X_i $(i=1,\ldots,n)$.

For every subset J of $\{1,\ldots,n\}$ we have $|\prod_{k\in J} \rho_k^{-1}| = \prod_{k\in J}|\rho_k|^{-1} \leq |\rho|^{\text{card } J} \leq |\rho|^n = |\rho^n|$, hence $|(\prod_{k\in J} \rho_k^{-1})\rho^{-n}| \leq 1$, thus by (4) and

(7) $(\prod_{k\in J} \rho_k^{-1})V_i = (\prod_{k\in J} \rho_k^{-1})\rho^{-n}U_i \subset U_i$, i.e.,

(8) $i \in \{1,\ldots,n\}$, $J \subset \{1,\ldots,n\} \Longrightarrow (\prod_{k\in J} \rho_k^{-1})V_i \subset U_i$.

By (7) and (1) there exists $\gamma_i \in D$ such that $\delta,\delta' \in D$, $\gamma_i \leq \delta$, $\gamma_i \leq \delta'$ imply $pr_i x_{\delta'}-pr_i x_\delta \in V_i$. Directedness of $(D,\leq)$ leads to $\gamma' \in D$ with $\gamma_i \leq \gamma'$ $(i=1,\ldots,n)$, so that we get

(9) $\delta,\delta' \in D$, $\gamma' \le \delta$, $\gamma' \le \delta'$, $i \in \{1,\dots,n\} \Longrightarrow pr_i x_\delta - pr_i x_{\delta'} \in V_i$.

Now there exists $\gamma_0 \in D$ with $\gamma \le \gamma_0$ and $\gamma' \le \gamma_0$.

We choose $\delta,\delta' \in D$ with $\gamma_0 \le \delta$, $\gamma_0 \le \delta'$ arbitrary and fix them for the next step of the proof. Accordingly, we use the abbreviations

(10) $x_i := pr_i x_\delta$, $x_i' := pr_i x_{\delta'}$ $(i = 1,\dots,n)$.

From (5), (10), (6), and the definition of ρ_i we get

(11) $x_i' - w_i \in U_i$, $x_i - w_i \in U_i$, $\rho_i w_i \in U_i$ $(i = 1,..,n)$

and from (9) moreover $x_i' - x_i \in V_i$ $(i = 1,..,n)$, thus by (8)

(12) $i \in \{1,\dots,n\}$, $J \subset \{1,\dots,n\} \Longrightarrow (\prod_{k\in J} \rho_k^{-1})(x_i' - x_i) \in U_i$.

Now everything is prepared for making an additive decomposition efficient:

$$f(x_1',\dots,x_n') - f(x_1,\dots,x_n) =$$

$$\sum_{i=1}^{n} [f(x_1,..,x_{i-1},x_i',x_{i+1}',..,x_n') - f(x_1,..,x_{i-1},x_i,x_{i+1}',..,x_n')] =$$

(13)
$$\sum_{i=1}^{n} f(x_1,..,x_{i-1},x_i'-x_i,x_{i+1}',\dots,x_n') =$$

$$\sum_{i=1}^{n} f(x_1-w_1+w_1,..,x_{i-1}-w_{i-1}+w_{i-1},x_i'-x_i,x_{i+1}'-w_{i+1}+w_{i+1},..,x_n'-w_n+w_n)$$

$$= \sum_{i=1}^{n} \sum_{J\subset\{1,..,n\}\setminus\{i\}} f(z_{1,J},..,z_{i-1,J},x_i'-x_i,z_{i+1,J},..,z_{n,J})$$

where $z_{k,J} := w_k$ for $k \in J$, $z_{k,J} := x_k - w_k$ for $k \in \{1,..,n\}\setminus J$ and $k < i$, $z_{k,J} := x_k' - w_k$ for $k \in \{1,..,n\}\setminus J$ and $k > i$. For

$$\tilde{z}_{k,J} := \begin{cases} \rho_k w_k & (k \in J) \\ z_{k,J} & (k \in \{1,..,n\}\setminus(J\cup\{i\})) \end{cases}$$

multilinearity of f together with (11), (12), and (3) yield

(14) $f(z_{1,J},..,z_{i-1,J},x_i'-x_i,z_{i+1,J},\dots,z_{n,J}) =$

$$f(\tilde{z}_{1,J},..,\tilde{z}_{i-1,J},(\prod_{k\in J}\rho_k^{-1})(x_i'-x_i),\tilde{z}_{i+1,J},\dots,\tilde{z}_{n,J}) \in W_1.$$

From (10), (13), (14), we obtain $f(x_{\delta'})-f(x_\delta) = f(x_1',..,x_n')-f(x_1,..,x_n) \in W_1+...+W_1$ ($n\cdot 2^{n-1}$ summands) and from (2) finally $f(x_{\delta'})-f(x_\delta) \in W$.

Since W was an arbitrary neighborhood of 0 in Y, $(f(x_\delta))_{\delta\in D}$ is a Cauchy net in Y, and since $(x_\delta)_{\delta\in D}$ was an arbitrary Cauchy net in $X_1\times..\times X_n$, f is a Cauchy morphism.

Theorem 2. Let $X_1,..,X_n,Y$ be topological $(K,|.|)$-vector spaces, Y in addition complete and separated, S_i a dense linear subspace of X_i ($i = 1,..,n$), and $f:S_1\times..\times S_n \longrightarrow Y$ multilinear and continuous. Then there exists a unique continuous extension $g:X_1\times..\times X_n \longrightarrow Y$ of f, and g is multilinear.

Proof. $X_1\times..\times X_n = \overline{S_1}\times..\times\overline{S_n} = \overline{S_1\times..\times S_n}$ guarantees that $S_1\times..\times S_n$ is a dense linear subspace of $X_1\times..\times X_n$. By Theorem 1, f is a Cauchy morphism, and by (III) f then has a unique continuous extension $g:X_1\times..\times X_n \longrightarrow Y$. Let be $i\in\{1,..,n\}$ and $\alpha,\beta\in K$ arbitrary but fixed. By virtue of the continuity of the linear operations in X_i and Y and the projection mappings, it is easily seen that the mapping $\varphi:((x_1,..,x_n),(z_1,..,z_n)) \longmapsto g(x_1,..,\alpha x_i+\beta z_i,..,x_n) - \alpha g(x_1,..,x_i,..,x_n) - \beta g(x_1,..,z_i,..,x_n)$ is continuous. Since f is multilinear, φ vanishes on $(S_1\times..\times S_n)\times(S_1\times..\times S_n)$, and separatedness of Y makes φ vanish identically. As i,α,β were arbitrary, g is multilinear.

References

[1] BOURBAKI, N., Topologie générale, chap. 1 et 2, 4e édition, Hermann, Paris 1965.

[2] BOURBAKI, N., Topologie générale, chap. 3 et 4, 3e édition, Hermann, Paris 1960.

[3] BOURBAKI, N., Espaces vectoriels topologiques, chap. 1 à 5, Masson, Paris 1981.

[4] RÄTZ, J., Remark 1. The 20th International Symposium on Functional Equations. Aequationes Math. 24 (1982) 287-288.

[5] RÄTZ, J., Another note on Cauchy-regular functions. Publ. Inst. Math. Beograd 33 (47)(1983) 197-202.

[6] RÄTZ, J., Some remarks on continuous multimorphisms between topological groups. The 21st International Symposium on Functional Equations. Aequationes Math. 26 (1984) 248.

[7] SNIPES, R.F., Cauchy-regular functions. J. Math. Anal. Appl. 79 (1981) 18-25.

Mathematisches Institut
Universität Bern
Sidlerstr. 5
CH-3012 Bern, Schweiz

Received 27 February, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 3, June 1986 juin

ON INFLECTIONAL SPACE CURVES WITH FOUR VERTICES

Tibor Bisztriczky

Presented by H.S.M. Coxeter F.R.S.C.

The Four-vertex theorem for curves in Eucledian three-space E_3 states that a sufficiently differentiable simple curve lying on a "suitable" convex surface possesses at least four "vertices". Sufficiently differentiable implies that the exceptional points of the curves are vertices (points with a stationary osculating plane), and spheres and ovaloids are examples of suitable surfaces.

Not much is known about space curves with exactly four vertices, and it is the aim of this note to gather some (closely related) results about such curves and to present a purely geometric condition which they must satisfy.

1. A brief history

The above sufficiently differentiable curves are called inflectional and we define them synthetically.

Let $p,q,\ldots,L,M,\ldots$ and $\alpha,\beta,\ldots$ denote respectively the points, lines and planes of E_3, and let $\langle p,L,\alpha,\ldots\rangle$ denote the flat of E_3 spanned by $p,L,\alpha,\ldots$.

A curve Γ is a continuous map from a circle $C \subset E_3$ into E_3. A line, denoted by $\Gamma_1(t)$, is the tangent of Γ at t if $\Gamma_1(t) = \lim_{t\neq s\to t} \langle \Gamma(t),\Gamma(s)\rangle$ and a plane, denoted by $\Gamma_2(t)$, is the osculating plane of Γ at t if $\Gamma_2(t) = \lim_{t\neq s\to t} \langle \Gamma_1(t),\Gamma(s)\rangle$. We identify Γ with $\Gamma(T)$ and assume that $\Gamma_1(t)$ and

$\Gamma_2(t)$ exist, and depend continuously on t, for each $t \in C$. As we are interested in Γ with exactly four vertices, we may also assume that $|\alpha \cap \Gamma| < \infty$ for any $\alpha \subset E_3$. We call such a curve, a differentiable space curve.

Let $\Gamma(t) \in \alpha$. Then $|\alpha \cap \Gamma| < \infty$ implies that near $\Gamma(t)$, either Γ lies on one side of α or Γ lies on both sides of α. In case of the former [latter], we say that α supports [cuts] Γ at t. We set $\Gamma_0(t) = \Gamma(t)$ and

$$S_i(t) = \{\alpha \subset E_3 | \alpha \cap \Gamma_{i+1}(t) = \Gamma_i(t)\} , \quad i = 0,1 .$$

It is known that either all $\alpha \in S_i(t)$ support Γ at t or all $\alpha \in S_i(t)$ cut Γ at t. We say that Γ is inflectional if for any $t \in C$, $\alpha \in S_0(t)[S_1(t)]$ cuts [supports] Γ at t. Let Γ be inflectional. Then a point $\Gamma(t)$ is regular if $\Gamma_2(t)$ cuts Γ at t and a vertex [inflection] if $\Gamma_2(t)$ supports Γ at t. We denote by $n(\Gamma)$, the number of vertices of Γ.

Henceforth, Γ is a simple (no self-intersections) differentiable inflectional space curve. We note that if Γ lies on a convex surface then Γ lies on the boundary of its convex hull $H(\Gamma)$. If $\Gamma \subset \partial H(\Gamma)$ and $|L \cap \Gamma| \leq 2$ for any L, we say that Γ is convex. If $4 = \max\{|\alpha \cap \Gamma| \mid \alpha \subset E_3\}$, we say that Γ is of order four. If for $\Gamma(s) \neq \Gamma(t)$ there is an α, continuously dependent on $\Gamma(s)$ and $\Gamma(t)$, such that $\alpha \cap \Gamma = \{\Gamma(s),\Gamma(t)\}$, we say that Γ is strictly-convex. We note that a strictly-convex curve is convex. Finally, a chord of Γ is a closed line segment bounded by two points of Γ.

Of the numerous articles on the Four-vertex theorem for inflectional space curves; we cite [1] for strictly-convex curves, [8] for spherical curves and [3] for convex curves. As the following results indicate, each of these deals with curves with exactly four vertices and with this intention, we also cite [6] for curves of order four. For an extensive history, we refer to [2].

1. ([1]) Let $\Gamma \subset E_3$ be strictly-convex. Then $n(\Gamma) = 4$ if and only if Γ is of order 4.

2. ([8] and [3]) Let $\Gamma \subset E_3$ be convex. Then $n(\Gamma) = 4$ if and only if each point of int $H(\Gamma)$ lies on the osculating plane of exactly four points of Γ, and none of these four points is a vertex of Γ.

3. ([6]) Let $\Gamma \subset E_3$ be of order four. Then $n(\Gamma) = 4$ if and only if Γ is convex.

4. Let $\Gamma \subset E_3$ be convex. If Γ is of order four then $n(\Gamma) = 4$.

We note that 4 follows from the Four-vertex theorem and the fact that a curve of order four has at most four inflections; cf. [6]. Since the "order four" property characterizes strictly-convex Γ with $n(\Gamma) = 4$ and a convex Γ need not be strictly-convex, it is not reasonable to expect the converse of 4 to be true. A more promising approach is indicated by

5. ([6]) Let $\Gamma \subset E_3$ be of order four. If $n(\Gamma) = 4$ then each point of int $H(\Gamma)$ lies on exactly two chords of Γ.

We claim that this geometrical result, without the equality, can be extended to convex curves and conjecture that the converse of 5 is true for convex curves.

2. Inflectional space curves

Since strictly-convex and spherical curves are convex, we assume from now on that $\Gamma: C \longrightarrow E_3$ is a simple, differentiable inflectional convex space curve with $n(\Gamma) = 4$. We then note (cf. [3]) that $\Gamma_1(t) \cap \text{int } H(\Gamma) = \emptyset$ for $t \in C$.

Let P_3 be the projective closure of E_3. We extend our notation to P_3 and fix a $\beta \subset P_3$ such that $\beta \cap H(\Gamma) = \emptyset$. For $b \in \operatorname{int} H(\Gamma)$, we define $\Gamma^b(t) = \langle b,\Gamma(t)\rangle \cap \beta$ and $\Gamma_1^b(t) = \langle b,\Gamma_1(t)\rangle \cap \beta$; $t \in C$. Then $\Gamma^b : C \longrightarrow \beta$ is a differentiable plane curve with the tangent $\Gamma_1^b(t)$ at $t \in C$. We call Γ^b the projection of Γ from b on β.

A point of Γ^b is regular [singular] if Γ^b is [not] locally convex at the point. Clearly, $|L \cap \Gamma^b| < \infty$ for any $L \subset \beta$ and thus a singular point of Γ^b is a cusp, a beak or an inflection. Next let $\Gamma^b(t) \in L \subset \beta$. Then L supports [cuts] Γ^b if near $\Gamma^b(t)$, Γ^b lies on one side [both sides] of L. Thus L supports Γ^b at t if and only if $\langle b,L\rangle$ supports Γ at t.

We now list some properties that $\Gamma^b \subset \beta$ may possess. We say that Γ^b is inflectional if every singular point of Γ^b is an inflection. Next Γ^b is unbounded if every line in β meets Γ^b, and Γ^b is even if every line in β cuts Γ^b at an even number of points. Finally, Γ^b is pseudoline if Γ^b is simple and $\beta \setminus \Gamma^b$ is connected. We note that pseudolines need not be differentiable.

6. LEMMA. *Let Γ^b be the projection of Γ from b on β; $b \notin \operatorname{int} H(\Gamma)$ and $\beta \cap H(\Gamma) = \emptyset$. Then*

6.1 *Γ^b is inflectional, and $\Gamma^b(t)$ is an inflection if and only if $b \in \Gamma_2(t)$ and $\Gamma(t)$ is not a vertex of Γ,*

6.2 *Γ^b has exactly four inflections and*

6.3 *Γ^b is even and unbounded.*

PROOF. We refer to [3] for the proof of 6.1, and observe that 6.1 and 2 imply 6.2. Since Γ is a closed curve in E_3 and $b \in \operatorname{int} H(\Gamma)$, every plane through b cuts Γ at a positive even number of points and thus 6.3. □

Finally, the proof of our claim is based on

7. ([4]) A simple, even, unbounded, differentiable inflectional curve in a real projective plane has at least six inflections.

8. THEOREM. Let $\Gamma: C \longrightarrow E_3 \subset P_3$ be a simple, differentiable inflectional convex space curve with $n(\Gamma) = 4$. Then each $b \in \operatorname{int} H(\Gamma)$ lies on at least two chords of Γ.

PROOF. Let Γ^b be the projection of Γ from $b \in \operatorname{int} H(\Gamma)$ on β, $\beta \cap H(\Gamma) = \emptyset$. Since Γ is simple, Γ^b possesses at most double points. By 6 and 7, Γ^b is not simple and there are $s \neq t$ in C such that $p = \Gamma^b(s) = \Gamma^b(t)$ and $b \in \langle \Gamma(s), \Gamma(t) \rangle \cap \operatorname{int} H(\Gamma)$. Suppose that p is the only double point of Γ^b. We claim that

(1) Γ^b does not cross itself at p; hence, $\Gamma_1^b(s) = \Gamma_1^b(t) = N$ and N supports Γ^b at s and t, and

(2) N does not cut Γ^b at any point.

Let C be oriented and denote by $[s,t]$ ($[t,s]$) the closed oriented arcs of C from s to t [t to s]. Then $\Gamma^b[s,t]$ and $\Gamma^b[t,s]$ are simple closed curves which meet only at p. We note that Γ^b crosses itself at p if and only if $\Gamma^b[s,t]$ and $\Gamma^b[t,s]$ do not cross at p. Let $p \notin L \subset \beta$. Then $\langle b,L \rangle \cap \langle \Gamma(s), \Gamma(t) \rangle = b$, $\langle b,L \rangle$ strictly separates $\Gamma(s)$ and $\Gamma(t)$ in $H(\Gamma)$ and $\langle b,L \rangle$ cuts each of $\Gamma[s,t]$ and $\Gamma[t,s]$ at an odd number of points. Thus L cuts each of $\Gamma^b[s,t]$ and $\Gamma^b[t,s]$ at an odd number of points and it follows that these two simple curves are pseudolines. Then (cf. [5]) $\Gamma^b[s,t] \cap \Gamma^b[t,s] = p$ yields that the curves cross at p.

Since $N = \Gamma_1^b(s) = \Gamma_1^b(s)$ supports Γ^b at s and t, we can deform (cf. the deformations alpha and delta in [7]) Γ^b slightly at $\Gamma^b(s)$ or $\Gamma^b(t)$ in such a

manner as to break the contact at p while preserving every other property of Γ^b. We thus obtain a simple, even, differentiable inflectional curve with exactly four inflections. By 7, this curve is not unbounded and it must be disjoint from some line arbitrarily close to N. Clearly, this is possible only if Γ^b lies locally one side of N at each point of $N \cap \Gamma^b$; that is, (2).

Since $\langle b,N \rangle$ supports Γ^b at each point of contact and $\Gamma \subset \partial H(\Gamma)$ is a closed curve, it follows that $\langle b,N \rangle$ supports $H(\Gamma)$ and thus $b \in \partial H(\Gamma)$; a contradiction. □

REFERENCES

[1] M. Barner, Über die Mindestanzahl stationärer Schmiegebenen bei geschlossenen streng-konvexen Raumkurven. Abh. Math. Sem. Univ. Hamburg, 20 (1956), 196-215.

[2] M. Barner and F. Flohr, Der Vierscheitelsatz und seine Verallgemeinerungen. Der Math. Unterr. (1958), 43-73.

[3] T. Bisztriczky, Inflectional convex space curves. Canad. J. Math. 36 (1984), 537-549.

[4] T. Bisztriczky, Convex sets and plane curve singularities, to appear.

[5] J.E. Goodman and R. Pollack, Proof of Grünbaum's conjecture on the stretchability of certain arrangements of pseudolines. J. Combin. Theory Ser. A 29 (1980), 385-390.

[6] P. Scherk, Über reele geschlossene Raumkurven vierter Ordnung. Math. Ann., 112 (1936), 743-766.

[7] J. von Sz.Nagy, Über die charakteristischen Zahlen einer Kurve vom Maximal-klassenindex. Math. Ann. 100 (1928), 164-178.

[8] J.L. Weiner, Global properties of spherical curves. J. Diff. Geom. 12 (1977), 425-434.

University of Calgary
Calgary, Alberta
Canada T2N 1N4

Received 24 March, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 3, June 1986 juin

ORTHOGONAL SPHERES

J. A. Lester

Presented by H.S.M. Coxeter F.R.S.C.

§1. Introduction and preliminaries. We consider a problem of W. Benz: characterize the injections from the set of spheres in Euclidean n-space $\mathbb{E}_n$ ($n \geqslant 2$) into itself which preserve pairs of orthogonal spheres. We show that such mappings must be induced by similarities of $\mathbb{E}_n$.

Some notation and preliminaries: the sphere in $\mathbb{E}_n$ with centre $\mathbf{a} \in \mathbb{E}_n$ and radius $\rho > 0$ has equation $(\mathbf{x} - \mathbf{a})\cdot(\mathbf{x} - \mathbf{a}) = \rho^2$ (the dot denotes the usual dot product on $\mathbb{E}_n$). Two spheres with centres $\mathbf{a}_1$ and $\mathbf{a}_2$ and radii ρ_1 and ρ_2 are orthogonal iff $(\mathbf{a}_1 - \mathbf{a}_2)\cdot(\mathbf{a}_1 - \mathbf{a}_2) = \rho_1^2 + \rho_2^2$. A similarity of $\mathbb{E}_n$ is a mapping of the form $\mathbf{x} \to \alpha T\mathbf{x} + \mathbf{b}$ for some $0 \neq \alpha \in \mathbb{R}$, $\mathbf{b} \in \mathbb{E}_n$ and $T:\mathbb{E}_n \to \mathbb{E}_n$ an isometry (orthogonal linear transformation).

We proceed as follows: in §2, we reformulate the problem as one in projective (n+1)-space, where we show that our mapping preserves certain linear sections of its domain. For an appropriate choice of hyperplane at infinity, we then (in §3) extend the mapping to a line preserving mapping of the corresponding affine space. By the fundamental theorem of affine geometry, this extended mapping must then be affine; in fact, it turns out to be the affine (n+1)-space incarnation of some similarity of $\mathbb{E}_n$, thereby establishing the desired result.

§2. Projective formulation of the theorem. The spheres in $\mathbb{E}_n$ may be identified with the points outside an unruled quadric $\mathcal{Q}$ in (n+1)-dimensional projective space $\mathcal{P}_{n+1}$ as follows. On $\mathbb{R}^{n+2}$ (the space of homogeneous coordinated for $\mathcal{P}_{n+1}$), define the metric $[\ ,\ ]$ by

$$[\mathbf{X}, \mathbf{Y}] := \sum_{i=1}^{n} X_i Y_i - \tfrac{1}{2}(X_{n+1}Y_{n+2} + X_{n+2}Y_{n+1})$$

for all $\mathbf{X} := (x_1, x_2, \ldots, x_{n+2})$, $\mathbf{Y} := (y_1, y_2, \ldots, y_{n+2}) \in \mathbb{R}^{n+2}$. This metric has signature (n+1,1), and the equation of $\mathcal{Q}$ is $[\mathbf{X},\mathbf{X}] = 0$.

With the sphere with centre $\mathbf{a}$ and radius ρ in $\mathbb{E}_n$ we associate the point $A \propto (\mathbf{a}, 1, \mathbf{a}\cdot\mathbf{a} - \rho^2) \in \mathcal{P}_{n+1}$, which lies outside $\mathcal{Q}$ since $[A,A] > 0$. We have also that $[A,E] \neq 0$ for $E = (\mathbf{0}, 0, 1)$; conversely, any $A \in \mathcal{P}_{n+1}$ with $[A, A] > 0$ and $[A,E] \neq 0$ corresponds to a sphere in $\mathcal{P}_{n+1}$. Two spheres in $\mathbb{E}_n$ corresponding to A_1 and A_2 in $\mathcal{P}_{n+1}$ are orthogonal iff $[A_1,A_2] = 0$ (easy exercise); in projective terms, two spheres are orthogonal iff the corresponding points of $\mathcal{P}_{n+1}$ are conjugate.

The *points* of $\mathbb{E}_n$ may also be associated with points in $\mathcal{P}_{n+1}$: for each $\mathbf{x} \in \mathbb{E}_n$ set $X \propto (\mathbf{x}, 1, \mathbf{x}\cdot\mathbf{x})$. Since $[X,X] = 0$, X is on $\mathcal{Q}$, and since $[X,E] = 0$, X is not on the hyperplane tangent to $\mathcal{Q}$ at E. Conversely, any $X \in \mathcal{Q}$ with $[X,E] \neq 0$ corresponds to a point of $\mathbb{E}_n$. The point associated with $X \in \mathcal{Q}$ lies on the sphere associated with $A \in \mathcal{P}_{n+1}$ iff $[A,X] = 0$.

In $\mathcal{P}_{n+1}$, the similarity $\mathbf{x} \to \alpha\mathbf{T}\mathbf{x} + \mathbf{b}$ (for α, $\mathbf{T}$, and $\mathbf{b}$ as in §1) takes the form

$$\begin{bmatrix} \mathbf{x} \\ 1 \\ \mathbf{x}\cdot\mathbf{x} \end{bmatrix} \to \begin{bmatrix} \mathbf{T} & \alpha^{-1}\mathbf{b} & 0 \\ 0 & \alpha^{-1} & 0 \\ 2\mathbf{b}^t\mathbf{T} & \alpha^{-1}\mathbf{b}\cdot\mathbf{b} & \alpha \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ 1 \\ \mathbf{x}\cdot\mathbf{x} \end{bmatrix}.$$

The $(n+2)\times(n+2)$ matrix above represents an isometry of the metric $[\ ,\ ]$ on $\mathbb{R}^{n+2}$ with eigenvector E, or, in projective terms, a projective collineation on $\mathcal{P}_{n+1}$ fixing the quadric $\mathcal{Q}$ and the point E on $\mathcal{Q}$. (It thus preserves conjugacy of points; in particular, it maps the tangent hyperplane at E onto itself.) Conversely, any such projective collineation can be so represented for appropriate α, $\mathbf{T}$, and $\mathbf{b}$.

Formulated in projective terms, then, our theorem is as follows:

> An injection $\mathcal{Q}_0 \to \mathcal{Q}_0$ (where $\mathcal{Q}_0$ denotes the set of points of $\mathcal{P}_{n+1}$ outside $\mathcal{Q}$ and not on the hyperplane tangent to $\mathcal{Q}$ at E) which preserves pairs of conjugate points is the restriction to $\mathcal{Q}_0$ of a projective collineation of $\mathcal{P}_{n+1}$ fixing $\mathcal{Q}$ and E.

We define a *proper secant* of $\mathcal{Q}$ in $\mathcal{P}_{n+1}$ to be a line intersecting $\mathcal{Q}$ in two distinct points, neither of which is E.

Lemma 2.1: For every proper secant of $\mathcal{Q}$ in $\mathcal{P}_{n+1}$ there exist n pairwise conjugate points in $\mathcal{Q}_0$ all conjugate to each point of the secant. Conversely, any set of points in $\mathcal{P}_{n+1}$ all conjugate to each of n pairwise conjugate points in $\mathcal{Q}_0$ must lie on a proper secant of $\mathcal{Q}$.

Proof: In the (n+2)-dimensional space of homogeneous coordinates of $\mathcal{P}_{n+1}$, the coordinates of the points of a proper secant span a 2-space of signature (1,1) (with respect to the metric [,]) not containing E. The subspace of coordinates orthogonal to this 2-space thus has signature (n,0) (i.e. it is positive definite) and is not completely orthogonal to E. It thus contains an orthogonal basis $\{A_1, A_2, \ldots, A_n\}$ with $[A_i,E] \neq 0$, $i = 1,2,\ldots,n$. The points $A_1, A_2, \ldots, A_n \in \mathcal{Q}_0$ are the required pairwise conjugate points.

Conversely, a set of n pairwise conjugate points $A_1, A_2, \ldots, A_n$ in $\mathcal{Q}_0$ spans a positive definite n-space in $\mathbb{R}^{n+2}$ not orthogonal to E. The subspace orthogonal to this n-space is a 2-space of signature (1,1) not containing E, which coordinatizes a proper secant with all of its points conjugate to the points $A_1, A_2, \ldots, A_n$. ∎

Corollary 2.1: The mapping of the theorem takes sections of $\mathcal{Q}_0$ with proper secants into proper secants.

§3. Reduction to an affine theorem. Take the tangent hyperplane at E to be the hyperplane at infinity for the corresponding affine space $\mathcal{A}_{n+1}$; then in $\mathcal{A}_{n+1}$, $\mathcal{Q}$ is an elliptic paraboloid. Proper secants of $\mathcal{Q}$ are those secants intersecting $\mathcal{Q}$ in two distinct finite points, and may have any direction except that given by E.

In affine terms, it remains to prove the following:

> An injection $\mathcal{Q}_0 \to \mathcal{Q}_0$ (where $\mathcal{Q}_0$ denotes the points of $\mathcal{A}_{n+1}$ outside $\mathcal{Q}$) which map sections of $\mathcal{Q}_0$ with proper secants of $\mathcal{Q}$ into proper secants must be the restriction of an affine mapping $\mathcal{A}_{n+1} \to \mathcal{A}_{n+1}$ mapping $\mathcal{Q}$ into $\mathcal{Q}$.

We begin the proof of this result by extending the mapping to points inside $\mathcal{Q}$. In the following lemma we use the fact that since $\mathcal{Q}$ is convex, any line "close enough" to a proper secant of $\mathcal{Q}$ is also a proper secant.

Lemma 3.1: Let m_1, m_2 and m_3 be non-coplanar proper secants through a point $P \in \delta_{n-1}$ inside Q. Then m_1, m_2 and m_3 and P form part of a Desargues configuration all of whose lines are proper secants and all of whose points except P lie outside Q.

Proof: Take the finite parts of the lines m_1, m_2 and m_3 as coordinate axes in the 3-space they determine such that they intersect Q at points with coordinates $Q_1(1,0,0)$, $Q_2(0,1,0)$ and $Q_3(0,0,1)$. The three lines joining these points are proper secants, so for small enough $\varepsilon > 0$, the lines joining the points $A_1(1+\varepsilon,0,0)$, $A_2(0,1+\varepsilon,0)$ and $A_3(0,0,1+\varepsilon)$ (all of which lie outside Q) are also proper secants.

Denote by R_2 the point of Q on line A_1A_3 closer to A_3, and by R_1 the point of Q on A_2A_3 closer to A_3; then line R_1R_2 is a proper secant. Thus for some points C_1 and C_2 "near enough" to R_1 and R_2 on the same lines A_1A_3 and A_2A_3 but outside Q, line C_1C_2 is also a proper secant. These points have coordinates $C_2(\alpha,0,1+\varepsilon-\alpha)$ and $C_1(0,\beta,1+\varepsilon-\beta)$ for some $0 < \alpha, \beta < 1+\varepsilon$. By choosing ε small enough, C_1 and C_2 can be forced arbitrarily close to m_3; we can thus take $\alpha, \beta < 1$. Also, we may take $\alpha \neq \beta$.

For any ν with $\varepsilon < \nu < \min\{\varepsilon(1-\alpha)^{-1}, \varepsilon(1-\beta)^{-1}\}$, set

$$1 + \lambda := \alpha(1+\nu)(\alpha+\nu-\varepsilon)^{-1} \text{ and } 1 + \mu := \beta(1+\nu)(\beta+\nu-\varepsilon)^{-1};$$

then $\lambda \neq \mu$ and $0 < \lambda, \mu < \varepsilon$ (exercise). The points $B_1(1+\lambda,0,0)$, $B_2(0,1+\mu,0)$ and $B_3(0,0,1+\nu)$ are thus all outside Q; in fact, B_1 is on line segment Q_1A_1 and B_2 is on line segment Q_2A_2. Furthermore, B_1, C_2 and B_3 are collinear, as are B_2, C_1 and B_3, and all three of the lines through B_1, B_2 and B_3 are proper secants. (Fig. 1 a) illustrates the $m_1 - m_2$ plane.)

Since $\lambda \neq \mu$, lines B_1B_2 and A_1A_2 are not parallel, so they intersect at some point C_3 on the proper secant C_1C_2 (by Desargues' theorem). (Fig. 1 b) illustrates these lines.) Points B_1 and B_2 are on the same side of line A_1A_2, so C_3 is not between B_1 and B_2. But the points of δ_{n-1} inside Q on B_1B_2 *are* between B_1 and B_2, so C_3 is outside Q.

The points P, A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3 are thus the vertices of the required Desargues configuration. ∎

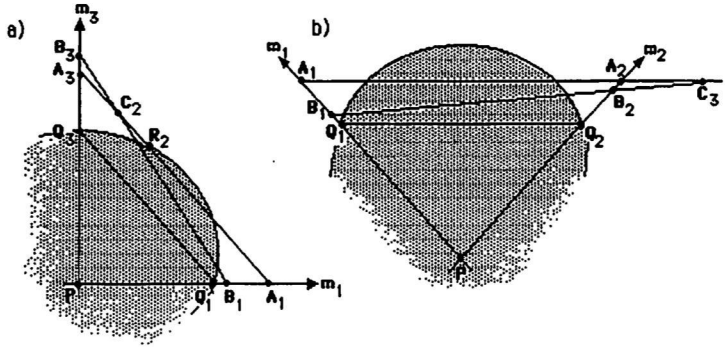

Fig. 1 (the interior of $\mathcal{Q}$ is shaded)

Because its lines are proper secants intersecting outside $\mathcal{Q}$ (except for $m_1 \cap m_2 \cap m_3 = P$), Desargues configurations like that of the lemma are preserved by our mapping. Thus the sections with $\mathcal{Q}_0$ of three non-coplanar secants through P map into proper secants through a point $\bar{P} \in \mathcal{S}_{n-1}$. This result can easily be extended to *all* proper secants through P, thereby inducing a mapping $P \to \bar{P}$ on the points inside $\mathcal{Q}$ which extends the original mapping to one on $\mathcal{S}_{n-1} \setminus \mathcal{Q}$. This extended mapping preserves sections of $\mathcal{S}_{n-1} \setminus \mathcal{Q}$ with proper secants, and can easily be extended (by a similar application of Desargues configurations) to a mapping defined on *all* of $\mathcal{S}_{n-1}$ with the same property.

The fact that *all* lines (including non-secants and improper secants) map into lines can now be easily established via Desargues' theorem again or by Pappus' theorem. The injectivity of the mapping follows as an easy exercise from its injectivity outside $\mathcal{Q}$, so by the fundamental theorem of affine geometry, the mapping is affine. That it takes $\mathcal{Q}$ into $\mathcal{Q}$ follows from its continuity and the fact that it maps $\mathcal{Q}_0$ into $\mathcal{Q}_0$, so the proof of the theorem is complete.

Author's address:

Department of Mathematics and Computer Science
California State University at Los Angeles
5151 State University Drive
Los Angeles, California 90032
U.S.A.

Received 26 March, 1986

Mailing Addresses

1. B. Aupetit
   Département de Mathématiques
   Statistique et Actuariat
   Université Laval
   Québec, Canada, G1K 7P4

2. T. Bisztriczky
   Department of Mathematics
   University of Calgary, Calgary
   Alberta, Canada, T2N 1N4

3. J. D'Almeida
   Département de Mathématiques
   Université de Caen
   14032 Caen Cedex, France

4. D. Demetrovics
   Computer and Automation Inst.
   Hungarian Acad. Sci.
   H-1132 Budapest, Victor Hugo U.
   18-22

5. A. Granville
   Department of Mathematics
   and Statistics
   Queen's University, Kingston
   Ontario, Canada, K7L 3N6

6. Y. Hellegouarch
   Département de Mathématiques et
   de Mécanique
   Université de Caen
   14032 Caen Cedex, France

7. J.A. Lester
   Department of Mathematics and
   Computer Science, California
   State University, 5151 State
   University Drive, Los Angeles
   California 90032, U.S.A.

8. I.A. Malcev
   Math. Inst. Siberian Branch
   Acad. Sci. USSR
   630090 Novosibirsk 90, USSR

9. J.-C. Massé
   Département de Mathématiques,
   Statistiques et Actuariat
   Université Laval, Québec
   Canada, G1K 7P4

10. G. Nachar
    Département de Mathématiques
    Université Claude Bernard-Lyon 1
    43, boulevard du 11 Novembre 1918
    69622 Villeurbanne Cedex, France

11. J. Rätz

Mathematische Institut
Universität Bern, Sidlerstr. 5
CH-3012 Bern, Schweiz

12. R.A.G. Seely

Department of Mathematics
John Abbott College, CP2000
Ste. Anne de Bellevue, Québec
Canada, H9X 3L9

13. J. L. Synge

Institute For Advanced Studies
Dublin 4, Ireland