C.R. Math. Rep. Acad. Sci. Canada
Vol. XVIII, No. 5 October 1996 octôbre

CONTENTS

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

New Orthonormal Sets and Frames in the Paley–Wiener Space

Ahmed I. Zayed

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

Abstract

The Paley-Wiener space B_σ^2, also known as the space of bandlimited functions with bandwidth σ, consists of all entire functions of exponential type at most σ that are square integrable when restricted to the real line. We show that the cardinal B-splines can be used to generate orthonormal sets, as well as, frames in B_σ^2. A new orthonormal set of functions in B_σ^2, is obtained from one single function by translating it by integer multiples of $2\pi/\sigma$. This function is calculated explicitly in terms of Young's function.

1 Introduction

The Paley-Wiener space of bandlimited functions, denoted by B_σ^2, is defined as the space of all functions $f(t) \in L^2(\mathcal{R})$ whose Fourier transforms, $\hat{f}$, have support in $[-\sigma, \sigma]$, or equivalently it is the space of all functions $f(t)$ that can be written in the form

$$f(t) = \frac{1}{\sqrt{2\pi}} \int_{-\sigma}^{\sigma} F(\omega) e^{-it\omega} d\omega,$$

for some $F \in L^2(-\sigma, \sigma)$.

We shall say that a function $S(t)$ is a sampling function with respect to the sequence $\{\gamma_n\}_{n=-\infty}^{\infty}$ if $S(\gamma_n) = \delta_{0,n}$ where $\{\gamma_n\}_{n=-\infty}^{\infty}$ is a sequence of real numbers such that $\gamma_0 = 0$. Throughout this article, we assume that S is either in $L^1(\mathcal{R})$ or $L^2(\mathcal{R})$.

One can easily verify that $\{\phi(t - t_n)\}_{n=-\infty}^{\infty}$, is an orthogonal basis of B_σ^2, where $\phi(t) = \sin\sigma t/\sigma t$ and $t_n = n\pi/\sigma$. Moreover, the function $\phi(t)$ is readily seen to be a sampling function with respect to the sequence $\{t_n\}_{n=-\infty}^{\infty}$. As a consequence of that, we have for any $f \in B_\sigma^2$

$$f(t) = \sum_{n \in Z} f(t_n) \frac{\sin\sigma(t - t_n)}{\sigma(t - t_n)},$$

which is known as the Whittaker-Shannon-Kotel'nikov sampling theorem for bandlimited functions [5].

It is known [1, 2] that the cardinal B-spline of order n, $(n = 0, 1, 2, \ldots)$, $\phi_n(x)$, with knots at the integers, can be used to generate an orthonormal wavelet basis of $L^2(\mathcal{R})$ of the form ${}_n\psi_{m,k}(x) = 2^{-m/2}\psi(2^{-m}x - k)$; $k, m \in Z$.

In this article we borrow some ideas from wavelet analysis and sampling theory to show that the Fourier transform of the square root of the cardinal B-splines can be used to generate orthonormal sets and frames in various Paley-Wiener spaces consisting of functions with different bandwidth. Although the results provide only existence of such orthonormal sets of functions, we have been able to calculate one such set in closed form using Young's function.

2 Preliminaries:

Young's functions were introduced by W. H. Young in 1912 [3] in his investigation of non-converging Fourier series. They also appeared in connection with the Hardy transform, which generalizes the Hankel and the Y transforms; for more details, see [4]. Young's function of order $\nu (\nu \geq 0)$ is defined by

$$\mathbf{Y}_\nu(z) = z^\nu \sum_{k=0}^{\infty} \frac{(-1)^k z^{2k}}{\Gamma(\nu + 2k + 1)} . \tag{1}$$

Clearly, $\mathbf{Y}_0(z) = \cos z$ and $\mathbf{Y}_1(z) = \sin z$. It can be shown that $\mathbf{Y}_\nu(z)/z^\nu$ is an entire function of exponential type. For $0 < \nu < 1$, $\mathbf{Y}_\nu$ is no longer periodic, but fills up the analytical gap between the sine and cosine functions.

We define the cardinal B-spline, ϕ_n, of order n as follows:

$$\phi_0(\omega) = \chi_{(-\sigma/2, \sigma/2)}(\omega) ,$$

and

$$\phi_n(\omega) = \sqrt{(2\pi)}(\phi_{n-1} * \phi_0)(\omega), \quad n = 1, 2, \ldots ,$$

where χ_A is the characteristic function of A.

3 The main results

Theorem 1 *Let S be a sampling function with respect to the sequence $\{t_n = n\pi/\sigma\}_{n\in Z}$ such that $\hat{S}(w) > 0$ a.e. Then S generates an orthonormal family of functions $\{\psi_n(t)\}_{n\in Z}$ in $L^2(\mathcal{R})$, each of which is obtained from one single function ψ by a translation by an integer multiple of π/σ, namely, $\psi_n(t) = \psi(t - t_n)$ for all $n \in Z$.*

Conversely, any orthonormal family in $L^2(\mathcal{R})$ that is generated from one single function by translations by t_n can be obtained from a sampling function (with respect to the sequence $\{t_n\}_{n\in Z}$) with positive Fourier transform.

Now we show how the cardinal B-splines can be used to generate orthonormal sets in the Paley–Wiener space. But first, let us recall that the set $\{\phi(t - k\pi/\sigma)\}_{k=-\infty}^{\infty}$ is orthonormal in B_σ^2, where $\phi(t) = \sqrt{\sigma/\pi}\ (\sin \sigma t/\sigma t)$. In terms

of Young's function, ϕ can be rewritten as $\phi(t) = \sqrt{\sigma/\pi}\, Y_1(\sigma t)/(\sigma t)$. In the next theorem we show, among other things, that there is another orthonormal system in B_σ^2 that is generated by Young's function of order 3/2.

Theorem 2 *a) Let $\phi_n(w)$ be the cardinal B-spline of order n defined above. Fix n and define $\psi_n(t)$ by*

$$\hat{\psi}_n(\omega) = \frac{1}{\sigma^{(n+1)/2}} \sqrt{\phi_n(\omega)},$$

and set $\psi_{n,k}(t) = \psi_n\left(t - \frac{2k\pi}{\sigma}\right)$, $k = 0, \pm 1, \pm 2, \ldots$. Then $\{\psi_{n,k}(t)\}_{k=-\infty}^{\infty}$ is an orthonormal set in the Paley-Wiener space $B^2_{(n+1)\sigma/2}$. In particular, $\left\{g\left(t - \frac{2k\pi}{\sigma}\right)\right\}_{k\in Z}$ is orthonormal in B_σ^2, where

$$g(t) = \sqrt{\frac{\sigma}{2}} \frac{Y_{3/2}(\sigma t)}{(\sigma t)^{3/2}},$$

and $Y_{3/2}(z)$ is Young's function of order $\frac{3}{2}$.

b) The set $\left\{g\left(t - \frac{2k\pi}{\sigma}\right)\right\}_{k\in Z}$ is complete in $B^2_{\sigma/2}$, but not in B_σ^2, and, in addition, it is a frame in B_λ^2 for any $0 < \lambda < \sigma/2$.

References

[1] C. Chui, *An Introduction to Wavelets*, Academic Press, New York (1992).

[2] I. Daubechies, *Ten Lectures on Wavelets*, SIAM Publications, Soc. Indust. Appl. Math., Philadelphia (1992).

[3] W.H. Young, On infinite integrals involving a generalization of the sine and cosine functions, *Quart. J. Math.*, Vol. 4 (1912), pp. 161—177.

[4] A. I. Zayed, *Function and Generalized Function Transformations*, CRC Press, Boca Raton, Fl (1996).

[5] A. I. Zayed, *Advances in Shannon's Sampling Theory*, CRC Press. Boca Raton, Fl (1993).

Received May 7, 1996

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

Note on Wendt's determinant

Aleksander Grytczuk

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

1. Introduction. Let $A = circ(a_0, a_1, \ldots, a_{n-1})$ be a given circulant matrix. Stern proved ([3]), that $\det A = \prod_{j=0}^{n-1} f(\varepsilon_j)$, where ε_j are the n-th roots of unity and $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$. Next, in 1894 Wendt [4] introduced special form of the circulant matrix. Namely, he considered the matrix $W = circ\left\{\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n-1}\right\}$, where $\binom{n}{k}, n \geq 2$ denote the binomial coefficient. From the Stern's result easily follows that $W_n = \det W = \prod_{j=0}^{n-1} ((1+\varepsilon_j)^n - 1)$.

Wendt applied this determinant to examination of Fermat Last Theorem, (see [2] ,p.62-63). The following interesting properties are known:

(1) $W_n = -(2^n - 1)u^2, n = 2l; u \in Z$

(2) if d/n then W_d / W_n.

(3) $W_n = 0$ iff $6/n$.

2. Result.

In this Note we prove an extension of the property (1) proving (1) for any natural number $n \geq 2$ and giving more information about the number $n \in Z$. Namely, the following Theorem is true :

Theorem 1. Let $W_n = \det circ\left\{\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n-1}\right\}$, then

$$(4) \qquad W_n = -(2^n - 1)\left(\prod_{k=1}^{l-1} \xi_k\right)^2 \quad , \text{if} \quad n = 2l$$

$$(5) \qquad W_n = (2^n - 1)\left(\prod_{k=1}^{l} \xi_k\right)^2 \quad , \text{if} \quad n = 2l+1.$$

where

$$(6) \qquad \xi_k = 2^n(-1)^k \cos^n \frac{\pi k}{n} - 1.$$

Proof. By the result of Stern we have $W_n = \prod_{k=0}^{n-1} \xi_k, \xi_k = (1+\varepsilon_k)^n - 1$ where $\varepsilon_k; k = 0,1,\ldots,n-1$ are the roots of unity of the degree n. Since $\varepsilon_k = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$ and $1 + \cos\frac{2\pi k}{n} = 2\cos^2\frac{\pi k}{n}, \sin\frac{2\pi k}{n} = 2\sin\frac{\pi k}{n}\cos\frac{\pi k}{n}$ then we obtain

$$(7) \qquad \xi_k = (1+\varepsilon_k)^n - 1 = 2^n(-1)^k \cos^n \frac{\pi k}{n} - 1.$$

From (7) we have $\xi_0 = 2^n - 1$ and we can prove that $\xi_k = \xi_{n-k}$. Indeed, by (7) it follows that

$$(8) \qquad \xi_{n-k} = 2^n(-1)^{n-k} \cos^n \frac{\pi(n-k)}{n} - 1$$

and $\cos\frac{\pi(n-k)}{n} = -\cos\frac{\pi k}{n}$, then by (8) it follows that

$$\xi_{n-k} = 2^n(-1)^k \cos^n \frac{\pi k}{n} - 1 = \xi_k .$$

Therefore (5) is proved. On the other hand if $n = 2l$ then by (7) it follows that $\xi_1 = \xi_l = 2^n(-1)^l \cos^n \frac{\pi}{2} - 1 = -1$ and consequently (4) is fulfilled. The proof of the Theorem 1 is complete.

Remark. From the Theorem easily follows (1) and (2).

Another application of this Theorem is contained in the following :

Corollary. For any natural number $n \geq 2$ we have

$$(*) \qquad \sum_{k=0}^{n-1} (-1)^k \cos^n \frac{\pi k}{n} = \frac{n}{2^{n-1}} .$$

Proof. Let $W = circ\left\{\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n-1}\right\}$. Then it is well-known that the trace of the matrix W is equal to the sum of the eigenvalues of this matrix . Hence $\sum_{k=0}^{n-1} \xi_k = TrW$. On the other hand we have $TrW = n$ and consequently we get

$$(9) \qquad \sum_{k=0}^{n-1} \xi_k = n .$$

By the Theorem 1 and (9) it follows that

$$(10) \qquad \sum_{k=0}^{n-1} \xi_k = 2^n \sum_{k=0}^{n-1} (-1)^k \cos^n \frac{\pi k}{n} - n .$$

Comparing (9) and (10) we obtain $2^n \sum_{k=0}^{n-1} (-1)^k \cos^n \frac{\pi k}{n} = 2n$ and the proof of Corollary is complete.

Moreover, we can prove the following :

Theorem 2. Let $n = 2l$, $3 \nmid n$, then $\prod_{p-1 \mid 2l} p \mid W_{2l}$, $p > 2$.

Proof. For the proof of the Theorem 2 we use two following Lemmas :

Lemma 1. (see, [1]) Let B_{2l} denote the $2l$-th Bernoulli number. Then for every positive integer l we have

$$B_{2l} = \frac{(-1)^{l-1} lT(l)}{2^{2l-1}(2^{2l}-1)} \text{ ,where } T(1)=1 \text{ and } T(l) = (-1)^{l-1} + \sum_{j=1}^{l-1} (-1)^{j+1} \binom{2l-1}{2j} T(l-j) \text{ , } l \geq 2$$

Lemma 2. Let $B_{2l} = \frac{N_{2l}}{D_{2l}}$, $(N_{2l}, D_{2l}) = 1$. Then $D_{2l} = \prod_{p-1/2l} p$.

Lemma 2 is well-known result of von Staudt and Clausen .

From the Theorem 1 we have

$$(11) \quad W_{2l} = -(2^{2l}-1)u^2 \text{ , } u = \prod_{k=1}^{l-1} \xi_k = 2^n \prod_{k=1}^{l-1} (-1)^k \cos^n \frac{\pi k}{n} - 1 .$$

By Lemma 1 , Lemma 2 and (11) we obtain

$$(12) \quad 2^{2l-1} N_{2l} W_{2l} = (-1)^l lT(l)u^2 \prod_{p-1/2l} p .$$

Since $3 \nmid l$ then by (3) it follows that $W_{2l} \neq 0$ and from (12) we get

$2^{2(l-1)} N_{2l} W_{2l} = (-1)^l lT(l)u^2 \prod_{p-1/2l} p, p > 2$. Since $(p, 2^{2l-1}) = (p, N_{2l}) = 1$ then by the last equality it follows that $\prod_{p-1.2l} p / W_{2l}, p > 2$ and the proof of the Theorem 2 is complete .

References .

[1] A. Grytczuk and J. Grytczuk - " A primality test for Fermat numbers "- (to appear in : Acta Acad. Paed. Agriensis- Sectio Mat. Eger)

[2] P. Ribenboim - 13 Lectures on Fermat's Last Theorem - Springer-Verlag- - 1979.

[3] M.A.Stern - " Einige Bemerkungen uber eine Determinante "- J.Reine Angew.Math. 73 (1871), 374-380.

[4] E. Wendt - " Arithmetischen studien uber den Letzen Fermatschen Satz , welcher aussagt dass die Gleichung $a^n = b^n + c^n$ für $n > 2$, in ganzen Zahlen nicht auflosbar ist ". - J. Reine Angew. Math. 13(1894), 335-346 .

Institute of Mathematics
Department of Algebra and Number Theory
T.Kotarbiński Pedagogical University
65-069 Zielona Góra , Poland .

Received July 31, 1996

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

GROUPE DES CLASSES DES ANNEAUX DE POLYNÔMES SUR UN D+M

Driss Nour el abidine

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

INTRODUCTION

Les anneaux considérés sont commutatifs unitaires. Si R est un anneau intègre, on désigne par $R^{(n)} = R[X_1,\ldots,X_n]$ l'anneau de polynômes à n indéterminées à coefficients dans R si $n \geq 1$ et $R^{(0)} = R$, Cl(R) son groupe des classes (cf. [6, 7]) (*notion introduite par* A.BOUVIER et M.ZAFRULLAH pour *un anneau intègre, et qui généralise les notions classiques définies dans la classe des anneaux de Krull ou de Prüfer*), Pic(R) son groupe de Picard et G(R) = Cl(R)/Pic(R) son groupe local des classes (cf. [5, 7]).

Soient A et R deux anneaux intègres tels que A = K + M et R = D + M, où K est un corps, M est un idéal maximal de A et D est un sous anneaux du corps K, l'anneau ainsi construit, est étudié dans plusieurs articles [1], [3] et [8]. Dans [1], D.F.ANDERSON et A.RYCKAERT se sont intéressés spécialement au groupe des classes de ce type d'anneaux, et ils ont établit le résultat suivant : si K = Frac(D) (*corps des fractions de D*), alors il existe un diagramme commutatif avec lignes et colonnes exactes :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Pic}(D) & \xrightarrow{\alpha'} & \mathrm{Pic}(R) & \xrightarrow{\beta'} & \mathrm{Pic}(A) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Cl}(D) & \xrightarrow{\alpha} & \mathrm{Cl}(R) & \xrightarrow{\beta} & \mathrm{Cl}(A) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & G(D) & \xrightarrow{\alpha''} & G(R) & \xrightarrow{\beta''} & G(A) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Dans cet article, nous nous intéressons à donner une généralisation du résultat précédent, c'est-à-dire, à relier, pour tout $n \in \mathbb{N}$, le groupe des classes et le groupe local des classes de l'anneau $R^{(n)}$ à ceux des anneaux $D^{(n)}$ et $A^{(n)}$.

0. NOTATION - TERMINOLOGIE

Soient R un anneau intègre, K son corps des fractions. Etant donnés I et J deux idéaux fractionnaires de R, on note par $I : J = \{x \in K : xJ \subset I\}$, $I^{-1} = R : I$, $I_v = (I^{-1})^{-1}$ et $I_t =$

$\cup J_v$, où J parcourt l'ensemble des idéaux de type fini contenus dans I. On dit que I est un v-idéal (resp. un t-idéal, un idéal v-fini) si $I_v = I$ (resp. si $I_t = I$, si $I = J_v$ où J est un idéal de type fini contenu dans I).On désigne par D(R) l'ensemble des idéaux divisoriels de R, Cart(R) l'ensemble des idéaux inversibles de R, $D_f(R)$ l'ensemble des idéaux v-finis de R et P(R) l'ensemble des idéaux principaux de R. On dit qu'un t-idéal I est t-inversible, s'il existe un t-idéal J tel que $(IJ)_t = R$. Désignons par $I_t(R)$ l'ensemble des t-idéaux t-inversibles de R. $I_t(R)$ est le plus grand sous-groupe du monoïde $D_f(R)$ [2]. Comme dans [6], on appelle le groupe des classes, le groupe $Cl(R) = I_t(R)/P(R)$. Lorsque R est un anneau de Krull (resp. un anneau de Prüfer), Cl(R) est l'habituel groupe des classes D(R)/P(R) [9] (resp. Pic(R) = Cart(R)/P(R)). Si $I \in I_t(R)$, [I] désignera sa classe dans Cl(R). On rappelle, que si B est une extension plate de R, alors il existe un homomorphisme $\varphi : Cl(R) \longrightarrow Cl(B)$ défini par $\varphi([I]) = [IB]$, où $I \in I_t(R)$ [1].

Cette note fait partie des travaux de l'auteur présentés dans sa thèse [11]. Les notations et les résultats de base sont de [1], [4], [6] et [10].

1. QUELQUES PROPRIETES DE L'ANNEAU $(D+M)[X_1,\ldots,X_n]$

On a besoin de deux lemmes techniques concernant les propriétés, plus au moins classiques, des anneaux de type $(D + M)^{(n)}$ qu'on va utiliser par la suite pour évaluer leur groupe des classes et leur groupe local des classes.

Lemme 1.

1/ Soit J un idéal entier de $R^{(n)}$, alors J contient $M[X_1,\ldots,X_n]$ si et seulement si $J = I + M[X_1,\ldots,X_n]$, où I est un idéal de $D^{(n)}$.

2/ $R^{(n)}$ est un $D^{(n)}$-module fidèlement plat.

3/ I est un idéal fractionnaire de type fini (resp. inversible) de $D^{(n)}$ si et seulement si $IR^{(n)}$ est un idéal fractionnaire de type fini (resp. inversible) de $R^{(n)}$.

4/ I est un idéal fractionnaire principal si et seulement si $IR^{(n)}$ est principal.

Preuve: [cf. [1, Prop.2.1].

Lemme 2. Pour tout I idéal entier de $D^{(n)}$ dont la trace sur D est non nulle ; on a :

1/ $(IR^{(n)})^{-1} = I^{-1}R^{(n)}$.

2/ $(IR^{(n)})_v = I_vR^{(n)}$.

3/ $I \in D_f(D^{(n)})$ si et seulement si $IR^{(n)} \in D_f(R^{(n)})$.

Preuve: On reprend les mêmes techniques utilisées dans [1, Prop.2.4], et on exploite le fait que I soit un idéal entier tel que $I \cap D \neq 0$ vérifie $IR^{(n)} = I+M^{(n)}$ et $I^{-1}R^{(n)} = I^{-1}+M^{(n)}$.

Théorème. Soient $A = K + M$ et $R = D + M$, où D est un sous anneau de K. Si $Frac(D) = K$, alors il existe un diagramme commutatif avec lignes et colonnes exactes :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Pic(D^{(n)}) & \xrightarrow{\alpha'} & Pic(R^{(n)}) & \xrightarrow{\beta'} & Pic(A^{(n)}) & \longrightarrow & 0 \quad (**) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Cl(D^{(n)}) & \xrightarrow{\alpha} & Cl(R^{(n)}) & \xrightarrow{\beta} & Cl(A^{(n)}) & & (*) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & G(D^{(n)}) & \xrightarrow{\alpha''} & G(R^{(n)}) & \xrightarrow{\beta''} & G(A^{(n)}) & & (***) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

De plus, la suite $0 \longrightarrow Pic(D^{(n)}) \longrightarrow Pic(R^{(n)}) \longrightarrow Pic(A^{(n)}) \longrightarrow 0$ est scindée.

Preuve : Pour la preuve de ce théorème, nous allons nous inspirer da la même technique utilisée dans [1, Theorem 3.3]. Pour cela, la démonstration se fait en trois étapes:

L'exactitude de la suite (*) :

Puisque $R^{(n)}$ est un $D^{(n)}$-module plat et que $A^{(n)}$ est un $R^{(n)}$-module plat comme anneau des fractions de $R^{(n)}$ (Lemme 1), les morphismes α et β sont bien définis par : $\alpha[I] = [IR^{(n)}]$ pour tout $I \in I_t(D^{(n)})$ et $\beta[J] = [JA^{(n)}]$ pour tout $J \in I_t(R^{(n)})$ (§ 0). En outre, $IR^{(n)}$ est principal si et seulement si I est principal dans $D^{(n)}$ (Lemme 1), d'où l'injectivité de α.

Parmi les difficultés qui s'imposent à la généralisation de ce théorème, sera la preuve de l'égalité $Im\alpha = Ker\beta$. On va procéder d'une autre manière que celle de [1] en se ramenant uniquement aux t-idéaux t-inversibles entiers de R dont la trace sur D est non nulle, en effet : soit $I \in I_t(D^{(n)})$, alors $IK^{(n)} \in I_t(K^{(n)})$; donc $IK^{(n)}$ est un idéal principal de $K^{(n)}$ car $Cl(K^{(n)}) = 0$ [9], par suite $IA^{(n)} = IK^{(n)}A^{(n)} = gK^{(n)}A^{(n)} = gA^{(n)}$ avec $g \in Frac(K^{(n)})$ (car $K^{(n)}A^{(n)} = A^{(n)}$), ce qui montre que $Im\alpha$ est inclus dans $Ker\beta$. Démontrons l'inclusion inverse. Soit $[I] \in Ker\beta$ où $I \in I_t(R^{(n)})$; $\beta[I] = 0$ équivaut à $IA^{(n)} = xA^{(n)}$, on peut supposer que $x \in I$ car $R^{(n)}{}_S = A^{(n)}$, où S est la partie multiplicative $D\backslash\{0\}$. Posons $J = x(I : R^{(n)})$; on a $x(I : R^{(n)})A^{(n)} = x(IA^{(n)} : A^{(n)}) = A^{(n)}$ car I est v - fini [1, Prop. 2.2], donc $JA^{(n)} = A^{(n)}$. S'il existe un idéal $I_D \in I_t(D^{(n)})$ tel que $\alpha[I_D] = [J]$, donc $J = bI_DR^{(n)}$ avec $b \in Frac(R^{(n)})$, alors $I = I_v = xJ^{-1} = x(bI_DR^{(n)})^{-1} = xb^{-1}I_D^{-1}R^{(n)}$ car I_D est v - fini [1, Prop. 2.2], ce qui montre que $[I] = [I_D^{-1}R^{(n)}] = \alpha[I_D^{-1}]$. Donc on peut supposer que I est entier et $IA^{(n)} = A^{(n)}$; d'où $I \cap D \neq 0$. D'après le lemme 1, $I = I_DR^{(n)}$, où $I_D = I \cap D^{(n)}$. Comme $I \in D_f(R^{(n)})$ (§ 0), on a $I_D \in D_f(R^{(n)})$ (Lemme 2), et ce qui montre que $I^{-1} = I_D^{-1}R^{(n)}$ car I_D est v - fini [1, Prop. 2.2]. On a $R^{(n)} = (II^{-1})_v =$

$(I_D R^{(n)} I_D^{-1} R^{(n)}))_v = (I_D I_D^{-1} R^{(n)})_v = (I_D I_D^{-1})_v R^{(n)}$ car $I_D I_D^{-1}$ est un idéal entier dont la trace sur D est non nulle (Lemm 2). Par conséquent $(I_D I_D^{-1})_v = D^{(n)}$ (Lemme 1), et ce qui montre que $I_D \in I_f(D^{(n)})$; d'où $\mathrm{Ker}\beta$ est inclus dans $\mathrm{Im}\alpha$.

L'exactitude de la suite (**) se démontre de la même manière que [1, Prop. 3.1] ; il suffit de remarquer que le diagramme suivant

$$\begin{array}{ccc} R^{(n)} & \longrightarrow & D^{(n)} \\ \downarrow & & \downarrow \\ A^{(n)} & \longrightarrow & K^{(n)} \end{array}$$

reste un produit fibré et que $\mathrm{Pic}(K^{(n)}) = 0$.

L'exactitude de la suite (***) utilise les même arguments que celles dans [1, Th. 3.3].

ACKNOWLEDGMENTS

We would like to thank the referee for several helpful suggestions and corrections.

BIBLIOGRAPHIE

[1] D.F. ANDERSON - A. RYCKAERT.The class group of D+M. J. Pure Appl. Algebra, 52 (1982) 199-212.

[2] D.F. ANDERSON. A general theory of class groups. Comm. in Algebra, 16 (1988), 805-847.

[3] E. BASTIDA - R. GILMER. Overrings and divisorial ideals of rings of the form D+M. Michigan Math. J. 20 (1973), 79-95.

[4] N. BOURBAKI. Algèbre commutative, Chap. 1 à 10, Hermann.

[5] A. BOUVIER.The local class group of a Krull domain. Canad. Math. Bull. 26 (1983), 13-19.

[6] A. BOUVIER. Le groupe des classes d'un anneau intègre. 107ème congrès des sociétés savantes Brest, (1982), fasc. IV, (85-92).).

[7] A. BOUVIER - M. ZAFRULLAH. On some class groups of an integral domain. Bull. Soc. Math. Grèce (N.S) 29 (1988), 45-59.

[8] J. BREWER - E. RUTTER. D + M constructions with general overrings. Michigan Math. J. 23 (1976), 33-42.

[9] R. FOSSUM.The divisor class group of a Krull domain. S.Verlag, 1973.

[10] D. NOUR EL ABIDINE.Groupe des classes d'un anneau intègre. Ann. Univ. Ferrara - Sez. 36 (1990), 175-183.

[11] D. NOUR EL ABIDINE. Groupe des classes de certains anneaux intègres et idéaux transformés. Thèse de Doctorat, Lyon 1992.

Département de Mathématiques & Faculté des Sciences et Techniques de Mohammedia - B. P. 146 - Morocco.

Received April 24, 1996

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

PROOF OF A CONJECTURE OF TERJANIAN FOR REGULAR PRIMES

CHARLES HELOU

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

ABSTRACT. G. Terjanian conjectured that if, in the cyclotomic field of l-th roots of unity, with l a prime number ≥ 5, the norm residue symbol, at the prime above l, pairing $\alpha_1 = a - \zeta$ with the "cyclotomic units" is equal to 1, where $a \in \mathbf{Z}$ and ζ is a primitive l-th root of unity, then $a \equiv 0, 1$ or $-1 (mod\ l^2)$. We here prove the conjecture for the regular primes l.

INTRODUCTION

Let l be a prime number ≥ 5, ζ a primitive l-th root of unity in $\mathbf{C}$ and $\lambda = 1 - \zeta$. For $\alpha, \beta \neq 0$ in $\mathbf{Z}[\zeta]$, let $[\alpha, \beta]$ be the element of the finite field $\mathbf{F}_l$ defined by

$$(\alpha, \beta)_\lambda = \zeta^{[\alpha,\beta]},$$

where $(\alpha, \beta)_\lambda$ is the norm residue symbol relative to the prime ideal (λ), as defined in [2]. When $[\alpha, \beta] = 0$, we say that α and β are orthogonal. We denote by C the multiplicative group generated by the cyclotomic units $u_n = \frac{1-\zeta^n}{1-\zeta}$ $(1 \leq n \leq l-1)$. Let $a \in \mathbf{Z}$ and $\alpha_1 = a - \zeta$. G. Terjanian conjectured ([5]) that α_1 is orthogonal to (every element in) C if and only if $a \equiv 0$, 1 or -1 $(mod\ l^2)$. He showed that whenever this property, called LC, holds for l, the first case of Fermat's Last Theorem holds for l too. He also introduced an equivalent property $(LC)^+$ ([6]): α_1 is orthogonal to the multiplicative group U^+ of real units (resp. $C^+ = C \cap \mathbf{R}$ of real cyclotomic units), in $\mathbf{Q}(\zeta)$, if and only if $a \equiv 0$ or -1 $(mod\ l)$ or $a \equiv 1$ $(mod\ l^2)$. His proof of the equivalence of LC and $(LC)^+$ amounted essentially to showing that $a - \zeta$ is orthogonal to C^+ if and only if $a^l - \zeta$ is orthogonal to C.

In a previous paper ([3]), we established necessary and sufficient conditions for α_1 to be orthogonal to C, and noted the reduction of the conjecture to showing that if α_1 is orthogonal to C then $a \equiv 0$, 1 or -1 $(mod\ l)$. In this paper, based on the previous one, we prove that the conjecture is true for all regular primes $l \geq 5$. This also follows from ([5], Enoncé 8), which refers to arguments of Hasse and Mirimanoff. However, the present approach is quite different, as the proof here uses a result of Carlitz and Olson ([1, 4]) expressing a determinant of Maillet in terms of the relative class number of $\mathbf{Q}(\zeta)$.

I am grateful to Guy Terjanian who brought the result in ([1]) to my attention, and shared with me some of his unpublished work and insights into the subject.

1991 *Mathematics Subject Classification.* 11R18, 11A15, 11D41.

§1 ORTHOGONALITY CONDITIONS

We assume in the sequel that the relative integer $a \not\equiv 1 (mod\ l)$. By Theorem 2 of [3], α_1 is orthogonal to C if and only if the following two conditions are satisfied:

$$\text{(I)} \qquad a^l \equiv a, \quad (a-1)^l \equiv a-1, \quad (a+1)^l \equiv a+1 \qquad (mod\ l^2)$$

and

$$\text{(II)} \qquad \sum_{k=1}^{l-1} \left[\frac{nk}{l}\right] \frac{a^k}{k} = 0, \quad \text{in } \mathbf{F}_l, \quad \text{for } 1 \le n \le l-1$$

where, for a real number x, $[x]$ is the largest integer $\le x$.

It is easily verified that

$$(1) \qquad \left[\frac{nk}{l}\right] + \left[\frac{(l-n)k}{l}\right] = k-1 \qquad (1 \le n,\ k \le l-1).$$

Hence, for $1 \le n \le l-1$,

$$(2) \qquad \sum_{k=1}^{l-1} \left[\frac{nk}{l}\right] \frac{a^k}{k} + \sum_{k=1}^{l-1} \left[\frac{(l-n)k}{l}\right] \frac{a^k}{k} = \sum_{k=1}^{l-1} (k-1)\frac{a^k}{k} =$$
$$\sum_{k=1}^{l-1} a^k - \sum_{k=1}^{l-1} \frac{a^k}{k} = \frac{a^l - a}{a-1} - \frac{(a-1)^l - a^l + 1}{l},$$

the last equality following from [3], Lemma 2. In $\mathbf{F}_l$, $\frac{a^l-a}{a-1} = 0$ and, taking into account condition (I), $\frac{(a-1)^l - a^l + 1}{l} = 0$. Therefore, in conjunction with (I), we have

$$(3) \qquad \sum_{k=1}^{l-1} \left[\frac{(l-n)k}{l}\right] \frac{a^k}{k} = -\sum_{k=1}^{l-1} \left[\frac{nk}{l}\right] \frac{a^k}{k} \qquad (1 \le n \le l-1),$$

so that in (II), the equation for $l-n$ is a consequence of that for n. Thus, one may limit consideration in (II) to $1 \le n \le \frac{l-1}{2}$, and even to $2 \le n \le \frac{l-1}{2}$, since the equation for $n = 1$ is a trivial identity. We also note that the equation for $n = 2$ can be written

$$\text{(II-2)} \qquad \sum_{k=\frac{l+1}{2}}^{l-1} \frac{a^k}{k} = 0.$$

Exchanging k and n in (1), we get

$$(1') \qquad \left[\frac{nk}{l}\right] + \left[\frac{n(l-k)}{l}\right] = n-1 \qquad (1 \le n,\ k \le l-1).$$

Hence, for $1 \leq n \leq l-1$,

$$(4) \qquad \sum_{k=1}^{l-1} \left[\frac{nk}{l}\right] \frac{a^k}{k} = \sum_{k=1}^{\frac{l-1}{2}} \left[\frac{nk}{l}\right] \frac{a^k}{k} + \sum_{k=1}^{\frac{l-1}{2}} \left[\frac{n(l-k)}{l}\right] \frac{a^{l-k}}{l-k} =$$
$$\sum_{k=1}^{\frac{l-1}{2}} \left[\frac{nk}{l}\right] \frac{a^k + a^{l-k}}{k} + (n-1) \sum_{j=\frac{l+1}{2}}^{l-1} \frac{a^j}{j},$$

where the latter sum is equal to 0 if (II-2) is satisfied. Moreover, in the sum before the last, if $1 \leq n \leq \frac{l-1}{2}$, one may drop the terms corresponding to $k = 1, 2$, for which $\left[\frac{nk}{l}\right] = 0$. Therefore the conditions (I) and (II) are equivalent to the conjunction of (I), (II-2) and the following

$$(II') \qquad \sum_{k=3}^{\frac{l-1}{2}} \left[\frac{nk}{l}\right] \frac{a^k + a^{l-k}}{k} = 0 \qquad (3 \leq n \leq \frac{l-1}{2}).$$

Hence

Proposition 1. *Let $a \in \mathbf{Z}$, $a \not\equiv 1 \pmod{l}$ and $\alpha_1 = a - \zeta$. Then α_1 is orthogonal to the group C of cyclotomic units in $\mathbf{Z}[\zeta]$ if and only if the conditions (I), (II-2) and (II') are satisfied. In particular, in this case, the elements $y_k = \frac{a^k + a^{l-k}}{k}$ in $\mathbf{F}_l$ $(3 \leq k \leq \frac{l-1}{2})$ form a solution of the system of $\frac{l-5}{2}$ linear homogeneous equations in $\frac{l-5}{2}$ unknowns*

$$(S) \qquad \sum_{k=3}^{\frac{l-1}{2}} \left[\frac{nk}{l}\right] y_k = 0 \qquad (3 \leq n \leq \frac{l-1}{2}).$$

Remark 1 The system (S) is trivial for $l = 5$. But then, one may check directly that the only solutions of (II-2) are $a \equiv 0$ or $2 \pmod 5$, in which case condition (I) is then satisfied only if $a \equiv 0 \pmod{5^2}$. Thus the conjecture holds for $l = 5$ and we may assume in what follows that $l \geqq 7$.

Let Δ_l be the determinant of the $\frac{l-5}{2} \times \frac{l-5}{2}$ matrix A of coefficients of (S), i.e.

$$(6) \qquad A = \left(\left[\frac{nk}{l}\right]\right)_{3 \leq n,\ k \leq \frac{l-1}{2}}, \qquad \Delta_l = |A|.$$

We may compute Δ_l in $\mathbf{Z}$ and then reduce it $(\mathrm{mod}\ l)$ to get its value in $\mathbf{F}_l$.

§2 Maillet's determinant

For any $x \in \mathbf{Z}$, denote by $res_l(x)$ the least residue $\geqq 0$ of $x \pmod l$, i.e.

$$(7) \qquad res_l(x) = x - l\left[\frac{x}{l}\right].$$

If $l \nmid x$, denote by x' the least positive inverse of x $(mod\ l)$, i.e. $1 \leq x' \leq l-1$ and $xx' \equiv 1\ (mod\ l)$.

Maillet's determinant is defined ([1, 4]) to be of order $\frac{l-1}{2}$ and to have its (n,k)-th entry equal to $res_l(nk')$, for $1 \leq n,\ k \leq \frac{l-1}{2}$, i.e.

$$D_l = \left| \left(res_l(nk') \right)_{1 \leq n,\ k \leq \frac{l-1}{2}} \right| . \tag{8}$$

In order to relate Δ_l and D_l, we start with Δ_l. In view of (7), if we multiply the matrix A by l, we get

$$lA = (nk - res_l(nk))_{3 \leq n,\ k \leq \frac{l-1}{2}} \quad , \quad |lA| = l^{\frac{l-3}{2}} \Delta_l . \tag{9}$$

Augmenting the matrix lA by a first column corresponding to $k=2$ in (9) then by a first row equal to $(2k)_{2 \leq k \leq \frac{l-1}{2}}$, we get the $\frac{l-3}{2} \times \frac{l-3}{2}$ matrix

$$B = (b_{nk})_{2 \leq n,\ k \leq \frac{l-1}{2}} \quad , \quad |B| = 4|lA| = 4l^{\frac{l-3}{2}} \Delta_l \ , \tag{10}$$

with $b_{nk} = nk - res_l(nk)$ if $3 \leq n \leq \frac{l-1}{2}$ and $b_{nk} = 2k$ if $n = 2$ $(2 \leq k \leq \frac{l-1}{2})$; the expression for the determinant of B being obtained by expansion along the first column. If, for every $3 \leq n \leq \frac{l-1}{2}$, we subtract from the row corresponding to n, in B, the first row multiplied by $n/2$, we get a matrix whose entries are of the form $\pm res_l(nk)$. We thus have

$$B' = (res_l(nk))_{2 \leq n,\ k \leq \frac{l-1}{2}} \quad , \quad |B'| = \pm|B| = \pm 4 l^{\frac{l-3}{2}} \Delta_l . \tag{11}$$

Let C be the $\frac{l-1}{2} \times \frac{l-1}{2}$ matrix obtained by augmenting B' by a first column all of whose entries are equal to 2 then by a first row whose first entry is 1 and all the others are 0. Thus B' borders B with a first row equal to $(1,0,\ldots,0)$ and a first column equal to $(1,2,\ldots,2)$, and we have $|C| = |B'|$. Adding to the first row of C the second row multiplied by $1/2$; then multiplying, in the resulting matrix, the first column by $l/2$, we get a matrix C' whose first column has all its entries equal to l and whose entries in the other columns are $res_l(nk)$ for $1 \leq n \leq (l-1)/2$, $2 \leq k \leq (l-1)/2$. Moreover $|C'| = \frac{l}{2}|C| = \frac{l}{2}|B'|$. In C', we add the first column to all the remaining ones; next, we add the new second column to the first one, then we multiply the resulting first column by $1/2$. We obtain a matrix C'' all of whose entries are of the form $l + res_l(nk)$ and whose determinant is $|C''| = \frac{1}{2}|C'| = \frac{l}{4}|B'|$. Thus, in view of (11), we have

$$C'' = (l + res_l(nk))_{1 \leq n,\ k \leq \frac{l-1}{2}} \quad , \quad |C''| = \pm l^{\frac{l-3}{2}} \Delta_l . \tag{12}$$

This leads to

Lemma.

$$D_l = \pm l^{\frac{l-3}{2}} \Delta_l .$$

Proof. Let π be the permutation of $\{1,2,\ldots,(l-1)/2\}$ given by $\pi(k) = min(k', l-k')$. By definition, D_l is the determinant of the matrix $R = (r_{nk})$ whose entries are

$r_{nk} = res_l(n\pi(k))$ if $k' \leq (l-1)/2$ and $r_{nk} = l - res_l(n\pi(k))$ if $k' \geqq (l+1)/2$, for $1 \leq n,\ k \leq (l-1)/2$. Since π is an involution, it is easily checked that $k' \leq (l-1)/2$ if and only if $\pi(k)' \leq (l-1)/2$. Thus, setting $j = \pi(k)$ and reordering the columns of R, we get a matrix

$$R' = (x_{nj})_{1 \leq n,\ j \leq \frac{l-1}{2}} \quad , \quad D_l = \pm|R'| \ , \tag{13}$$

with $x_{nj} = res_l(nj)$ if $j \notin J$ and $x_{nj} = l - res_l(nj)$ if $j \in J$, where J is the set of integers $1 \leq j \leq (l-1)/2$ such that $j' \geqq (l+1)/2$. Since the determinant of a matrix is a multilinear alternating function of its columns, we have

$$|R'| = \pm \sum_{j \in J} |R_j| \ , \tag{14}$$

where R_j is the $\frac{l-1}{2} \times \frac{l-1}{2}$ matrix whose j-th column has all its entries equal to l and whose entries in the other columns are $res_l(nk)$ for $k \neq j$ $(1 \leq n,\ k \leq (l-1)/2)$. Note that the determinant with entries $res_l(nk)$ $(1 \leq n,\ k \leq (l-1)/2)$ and all $|R_j|$ with $j \geqq 3$ have their second column equal to twice their first one, and are thus equal to 0. Therefore the summation in the right-hand side of (14) is for $j \in J \cap \{1,2\}$; and since $1 \notin J$ while $2 \in J$, then

$$|R'| = \pm|R_2|. \tag{15}$$

We similarly have for the matrix C'' in (12)

$$|C''| = \sum_{j=1}^{(l-1)/2} |R_j| = |R_1| + |R_2|. \tag{16}$$

Moreover, R_1 and R_2 differ only in their first two columns; and the second column in R_1 is twice the first one in R_2. Therefore $|R_1| = -2|R_2|$, and (16) becomes

$$|C''| = -|R_2|. \tag{17}$$

From (13), (15) and (17), $|D_l| = \pm|C''|$. Hence the result, in view of (12).

Proposition 2. *We have*

$$\Delta_l = \pm h^- \ ,$$

where h^- is the relative class number of $\mathbb{Q}(\zeta)$, i.e. $h^- = \frac{h}{h^+}$ where h and h^+ are the class numbers of $\mathbb{Q}(\zeta)$ and of its maximal real subfield $\mathbb{Q}(\zeta)^+$, respectively ([7]).

Proof. This resuls from the formula proved in [1] (see also [4]):

$$D_l = \pm l^{\frac{l-3}{2}} h^-$$

in view of the Lemma above.

§3 Conclusion

Theorem. *If l is a regular prime ≥ 5, then Terjanian's conjecture is true for l.*

Proof. We may assume $l \geq 7$, by Remark 1. Let $\alpha_1 = a - \zeta$ be orthogonal to C and suppose $a \not\equiv 1 \ (mod\ l)$. By Proposition 1, the elements $y_k = (a^k + a^{l-k})/k$ in $\mathbf{F}_l$ $(3 \leq k \leq (l-1)/2)$ form a solution of the system (S) of linear homogeneous equations. The determinant of the coefficients of (S) is, by Proposition 2, $\Delta_l = \pm h^-$. Since l is a regular prime, i.e. l does not divide the class number h of $\mathbf{Q}(\zeta)$, then l does not divide the factor h^- of h, i.e. $\Delta_l \neq 0$ in $\mathbf{F}_l$. Thus the system (S) has only the trivial solution in $\mathbf{F}_l$, i.e. $a^k + a^{l-k} \equiv 0 \ (mod\ l)$ for $3 \leq k \leq (l-1)/2$. Hence

$$a^{2k} \equiv -a^l \equiv -a \ (mod\ l) \qquad (3 \leq k \leq (l-1)/2).$$

In particular, $a^{l-1} \equiv -a \ (mod\ l)$, i.e. either $a \equiv 0 \ (mod\ l)$ or $a^{l-1} \equiv 1 \equiv -a \ (mod\ l)$. Thus, having assumed $a \not\equiv 1 \ (mod\ l)$, we have $a \equiv 0$ or $-1 \ (mod\ l)$. It then follows that ([3], Proposition 6) $a \equiv 0$ or $\pm 1 \ (mod\ l^2)$. This, in conjunction with Proposition 42 of [5], proves the desired conjecture (that l possesses the property LC, in the terminology of [5], §8).

Remark 2 In view of what was said in the Introduction (based on [5], Theorem 2), the previous Theorem implies a new (albeit indirect) proof of the first case of Fermat's Last Theorem for regular primes.

References

1. L. Carlitz, F.R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. 6 (1955), 265-269.
2. H. Hasse, *Bericht über die neueren Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetz*, Jahresbericht der D.M.V., Leipzig Berlin, 1930.
3. C. Helou, *Norm residue symbol and cyclotomic units*, Acta Arith. 73 (1995), 147-188.
4. P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer Verlag, New York Heidelberg Berlin, 1979.
5. G. Terjanian, *Sur la loi de réciprocité des puissances l-èmes*, Acta Arith. 54 (1989), 87-125.
6. G. Terjanian, *Correspondence* (1994).
7. L. Washington, *Introduction to Cyclotomic Fields*, Springer Verlag, New York Heidelberg Berlin, 1982.

Penn State University, Delaware County, 25 Yearsley Mill Rd, Media, PA 19063
e-mail address: cxh22@psuvm.psu.edu

Received July 31, 1996

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

The A-B-C-Cohomologies for Dynamical Systems

Oleg I. Bogoyavlenskij*

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

Abstract: The A-B-C-cohomologies $H^m_A(V, M^n)$, $H^m_B(V, M^n)$, $H^m_C(V, M^n)$ are introduced for a dynamical system V on a smooth manifold M^n. The representations R_m of the Lie algebra S of symmetries of the dynamical systems V in the A-B-C-cohomologies are constructed. The invariance of the B-cohomologies $H^m_B(V, M^n)$ with respect to any connected Lie group of symmetries of system V is established.

1. In paper [2], we introduced the cohomology $H^*(V, M^n)$ for the dynamical systems

$$\dot{x}^i = V^i(x^1, \cdots, x^n) \tag{1}$$

on the smooth manifolds M^n. In this paper we generalize that construction and consider a representation of the Lie algebra of symmetries S of the dynamical system V (1) in the newly-constructed A-B-C-cohomologies.

Let Λ^m_V be the linear space of the smooth differential m-forms on the manifold M^n that are invariant with respect to the dynamical system V (1). The operator i_V of the interior product and the operator d of the exterior derivation act on the V-invariant differential forms. Any V-invariant m-form ω_m is annihilated by the Lie derivative [1] $L_V = i_V \circ \mathrm{d} + \mathrm{d} \circ i_V$, $L_V \omega_m = 0$. Therefore the two operators i_V and d satisfy the equations

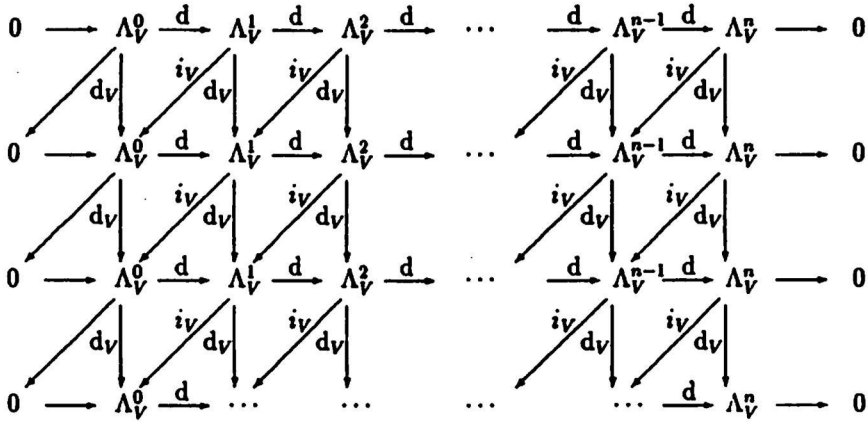
*Supported by NSERC grant OGPIN 337.

$$i_V^2 = 0, \quad d^2 = 0, \quad i_V \circ d = -d \circ i_V \tag{2}$$

on the V-invariant differential forms. In view of Eqs. (2), the operator $d_V = i_V \circ d = -d \circ i_V$ satisfies the equations

$$d_V^2 = 0, \quad d_V \circ i_V = i_V \circ d_V = 0, \quad d_V \circ d = d \circ d_V = 0. \tag{3}$$

The linear spaces Λ_V^m of the V-invariant differential forms with the three operators i_V, d and $d_V = i_V \circ d$ form the A-, B- and C-complexes respectively:



These complexes are invariant with respect to a shift in the vertical direction. Therefore their cohomologies have only one index.

II. We define three different rings of the A-, B- and C-cohomologies

$$H_A^*(V, M^n), \quad H_B^*(V, M^n), \quad H_C^*(V, M^n). \tag{4}$$

The ring structures in the cohomologies (4) are induced by the wedge product of the V-invariant differential forms. The rings $H_A^*(V, M^n)$, $H_B^*(V, M^n)$ and $H_C^*(V, M^n)$ are cohomologies with respect to the operators i_V, d and d_V respectively:

$$H_A^*(V, M^n) = \operatorname{Ker} i_V / \operatorname{Im} i_V, \quad H_B^*(V, M^n) = \operatorname{Ker} d / \operatorname{Im} d,$$

$$H_C^*(V, M^n) = \operatorname{Ker} d_V / \operatorname{Im} d_V.$$

The linear spaces (4) inherit the ring structure with respect to the wedge product of the V-invariant differential forms because the operators i_V and d are skew-derivations and the operator $\mathrm{d}_V = i_V \circ \mathrm{d}$ is a derivation:

$$\mathrm{d}_V(\omega \wedge \eta) = \mathrm{d}_V\omega \wedge \eta + \omega \wedge \mathrm{d}_V\eta.$$

Here ω and η are arbitrary V-invariant differential forms.

Remark 1. Recall that the B-cohomologies $H_B^*(V, M^n)$ coincide with those introduced in our paper [2]. Probably, the B-cohomologies are the most important of the A-B-C types considered here because of their interrelationships with the de Rham cohomologies [2-4]. Another reason is that only the B-cohomologies have analogues for the mappings of the manifold M^n into itself. Let $T : M^n \longrightarrow M^n$ be an arbitrary smooth mapping. There exists a complex of T-invariant differential forms with the operator d. We define the cohomologies of the mapping T: $H_B^*(T, M^n) = \mathrm{Ker}\,\mathrm{d}/\mathrm{Im}\,\mathrm{d}$. If T is a shift for the time $1/n$ along the trajectories of the dynamical system V (1), then the cohomologies $H_B^*(T, M^n)$ of the mapping T form an approximation of the B-cohomologies $H_B^*(V, M^n)$ of the dynamical system V.

Remark 2. For any constant c, the operator $\mathrm{d}_c = \mathrm{d} + c i_V$ satisfies the equation $\mathrm{d}_c^2 = 0$ on the V-invariant differential forms. Therefore there exist the cohomologies with respect to the operator d_c as well.

III. An example. Let us consider the dynamical system V:

$$\dot{J}_i = 0, \quad \dot{\varphi}_i = J_i \tag{5}$$

in the toroidal domain $\mathcal{O} = B_a \times \mathbb{T}^k$ where B_a is a k-dimensional ball, and $J_i \in B_a$, $\varphi_i \in \mathbb{T}^k$. The system (5) is the canonical form [3] of all Liouville-integrable Hamiltonian systems that are non-degenerate in the Kolmogorov sense and have compact invariant submanifolds. In paper [3], we demonstrated that the V-invariant 1-, 2-, and 3-forms have the form

$$\omega_1 = \theta_i(J)\mathrm{d}J_i, \tag{6}$$

$$\omega_2 = a_{i\ell}(J)\mathrm{d}J_i \wedge \mathrm{d}J_\ell + b_{i\ell}(J)\mathrm{d}J_i \wedge \mathrm{d}\varphi_\ell, \tag{7}$$

$$\omega_3 = b_{i\ell m}(J)\mathrm{d}J_i \wedge \mathrm{d}J_\ell \wedge \mathrm{d}\varphi_m + c_{i\ell m}(J)\mathrm{d}J_i \wedge \mathrm{d}J_\ell \wedge \mathrm{d}J_m. \tag{8}$$

Here coefficients $a_{i\ell}(J)$ and $c_{i\ell m}(J)$ are alternating and coefficients $b_{i\ell}(J)$ and $b_{i\ell m}(J)$ satisfy the equations $b_{i\ell}(J) = b_{\ell i}(J)$, $b_{i\ell m}(J)+b_{\ell mi}(J)+b_{mi\ell}(J) = 0$.

(*a*) For the V-invariant differential forms (6) - (8), we have

$$i_V\omega_1 = 0, \quad i_V\omega_2 = -b_{i\ell}(J)J_\ell \mathrm{d}J_i, \quad i_V\omega_3 = b_{i\ell m}(J)J_m \mathrm{d}J_i \wedge \mathrm{d}J_\ell. \tag{9}$$

Hence we find $H^1_A(V,\mathcal{O}) = 0$, $H^2_A(V,\mathcal{O}) = R^\infty$. The elements of the cohomology group $H^2_A(V,\mathcal{O})$ are represented by the 2-forms

$$\omega_{2a} = b_{i\ell}(J)\mathrm{d}J_i \wedge \mathrm{d}\varphi_\ell, \tag{10}$$

where $b_{i\ell}(J) = b_{\ell i}(J)$ and $b_{i\ell}(J)J_\ell = 0$.

(*b*) In papers [2,3], we proved that $H^1_B(V,\mathcal{O}) = 0$, $H^2_B(V,\mathcal{O}) = R^\infty$, $H^3_B(V,\mathcal{O}) = 0$. The elements of the cohomology group $H^2_B(V,\mathcal{O})$ are represented by the closed 2-forms

$$\omega_{2b} = \frac{\partial^2 B(J)}{\partial J_i \partial J_\ell}\mathrm{d}J_i \wedge d\varphi_\ell, \tag{11}$$

where $B(J)$ is an arbitrary smooth function.

(*c*) Eqs. (7) and (9) yield $\mathrm{d}_V\omega_2 = -\mathrm{d}i_V\omega_2 = \mathrm{d}(b_{i\ell}(J)J_\ell) \wedge \mathrm{d}J_i$. Therefore the cohomologies $H^2_C(V,M^n) = R^\infty$ are represented by the 2-forms

$$\omega_{2c} = a_{i\ell}(J)\mathrm{d}J_i \wedge \mathrm{d}J_\ell + b_{i\ell}(J)\mathrm{d}J_i \wedge \mathrm{d}\varphi_\ell, \quad b_{i\ell}(J)J_\ell = \frac{\partial C(J)}{\partial J_i}, \tag{12}$$

where $C(J)$ is an arbitrary smooth function and $b_{i\ell}(J) = b_{\ell i}(J)$.

The formulae (10) - (12) imply that the three cohomology groups $H^2_A(V,\mathcal{O})$, $H^2_B(V,\mathcal{O})$, $H^2_C(V,\mathcal{O})$ are different and that the B-cohomology group $H^2_B(V,\mathcal{O})$ is the "smallest" one.

IV. **Theorem 1** *The Lie derivative operator L_U defines the representations R_m of the Lie algebra S of symmetries of a dynamical systems V in the cohomologies*

$$H^m_A(V,M^n), \quad H^m_B(V,M^n), \quad H^m_C(V,M^n).$$

The representations R_m in the B-cohomologies $H^m_B(V,M^n)$ are trivial.

Proof. For any symmetry $U \in S$ and any V-invariant (ℓ, k) tensor T^ℓ_k, we have $L_V L_U T^\ell_k = (L_U L_V - L_{[U,V]})T^\ell_k = 0$. Hence the (ℓ, k) tensor $L_U T^\ell_k$ is V-invariant.

(a) Any element of the group $H^m_A(V, M^n)$ has the form $\omega_m + i_V\omega_{m+1}$, where $i_V\omega_m = 0$. The two operators i_V and L_U commute in view of the identity $L_U i_V - i_V L_U = i_{[U,V]}$ and the equation $[U, V] = 0$. Hence we obtain

$$L_U(\omega_m + i_V\omega_{m+1}) = L_U\omega_m + i_V L_U\omega_{m+1}, \quad i_V L_U\omega_m = L_U i_V\omega_m = 0.$$

Therefore, the representation R_m is well defined.

(b) Any element of the group $H^m_B(V, M^n)$ has the form $\omega_m + \mathrm{d}\omega_{m-1}$, where $\mathrm{d}\omega_m = 0$. Applying the Cartan formula $L_U = \mathrm{d} \circ i_U + i_U \circ \mathrm{d}$, we find

$$L_U(\omega_m + \mathrm{d}\omega_{m-1}) = \mathrm{d}(i_U\omega_m + L_U\omega_{m-1}).$$

This element represents zero in the group $H^m_B(V, M^n)$.

(c) Any element of the group $H^m_C(V, M^n)$ has the form $\omega_m + \mathrm{d}_V\tilde{\omega}_m$ where $\mathrm{d}_V\omega_m = 0$. Applying Eqs. (2) and the equation $i_U \circ i_V = -i_V \circ i_U$, we obtain

$$L_U(\omega_m + \mathrm{d}_V\tilde{\omega}_m) = L_U\omega_m + \mathrm{d}_V L_U\tilde{\omega}_m,$$

$$\mathrm{d}_V L_U\omega_m = i_V\mathrm{d}(\mathrm{d} \circ i_U + i_U \circ \mathrm{d})\omega_m = \mathrm{d}i_U i_V\mathrm{d}\omega_m = \mathrm{d}i_U\mathrm{d}_V\omega_m = 0.$$

Therefore the representation R_m is well defined. □

Theorem 1 implies that any one-parametric group of symmetries of a dynamical system V defines the identity representation of $\mathbb{R}^1$ in the B-cohomologies $H^m_B(V, M^n)$. Therefore, any connected Lie group of symmetries G preserves the B-cohomologies $H^*_B(V, M^n)$ and does not preserve in general the cohomologies $H^*_A(V, M^n)$ and $H^*_C(V, M^n)$.

V. We introduce another set of cohomologies using Eqs. (2) and (3). The A-cohomologies $H^*_A(V, M^n)$ form a differential complex with respect to the operator d:

$$0 \longrightarrow H^0_A(V, M^n) \xrightarrow{d} H^1_A(V, M^n) \xrightarrow{d} \cdots \xrightarrow{d} H^n_A(V, M^n) \longrightarrow 0. \qquad (13)$$

Let $H^*_{AB}(V, M^n)$ denote the cohomology ring of the complex (13).

The B-cohomologies $H^*_B(V, M^n)$ form a differential complex with respect to the operator i_V:

$$0 \longleftarrow H^0_B(V, M^n) \xleftarrow{i_V} H^1_A(V, M^n) \xleftarrow{i_V} \cdots \xleftarrow{i_V} H^n_B(V, M^n) \longleftarrow 0. \qquad (14)$$

Let $H^*_{BA}(V, M^n)$ denote the cohomology ring of the complex (14). Note that the operator d_V annihilates the cohomologies $H^*_A(V, M^n)$ and $H^*_B(V, M^n)$.

The C-cohomologies $H^*_C(V, M^n)$ form the two differential complexes with respect to the operators i_V and d:

$$0 \longleftarrow H^0_C(V, M^n) \xleftarrow{i_V} H^1_C(V, M^n) \xleftarrow{i_V} \cdots \xleftarrow{i_V} H^n_C(V, M^n) \longleftarrow 0.$$

$$0 \longrightarrow H^0_C(V, M^n) \xrightarrow{d} H^1_C(V, M^n) \xrightarrow{d} \cdots \xrightarrow{d} H^n_C(V, M^n) \longrightarrow 0.$$

Let $H^*_{CA}(V, M^n)$ and $H^*_{CB}(V, M^n)$ denote the cohomology rings of these two complexes respectively.

Remark 3. The Lie derivative operator L_U defines the representations R_m of the Lie algebra S of symmetries of the dynamical systems V in the cohomologies $H^m_{AB}(V, M^n)$, $H^m_{BA}(V, M^n)$, $H^m_{CA}(V, M^n)$, $H^m_{CB}(V, M^n)$. The same methods as in Theorem 1 prove that the representations R_m in the cohomologies $H^m_{AB}(V, M^n)$ and $H^m_{BA}(V, M^n)$ are trivial.

References

[1] Marsden, J. E., & Ratiu, T. S. 1994 *Introduction to Mechanics and Symmetry.* New York: Springer Verlag.

[2] Bogoyavlenskij, O. I. 1995 *C.R. Math.Rep.Acad.Sci.Canada* **17**, 253-258.

[3] Bogoyavlenskij, O. I. 1996 *Comm. in Math. Physics.*

[4] De Rham, G. 1931 *Jour. de Math. Pures et Appl.* **10**, 115-200.

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

Received August 13, 1996

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

Fluid velocity fields derived from the Navier-Stokes equations

K. B. Ranger, F.R.S.C.

Department of Mathematics, University of Toronto
Toronto, Ontario, M5S 3G3, Canada

Abstract: It is shown that there is a class of solutions to the Navier-Stokes equations in which the pressure field is a general three-dimensional harmonic which may be considered as the forcing flow and one of the Cartesian components of velocity is an arbitrary function of position and time subject to suitable conditions explained in the presentation. The remaining two velocity components can be found by the application of appropriate integrability or consistency conditions.

Introduction According to the Oxford English Dictionary the word, 'arbitrary', means, 'derived from mere opinion or random choice'. The purpose of the following short paper is to show that the Navier-Stokes equations for viscous, incompressible flow can exhibit solutions in which one Cartesian component of fluid velocity is an arbitrary function of the space and time coordinates, subject to the usual preferential conditions of continuity and differentiability. In addition the pressure field is a general three dimensional harmonic. By the application of a suitable integrability or consistency condition it is possible to explicitly construct the remaining two velocity components. If $\underline{q}$ is the fluid velocity then the results found here are applicable to regions of the fluid in which $(\underline{q}\cdot\text{curl}\,\underline{q}) \neq 0$. Since $u_3 = (\underline{q}\cdot\hat{x}_3)$ is arbitrary, where $\mathcal{O}(x_1, x_2, x_3)$ is a fixed frame of reference, the velocity field $\underline{q}$ exists at least for a region of finite extent.

The flow equations and method of solution. The phenomenological equations describing the motion of a viscous incompressible liquid based on a Newtonian rheology are defined by

$$\frac{\partial \underline{q}}{\partial t} + (\underline{q}\cdot\underline{\nabla})\underline{q} = -\underline{\nabla}P + \nu\nabla^2\underline{q} \tag{1}$$

$$\text{div}\ \underline{q} = 0, \quad P = p/\rho_0 \tag{2}$$

where $\underline{q} = u_j\hat{x}_j$, $u_j \equiv u_j(x_1, x_2, x_3, t)$, $j = 1,2,3$ is the fluid velocity, $p \equiv p(x_1, x_2, x_3, t)$ is the pressure field, ρ_0 the constant density and ν the kinematic viscosity. It is convenient for the present analysis to decompose the velocity field in the form

$$\underline{q} = \underline{Q} + \underline{\nabla}\phi, \quad \underline{Q} = Q_j\hat{x}_j, \quad u_3 = Q_3 + o_{x_3}, \tag{3}$$

where $o, \underline{Q}$ are scalar and vector functions of (x_1, x_2, x_3, t) respectively. It is also supposed that u_3 is arbitrarily prescribed subject to suitable conditions of continuity and differentiability. There is also a further condition which will appear later in the analysis. With the aid of standard vector identities equations (1), (2), (3), can be recast in terms of an equivalent set of equations expressed by

$$[\underline{\gamma} \times (\underline{Q} + \underline{\nabla}\phi)] = [\text{curl}\,\underline{Q} \times (\underline{Q} + \nabla\phi)] = \underline{\nabla}B + \nu\nabla^2\underline{Q} - \frac{\partial \underline{Q}}{\partial t}, \tag{4}$$

$$\operatorname{div} \underline{Q} + \nabla^2 \phi = 0, \quad u_3 = Q_3 + \phi_{x_3}, \tag{5}$$

and $\underline{\gamma} = \operatorname{curl} \underline{Q} + \lambda(\underline{Q} + \nabla\phi)$, where λ is an arbitrary scalar function of position and time. The part of these equations involving $\underline{\gamma}$ will be relevant at a later point in the analysis. The scalar extended Bernoulli function is defined by $B = \nu\nabla^2\phi - \phi_t - P - \frac{1}{2}|\underline{q}|^2$. With $\underline{W} = W_j \hat{x}_j = \operatorname{curl} \underline{Q}$, this system of equations is completely equivalent to the set expressed by (1), (2) and

$$\phi_{x_1} = \frac{B_{x_2} + \nu\nabla^2 Q_2 + W_1 u_3}{W_3}, \quad \phi_{x_2} = \frac{W_2 u_3 - B_{x_1} - \nu\nabla^2 Q_1}{W_3}, \tag{6}$$

$$\phi_{x_3} = u_3 - Q_3, \quad \operatorname{div} \underline{Q} + \nabla^2 \phi = 0, \tag{7}$$

together with the equation

$$W_1(B_{x_1} + \nu\nabla^2 Q_1 - \frac{\partial Q_1}{\partial t}) + W_2(B_{x_2} + \nu\nabla^2 Q_2 - \frac{\partial Q_2}{\partial t}) + W_3(B_{x_3} + \nu\nabla^2 Q_3 - \frac{\partial Q_3}{\partial t}) = 0. \tag{8}$$

The basic assumption to be made at this point in the analysis is that $W_3 = \frac{\partial Q_2}{\partial x_1} - \frac{\partial Q_1}{\partial x_2} = K$ where $K \neq 0$ can be chosen to be a constant. In this case equations (6), (7) are linear inhomogeneous if u_3 is given or prescribed and may be exhibited in the form

$$\frac{\partial}{\partial x_1}(\nu\nabla^2 Q_1 - \frac{\partial Q_1}{\partial t} + W_1 u_3) + \frac{\partial}{\partial x_2}(W_2 u_3 - \nu\nabla^2 Q_1 + \frac{\partial Q_1}{\partial t}) + K\frac{\partial u_3}{\partial x_3} = 0, \tag{9}$$

$$K^2 + B_{x_1 x_1} + B_{x_2 x_2} + \frac{\partial}{\partial x_1}(\nu\nabla^2 Q_1 - \frac{\partial Q_1}{\partial t} - W_2 u_3) + \frac{\partial}{\partial x_2}(W_1 u_3 + \nu\nabla^2 Q_2 - \frac{\partial Q_2}{\partial t}) = 0, \tag{10}$$

$$(W_1 - \frac{\partial u_3}{\partial x_2})K + \frac{\partial}{\partial x_3}(W_2 u_3 - \nu\nabla^2 Q_1 + \frac{\partial Q_1}{\partial t}) - B_{x_1 x_3} = 0. \tag{11}$$

$$\frac{\partial Q_2}{\partial x_1} - \frac{\partial Q_1}{\partial x_2} = K. \tag{12}$$

As already remarked equations (9)-(12) constitute a linear inhomogeneous system and solutions exist for Q_j, $j = 1, 2, 3$. B without restricting u_3. In turn it follows from (6), (7) that ϕ also exists. However with the constraints $W_3 = K$, $Q_3 + \phi_{x_3} = u_3$, it appears that the additional equation (8) which is part of the full system of the Navier-Stokes equations is not satisfied and the system is over-determined. To show this is *not* the case can be established by the following argument. First it is observed that if $\underline{\gamma} = \operatorname{curl} \underline{Q} + \lambda(\underline{Q} + \underline{\nabla}\phi)$, where λ is any function of position and time then

$$\begin{aligned} &\operatorname{div}\{[\operatorname{curl} \underline{Q} \times (\underline{Q} + \underline{\nabla}\phi)] - \underline{\nabla} B - \nu\nabla^2 \underline{Q} + \frac{\partial \underline{Q}}{\partial t}\} \\ &= \operatorname{div}\{[\underline{\gamma} \times (\underline{Q} + \underline{\nabla}\phi)] - \underline{\nabla} B - \nu\nabla^2 \underline{Q} + \frac{\partial \underline{Q}}{\partial t}\} \\ &= ((\underline{Q} + \underline{\nabla}\phi) \cdot \operatorname{curl} \underline{\gamma}) - |\operatorname{curl} \underline{Q}|^2 - \lambda((\underline{Q} + \underline{\nabla}\phi) \cdot \operatorname{curl} \underline{Q}) - \nabla^2 B - \nu\nabla^2 \operatorname{div} \underline{Q} \\ &\quad + \frac{\partial}{\partial t} \operatorname{div} \underline{Q} = 0, \end{aligned} \tag{13}$$

if λ is defined by

$$\lambda = \frac{((\underline{Q} + \underline{\nabla}\phi) \cdot \text{curl } \underline{\gamma}) - |\text{curl } \underline{Q}|^2 - \nabla^2 B - \nu\nabla^2 \text{div } \underline{Q} + \frac{\partial}{\partial t}\text{div } \underline{Q}}{((\underline{Q} + \underline{\nabla}\phi) \cdot \text{curl } \underline{Q})}, \tag{14}$$

and $((\underline{Q} + \underline{\nabla}\phi) \cdot \text{curl } \underline{Q}) \neq 0$, in the fluid region. The partial differential equation for $\underline{\gamma}$ can then be displayed by

$$\underline{\gamma}((\underline{Q} + \underline{\nabla}\phi) \cdot \text{curl } \underline{Q}) = \text{curl } \underline{Q}((\underline{Q} + \nabla\phi) \cdot \text{curl } \underline{Q}) \tag{15}$$
$$+ (\underline{Q} + \underline{\nabla}\phi)\{((\underline{Q} + \underline{\nabla}\phi) \cdot \text{curl } \underline{\gamma}) - |\text{curl } \underline{Q}|^2 - \nabla^2 B - \nu\nabla^2 \text{div } \underline{Q} + \frac{\partial}{\partial t}\text{div } \underline{Q}\}.$$

This additional linear inhomogeneous equation possesses solutions for $\underline{\gamma}$ which exists in the fluid region ensuring that (13) is satisfied without restricting $\underline{Q}, B$ or u_3. In view of (13) there is a vector function $\underline{R} = R_j \hat{x}_j$ such that

$$[\text{curl } \underline{Q} \times [\underline{Q} + \underline{\nabla}\phi]] - \underline{\nabla}B - \nu\nabla^2 \underline{Q} + \frac{\partial \underline{Q}}{\partial t} = \text{curl } \underline{R}, \tag{16}$$

and from (6), (7) which lead to (9)-(12) it follows that

$$\frac{\partial R_2}{\partial x_3} - \frac{\partial R_3}{\partial x_2} = \frac{\partial R_3}{\partial x_1} - \frac{\partial R_1}{\partial x_3} = 0. \tag{17}$$

This in turn implies $\frac{\partial R_1}{\partial x_2} - \frac{\partial R_2}{\partial x_1} = 0$. At this point (8) can be satisfied and there is a solution of the Navier-Stokes equations in which u_3 is given or prescribed and $(\underline{q} \cdot \text{curl } \underline{q}) \neq 0$.

With this knowledge it is of interest to construct the remaining velocity components u_1, u_2. To this end it is expedient to consider the system of equations

$$\text{div } \{(\underline{q} \cdot \underline{\nabla})\underline{q} + \frac{\partial \underline{q}}{\partial t} + \underline{\nabla}P\} = \text{div } \underline{q} = 0. \tag{18}$$

$$\frac{\partial u_3}{\partial t} + (\underline{q} \cdot \underline{\nabla})u_3 = -P_{x_3} + \nu\nabla^2 u_3, \tag{19}$$

in which u_3 is prescribed. Since $\text{div } (\nu\nabla^2 \underline{q}) = 0$, equation (18) implies that

$$\frac{\partial \underline{q}}{\partial t} + (\underline{q} \cdot \underline{\nabla})\underline{q} = -\underline{\nabla}P + \nu\nabla^2 \underline{q} + \text{curl } \underline{H}, \tag{20}$$

where $\underline{H}$ is a vector function of position and time with $\text{div } \underline{H} = 0$. Equation (20) implies that the Navier-Stokes equations, viz.

$$\text{curl } \left\{ \frac{\partial \underline{q}}{\partial t} + (\underline{q} \cdot \underline{\nabla})\underline{q} + \underline{\nabla}P - \nu\nabla^2 \underline{q} \right\} = 0, \tag{21}$$

only if

$$\text{curl}^2 \underline{H} = \text{grad div } \underline{H} - \nabla^2 \underline{H} = -\nabla^2 \underline{H} = 0. \tag{22}$$

Since div $\underline{H} = 0$, there exists $\underline{S} \equiv S(x_1, x_2, x_3, t)$ such that $\underline{H} = \text{curl } \underline{S}$ and $\nabla^2 \underline{S} = 0$. In this case equation (20) can be re-written as

$$\frac{\partial \underline{q}}{\partial t} + (\underline{q} \cdot \underline{\nabla})\underline{q} = -\underline{\nabla} P + \nu \nabla^2 \underline{q} + \underline{\nabla} \text{div } \underline{S}, \tag{23}$$

and $\nabla^2 \text{div } \underline{S} = 0$. There are two situations to consider because if div $\underline{S}$ is constant, then the Navier-Stokes equations are satisfied but P, u_1, u_2 are determined by application of integrability conditions to the full system of equations and represent an excessively cumbersome exercise in terms of algebraic detail. As a result this case will be omitted from the present discussion. In the second case which is less complicated analytically, consistency is only achieved with the Navier-Stokes equations and the original system (18), (19), if P is chosen to be an arbitrary three dimensional harmonic, that is $\nabla^2 P = 0$. An appropriate representation for P is expressed by the integral formula in [1]. It is a straightforward matter to show that the only solutions of (18), (19) with P harmonic are solutions of the Navier-Stokes equations. This derivation may be illustrated by the following procedure.

If $\underline{q}$ is the Navier-Stokes solution with $\nabla^2 P = 0$, and $\underline{q}', P'$ is another solution of (18), (19) in which $(\underline{q} \cdot \hat{x}_3) = (\underline{q}' \cdot \underline{x}_3) = u_3$, and $\nabla^2 P' = 0$, then from the equation of continuity the most general form of $\underline{q}'$ is given by $\underline{q}' = \underline{q} + \text{curl } \psi \hat{x}_3$. The velocity fields $\underline{q}, \underline{q}'$ satisfy the system of equations

$$\begin{gathered} \text{div } \{(\underline{q} \cdot \underline{\nabla})\underline{q}\} = 0, \quad \text{div } \{(\underline{q}' \cdot \underline{\nabla})\underline{q}'\} = 0, \\ (\underline{q} \cdot \underline{\nabla})u_3 + \frac{\partial u_3}{\partial t} = -P_{x_3} + \nu \nabla^2 u_3, (\underline{q}' \cdot \underline{\nabla})u_3 + \frac{\partial u_3}{\partial t} = -P'_{x_3} - \nu \nabla^2 u_3. \end{gathered} \tag{24}$$

These equations imply that

$$\text{div } \{(\text{curl } \psi \hat{x}_3 \cdot \underline{\nabla})\underline{q} + (\underline{q} \cdot \underline{\nabla})\text{curl } \psi \hat{x}_3 + (\text{curl } \psi \hat{x}_3 \cdot \nabla)\text{curl } \psi \hat{x}_3\} = 0, \tag{25}$$

and

$$(\text{curl } \psi \hat{x}_3 \cdot \underline{\nabla})u_3 = P_{x_3} - P'_{x_3}, \tag{26}$$

or since $\nabla^2 P = \nabla^2 P' = 0$, (26) is equivalent to

$$\nabla^2 (\text{curl } \psi \hat{x}_3 \cdot \underline{\nabla})u_3 = 0. \tag{27}$$

The only consistent solution of (25), (27) without restricting $\underline{q}$ is $\psi =$ constant in which case $\underline{q}' = \underline{q}$.

Finally it is necessary to show (18), (19) with $\nabla^2 P = 0$ do in fact admit solutions u_1, u_2, because at first inspection the system appears to be over-determined. This is *not* the case and can be demonstrated by utilizing the earlier argument involving $\underline{\gamma}$. Now if $\underline{\gamma}' = \text{curl } \underline{q} + \lambda' \underline{q}$ where λ' is an arbitrary function of position and time, then

$$\begin{aligned} \text{div } \{(\underline{q} \cdot \underline{\nabla})\underline{q}\} &= \nabla^2 \frac{1}{2}|\underline{q}|^2 + \text{div } [\underline{\gamma}' \times \underline{q}] = \nabla^2 \frac{1}{2}|\underline{q}|^2 - (\underline{\gamma}' \cdot \text{curl } \underline{q}) + (\underline{q} \cdot \text{curl } \underline{\gamma}') \\ &= \nabla^2 \frac{1}{2}|\underline{q}|^2 - |\text{curl } \underline{q}|^2 + (\underline{q} \cdot \text{curl } \underline{\gamma}') - \lambda'(\underline{q} \cdot \text{curl } \underline{q}) = 0. \end{aligned} \tag{28}$$

if

$$\lambda' = \frac{\nabla^2 \tfrac{1}{2}|\underline{q}|^2 - |\text{curl } \underline{q}|^2 + (\underline{q} \cdot \text{curl } \underline{\gamma}')}{(\underline{q} \cdot \text{curl } \underline{q})}. \tag{29}$$

where $(\underline{q} \cdot \text{curl } \underline{q}) \neq 0$, in the fluid region. The partial differential equation for $\underline{\gamma}'$ is then given by

$$\underline{\gamma}' = \text{curl } \underline{q} + \underline{q} \frac{\{\nabla^2 \tfrac{1}{2}|\underline{q}|^2 - |\text{curl } \underline{q}|^2 + (\underline{q} \cdot \text{curl } \underline{\gamma}')\}}{(\underline{q} \cdot \text{curl } \underline{q})}. \tag{30}$$

Since (19) and $\text{div } \underline{q} = 0$ are both linear inhomogeneous if u_3 is prescribed then u_1, u_2 exist, and substitution in (30) shows that the equation for $\underline{\gamma}'$ is linear inhomogeneous and $\underline{\gamma}'$ exists so that (18) is satisfied. In fact there are solutions of (18) (19) which are mutually consistent provided that $(\underline{q} \cdot \text{curl } \underline{q}) \neq 0$.

It remains to construct the velocity components u_1, u_2 from (18), (19) and

$$u_2 = Au_1 + B', \tag{31}$$

where

$$A = -\frac{\partial u_3}{\partial x_1} \Big/ \frac{\partial u_3}{\partial x_2}, \quad B' = \left[\nu \nabla^2 u_3 - \frac{\partial u_3}{\partial t} - P_{x_3} - u_3 \frac{\partial u_3}{\partial x_3}\right] \Big/ \frac{\partial u_3}{\partial x_2}, \tag{32}$$

and from the equation of continuity

$$\frac{\partial u_1}{\partial x_2} = -\frac{1}{A}\frac{\partial u_1}{\partial x_1} - \frac{A_{x_2} u_1}{A} + C, \quad C = -\left(\frac{\partial B'}{\partial x_2} + \frac{\partial u_3}{\partial x_3}\right)\frac{1}{A}. \tag{33}$$

On explicit calculation (18) results in the equation

$$\begin{aligned} \text{div } (\underline{q} \cdot \underline{\nabla})\underline{q} &= 2\left\{\frac{\partial u_2}{\partial x_1} \cdot \frac{\partial u_1}{\partial x_2} + \frac{\partial u_3}{\partial x_1} \cdot \frac{\partial u_1}{\partial x_3} + \frac{\partial u_3}{\partial x_2} \cdot \frac{\partial u_2}{\partial x_3} - \frac{\partial u_1}{\partial x_1} \cdot \frac{\partial u_2}{\partial x_2} - \frac{\partial u_2}{\partial x_2} \cdot \frac{\partial u_3}{\partial x_3} - \frac{\partial u_1}{\partial x_1} \cdot \frac{\partial u_3}{\partial x_3}\right\} \\ &= 2\left\{\frac{\partial u_2}{\partial x_1} \cdot \frac{\partial u_1}{\partial x_2} + \frac{\partial u_3}{\partial x_1} \cdot \frac{\partial u_1}{\partial x_3} + \frac{\partial u_3}{\partial x_2} \cdot \frac{\partial u_2}{\partial x_3} - \frac{\partial u_1}{\partial x_1} \cdot \frac{\partial u_2}{\partial x_2} + \left(\frac{\partial u_3}{\partial x_3}\right)^2\right\} = 0. \end{aligned} \tag{34}$$

With the substitution (31) for u_2 in terms of u_1 a major simplification occurs because $\frac{\partial u_1}{\partial x_3}$ is eliminated and the only integrability condition is now

$$\left(\frac{\partial A}{\partial x_1}u_1 + \frac{\partial B'}{\partial x_1}\right)\frac{\partial u_1}{\partial x_2} - \left(\frac{\partial A}{\partial x_2}u_1 + \frac{\partial B'}{\partial x_2}\right)\frac{\partial u_1}{\partial x_1} = -\frac{\partial u_3}{\partial x_2} \cdot \frac{\partial A}{\partial x_3}u_1 - \left(\frac{\partial u_3}{\partial x_3}\right)^2 - \frac{\partial u_3}{\partial x_2} \cdot \frac{\partial B'}{\partial x_2}. \tag{35}$$

It is now possible to solve for $\frac{\partial u_1}{\partial x_1}, \frac{\partial u_1}{\partial x_2}$ from (33), (35) in the form

$$\frac{\partial u_1}{\partial x_1} = \frac{a'u_1^2 + b'u_1 + c'}{u_1 + d}, \quad \frac{\partial u_1}{\partial x_2} = \frac{au_1^2 + bu_1 + c}{u_1 + d}. \tag{36}$$

where

$$a = \frac{-\frac{\partial A}{\partial x_2}\cdot\frac{\partial A}{\partial x_1}}{\frac{\partial A}{\partial x_1}+A\frac{\partial A}{\partial x_2}}, \qquad a' = \frac{-\left(\frac{\partial A}{\partial x_2}\right)^2}{\frac{\partial A}{\partial x_1}+A\frac{\partial A}{\partial x_2}}, \tag{37}$$

$$b = \frac{A\frac{\partial u_3}{\partial x_2}\cdot\frac{\partial A}{\partial x_3}-\frac{\partial A}{\partial x_2}\cdot\frac{\partial B'}{\partial x_1}+AC\frac{\partial A}{\partial x_1}}{\frac{\partial A}{\partial x_1}+A\frac{\partial A}{\partial x_2}}, \qquad b' = \frac{AC\frac{\partial A}{\partial x_2}-\frac{\partial A}{\partial x_2}\cdot\frac{\partial B'}{\partial x_2}-\frac{\partial u_3}{\partial x_2}\cdot\frac{\partial A}{\partial x_3}}{\frac{\partial A}{\partial x_1}+A\frac{\partial A}{\partial x_2}}, \tag{38}$$

$$c = \frac{AC\frac{\partial B'}{\partial x_1}+A\left(\frac{\partial u_3}{\partial x_3}\right)^2+A\frac{\partial u_3}{\partial x_2}\cdot\frac{\partial B'}{\partial x_3}}{\frac{\partial A}{\partial x_1}+A\frac{\partial A}{\partial x_2}}, \qquad c' = \frac{AC\frac{\partial B'}{\partial x_2}-\left(\frac{\partial u_3}{\partial x_3}\right)^2-\frac{\partial u_3}{\partial x_2}\cdot\frac{\partial B'}{\partial x_3}}{\frac{\partial A}{\partial x_1}+A\frac{\partial A}{\partial x_2}}, \tag{39}$$

$$d = \frac{\frac{\partial B'}{\partial x_1}+A\frac{\partial B'}{\partial x_2}}{\frac{\partial A}{\partial x_1}+A\frac{\partial A}{\partial x_2}}, \qquad d' = \frac{\partial A}{\partial x_1}+A\frac{\partial A}{\partial x_2} \neq 0, \tag{40}$$

in the fluid region. Now the equations (18), (19) with $\nabla^2 P = 0$ have solutions in common with the flow equations and it only remains to apply the integrability or consistency condition $\frac{\partial^2 u_1}{\partial x_1 \partial x_2} = \frac{\partial^2 u_1}{\partial x_2 \partial x_1}$ to obtain the equation satisfied by u_1. This is found to be given by the cubic equation

$$p_0 u_1^3 + p_1 u_1^2 + p_2 u_1 + p_3 = 0 \tag{41}$$

where

$$p_0 = \frac{\partial a}{\partial x_1} - \frac{\partial a'}{\partial x_1}, \quad p_1 = d\frac{\partial a}{\partial x_1} + \frac{\partial b}{\partial x_1} - a\frac{\partial d}{\partial x_1} + ab' - ba' + a'\frac{\partial d}{\partial x_2} - d\frac{\partial a'}{\partial x_2} - \frac{\partial b'}{\partial x_2}$$

$$p_2 = 2(ac' - a'c) + d\frac{\partial b}{\partial x_1} - b\frac{\partial d}{\partial x_1} + \frac{\partial c}{\partial x_1} + b'\frac{\partial d}{\partial x_2} - d\frac{\partial b'}{\partial x_2} - \frac{\partial c'}{\partial x_2}$$

$$p_3 = bc' - cb' + d\frac{\partial c}{\partial x_1} - c\frac{\partial d}{\partial x_1} + c'\frac{\partial d}{\partial x_2} - d\frac{\partial c'}{\partial x_2}.$$

The cubic equation has at least one real root and can be treated by standard methods [2].

The calculation of u_1, u_2 in terms of P, u_3 now only requires a network of routine substitutions described by the above equations. This calculation is subject to the condition that $(q \cdot \operatorname{curl} q) \neq 0$, in the fluid region and this is guaranteed at least in a finite non-zero region of the fluid by the fact that u_3 is essentially arbitrary.

References

[1] Whittaker, E.T. and Watson, G.N., Ch. 18 in A course of Modern Analysis. *Cambridge University Press* 1962, p. 388-439.

[2] Birkhoff, G. & Maclane, S., A Survey of Modern Algebra, *Macmillan Company*, New York, 1953, p. 96.

Received November 4, 1996

C.R. Math Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

EXACT SOLUTIONS OF NAVIER-STOKES EQUATIONS BY RECURSIVE SERIES OF DIFFUSIVE QUOTIENTS

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

Abstract. Large classes of exact solutions for the velocity $\underline{u}$ and pressure p of suitably forced unsteady three dimensional Navier-Stokes equations are found, in rectangular coordinates. They are series $\underline{u} = \Sigma_m \underline{u_m}$, $p = \Sigma_m \overline{p_m}$, $\underline{u_m} = h^{-m}\underline{v_m}$, $\overline{p_m} = h^{-m}p_m$, where $\nabla_t h = \eta\nabla^2 h + r(\underline{x},t)h + s(\underline{x},t)$. The solution sequence $\{\underline{v_m}\}$ is obtained by introduction of a sequence of vector potentials $\{\underline{A_m}\}$ satisfying a difference relation $\underline{v_m} = \nabla \times \underline{A_m} + (m-1)\underline{A_{m-1}} \times (\nabla h)$, which also permits easy verification of incompressibility, where $\underline{A_m}$ satisfies linear differential equations. An auxiliary linear Poisson equation permits the determination of p_m from $\underline{v_m}$ and W_{m-1}, where $W_j = \{r, s, h, \underline{F}; v_1, \ldots, v_j, p_1, \ldots, p_j\}$, and $\underline{F}$ is a conservative force.

1. Introduction

General explicit methods (hodograph, Lie, Clarkson-Kruskal, pole series, etc.) for exact solution of non-linear systems have shown limited success with Navier-Stokes (N-S) systems. The Cole-Hopf solution of Burger's 1D model as the quotient $(-2\eta h^{-1}\nabla_x h)$ of two diffusions is well-known. The goal here is an extension of Cole-Hopf useful for N-S equations, initially considered by the writer around 1980, inspired by the BBGKY hierarchy for integration of the Liouville equation. Much of the work is based on electromagnetic (vector potential) techniques adapted to series of quotients, and conventional system theory for linear PDE. Rectangular coordinates are used to simplify analysis. The main equations (11), (21), (27) are slightly modified Ladyzhenskaya equations. Auxiliary are (12), (24), (32).

2. Proposals, Preliminaries, Incompressibility

The incompressible Navier-Stokes system is

$$\nabla_t \underline{u} + (u \cdot \nabla)\underline{u} + \nabla(\rho^{-1}p) = \eta\nabla^2\underline{u} + \underline{F},\ \underline{F} = -\nabla\Omega,\ \nabla \cdot \underline{u} = 0. \tag{1}$$

The ansatze proposed are

$$\underline{u} = \Sigma_m h^{-m}\underline{v_m},\quad p = \Sigma_m h^{-m} p_m,\quad \text{for } m \geq 1,\quad \text{where} \tag{2}$$

$$(\nabla_t - \eta\nabla^2)h = r(\underline{x},t)h + s(\underline{x},t),\quad h \neq 0 \text{ a.e.} \tag{3}$$

Eq. (3) is a forced (if $s \neq 0$), reaction (if $r \neq 0$) diffusion. Assume

$$\Omega = \Sigma_m h^{-m}\Omega_m, \tag{4}$$

where $\Omega_m(\underline{x},t)$ are independent of h. This series method could be called an SDQ (series diffusive quotient) method, since the paravelocities $\underline{v_m}$ are diffusions. The range of functions h satisfying Eq. (3) is large, since r and s are only assumed to be *piecewise* continuous, differentiable, etc.

From (2) and (3), rearranging powers of h^{-1} gives

$$\nabla_t \underline{u} = \Sigma_m h^{-m}\left[\nabla_t \underline{v_m} - mr\underline{v_m} - (m-1)\underline{v_{m-1}}(\eta\nabla^2 h + s)\right] \tag{5}$$

$$(6)\qquad (\underline{u}\cdot\nabla)\underline{u} = \Sigma_m h^{-m}\left[\Sigma_{\ell=1}^{m-1}(\underline{v}_\ell\cdot\nabla)\underline{v}_{m-\ell} - \Sigma_{\ell=1}^{m-2}(m-\ell-1)\underline{v}_{m-\ell-1}(\underline{v}_\ell\cdot\nabla)h\right].$$

From (2), note

$$(7)\qquad \nabla(\rho^{-1}p) = \rho^{-1}\Sigma_m h^{-m}[\nabla p_m - (m-1)p_{m-1}\nabla h].$$

$$(8)\qquad \underline{F} = -\Sigma_m h^{-m}[\nabla\Omega_m - (m-1)\Omega_{m-1}\nabla h].$$

The significant quantities $\nabla\cdot\underline{u}$, $\nabla\times\underline{u}$, $\nabla^2\underline{u}$ can also be expressed as SDQ. Thus

$$(9)\qquad \nabla\cdot\underline{u} = \Sigma_m h^{-m}[\nabla\cdot\underline{v}_m - (m-1)\underline{v}_{m-1}\cdot\nabla h],\ \nabla^2\underline{u} = \Sigma_m h^{-m}[\nabla^2\underline{v}_m$$
$$-2(m-1)(\nabla h\cdot\nabla)\underline{v}_{m-1} - (m-1)\underline{v}_{m-1}\nabla^2 h + (m-1)(m-2)\underline{v}_{m-2}(\nabla h)^2]$$

The first main result of the choice (2) of a quotient series for $\underline{u}$ is the incompressibility recursion theorem (which is independent of the choice (3) for h).

Theorem. *If $\{\underline{A}_m\}$ is any sequence of C'' vectors, and*

$$(10)\qquad \underline{v}_m = \nabla\times\underline{A}_m + (m-1)\underline{A}_{m-1}\times(\nabla h),\ \textit{for } m\geq 1,$$

then (2) implies that $\nabla\cdot\underline{u} = 0$ formally.

Outline of Proof. From (9), $\nabla\cdot\underline{u} = 0$ is implied by $\nabla\cdot\underline{v}_m = [(m-1)\underline{v}_{m-1}\cdot\nabla)]h$. But,

$$\nabla\cdot\underline{v}_m = (m-1)\nabla\cdot(\underline{A}_{m-1}\times(\nabla h)) = (m-1)[(\nabla\times\underline{A}_{m-1}\cdot\nabla]h$$
$$= (m-1)[(\underline{v}_{m-1} - (m-2)\underline{A}_{m-2}\times\nabla h))\cdot\nabla]h = (m-1)[(\underline{v}_{m-1}\cdot\nabla)h],$$

since the vector ∇h appears twice in the mixed triple product. Thus incompressibility is provided almost automatically by (2) and (10).

3. Momentum equation—first level

The momentum equations (1) are now separated by level, beginning with level 1 in h^{-1}. Collecting h^{-1} terms from (5) to (9) yields

$$(11)\qquad \nabla_t\underline{v}_1 - \eta\nabla^2\underline{v}_1 - r\underline{v}_1 + \nabla(\rho^{-1}p_1 + \Omega_1) = \underline{0},\ \nabla\cdot\underline{v}_1 = 0$$

The standard device of applying $\nabla\cdot$ and $\nabla\times$ to a vector equation yields first

$$(12)\qquad \nabla^2(\rho^{-1}p_1 + \Omega_1) = (\underline{v}_1\cdot\nabla)r$$

a Poisson equation for parapressure p_1 (if $\nabla r\neq 0$) which depends on $\underline{v}_1$, a Laplace equation, otherwise. Thus if r is time dependent only, then the p_1 problem is classical, but $\underline{v}_1$ must be found anyway.

Now $\nabla\times$ eliminates the force terms, leading to a para-vorticity equation

$$(13)\qquad \nabla\times[(\nabla_t - \eta\nabla^2 - r)\underline{v}_1] = (\nabla_t - \eta\nabla^2 - r)(\nabla\times\underline{v}_1) - (\nabla r)\times\underline{v}_1 = 0.$$

Again, if $\nabla r = 0$, the equation (13) simplifies to an unforced vector reaction diffusion equation for $\underline{\omega}_1 = \nabla \times \underline{v}_1$:

$$(\nabla_t - \eta\nabla^2 - r)\underline{\omega}_1 = 0, \ \nabla \cdot \underline{\omega}_1 = 0, \tag{14}$$

another Ladyzhenskaya equation which is almost classical, but apparently over-determined. This is also a problem for (13) if $\nabla r \neq 0$, since $\nabla \cdot \underline{v}_1 = 0$ is needed to "begin on" incompressibility.

The antivorticity device $\underline{v}_1 = \nabla \times \underline{A}_1$ is now invoked, producing a fourth-order properly determined equation

$$(\nabla_t - \eta\nabla^2 - r)\nabla \times (\nabla \times \underline{A}_1) - \nabla r \times (\nabla \times \underline{A}_1) = 0, \tag{15}$$

provided that $\nabla \cdot \underline{A}_1$ is not prescribed. The principal part of the operator in (15) is $\nabla^2(\nabla \times (\nabla \times))$, and the principal equation is

$$\nabla^2(\nabla \times (\nabla \times \underline{B})) = \nabla \times (\nabla \times (\nabla^2 \underline{B})) = \nabla \times (\nabla \times \underline{J}) = 0, \quad J = \nabla^2 \underline{B}. \tag{16}$$

An elementary Fourier treatment of (16), based on the expansion in a bounded cube, with $\underline{A}$ replaced by $\underline{J}$, yields conditions on the coefficients $d_{\ell\underline{n}}$, $e_{\ell\underline{n}}$ in a Fourier expansion for J_ℓ:

$$N_{\underline{n}}\underline{f}_{\underline{n}} = \begin{bmatrix} n_1^2 - n^2 & n_1 n_2 & n_1 n_3 \\ n_1 n_2 & n_2^2 - n^2 & n_2 n_3 \\ n_1 n_3 & n_2 n_3 & n_3^2 - n^2 \end{bmatrix} \begin{bmatrix} f_{1\underline{n}} \\ f_{2\underline{n}} \\ f_{3\underline{n}} \end{bmatrix} = 0 \tag{17}$$

where $n^2 = n_1^2 + n_2^2 + n_3^2$, and $\underline{f}_{\underline{n}}$ stands for $\underline{d}_{\underline{n}}$ or $\underline{e}_{\underline{n}}$. These Maxwell-type matrices $N_{\underline{n}}$ each of rank 2, have nice properties. If $n_j = 0$ for $j = 1$ or $j = 2$ or $j = 3$, but $\underline{n} \neq 0$, then $f_{jn} = 0$ and $\underline{n} \times \underline{f}_{\underline{n}} = 0$. If $n_j = n_k = 0$, then $f_{jn} = f_{kn} = 0$. If $n_1 n_2 n_3 \neq 0$, then the only constraint on $\underline{f}_{\underline{n}}$ is $\underline{n} \times \underline{f}_{\underline{n}} = 0$. The eigenvalues are $(0, -n^2, -n^2)$. These conditions are applicable to $\underline{f}_{\underline{n}} = \underline{d}_{\underline{n}}$ and $\underline{f}_{\underline{n}} = \underline{e}_{\underline{n}}$ independently, as the sine and cosine submodes of the solution are independent. Obviously finite Fourier series ($\underline{d}_{\underline{n}} = \underline{e}_{\underline{n}} = 0$ for $n_1 + n_2 + n_3 > N$) are possible. Thus,

$$\nabla^2 B_\ell(\underline{x}) = J_\ell(x) = d_{\ell,0} + \Sigma_{\underline{n}}[d_{\ell\underline{n}} \cos(2\pi(\underline{n} \cdot \underline{x})/L + e_{\ell\underline{n}} \sin(2\pi(\underline{n} \cdot \underline{x})/L)], \tag{18}$$

clearly Poisson equations forced by Fourier series. Because of linearity, the single mode complex equations $\nabla^2 \tilde{B}_{\ell\underline{n}}(x) = \tilde{f}_{\ell\underline{n}} e^{2\pi i(\underline{n}\cdot\underline{x})/L}$ can be solved for complex $\tilde{f}_{\ell n}$ and $\tilde{B}_{\ell n}$ over the region K as a Fourier series

$$\tilde{B}_{\ell\underline{n}}(\underline{x}) = \Sigma_{\underline{m}} \tilde{g}_{\ell\underline{n},\underline{m}} e^{2\pi i(\underline{m}\cdot\underline{x})/L}, \quad \text{where}$$

$$\tilde{g}_{\ell,\underline{n},\underline{n}} = -\frac{L^2}{4\pi^2 n^2} \tilde{f}_{\ell,n}, \quad \text{and} \quad \Sigma_{\underline{m}\neq\underline{n}} m^2 \tilde{g}_{\ell\underline{n},\underline{m}} = 0, \quad \ell = 1,2,3, \text{ all } \underline{n}. \tag{19}$$

Particular solutions are $\tilde{g}_{\ell\underline{n},\underline{m}} = 0$, $\underline{m} \neq \underline{n}$. So $B_\ell(x)$ are quadratics in $\underline{x}$ plus

$$\tilde{B}_{\ell,\underline{n}}(\underline{x}) = -\frac{L^2}{4\pi^2} \Sigma_{\underline{n}} \left[\frac{d_{\ell\underline{n}}}{n^2} \cos(2\pi(\underline{n} \cdot \underline{x})/L) + \frac{e_{\ell\underline{n}}}{n^2} \sin(2\pi(\underline{n} \cdot \underline{x})/L) \right]. \tag{20}$$

The solutions of the principal equation may be bounded and oscillatory.

Classification of (15) is difficult, because of the occurrence of $\nabla \times \underline{v}_1 = \nabla \times (\nabla \times \underline{A}_1)$ which prevents the time-independent parts of (15) or (13) from being strongly elliptic and so the entire

equation is not parabolic in the sense of Visik. Nevertheless it can be put in standard first order form, from which Taylor series can be constructed by routine methods.

The 54 distinct overt terms in (15), some appearing several times, include $\nabla_i A_{1j}$ (6), $\nabla_j \nabla_k A_{1k}$ (6), $\nabla_j^2 A_{1k}$ (6), $\nabla_i \nabla_j \nabla_k A_{1k}$ (6), $\nabla_i \nabla_j^2 A_{1k}$ (6), $\nabla_i^2 \nabla_j \nabla_k A_{1k}$ (18), and $\nabla_i^2 \nabla_j^2 A_{1k}$ (6). In addition, a minimum of 21 spatial bridging terms $\nabla_i \nabla_j \nabla_k A_{1\ell}$ are needed to reach the 24 fourth order terms (in one-derivative steps) from the 12 second order terms. From the six pure fourth order terms, three (i.e., $\nabla_1^4 A_{12}, \nabla_2^4 A_{13}, \nabla_3^4 A_{11}$) can be chosen to solve for in terms of the other $72 = 75 - 3$ derivative states via four 33×33 state matrices for the first level, unsteady case. These matrices are 98% sparse, and can be decomposed.

Equations of the type (15) are critical to this method, as they appear at every level, always the same size with increasingly complex entries, and generally forced, unlike (15).

4. Momentum Equations—Second Level

Collecting the h^{-2} terms in (3) from (4), (5), (6), (7), (9) leads to

$$(21) \qquad \begin{aligned}&(\nabla_t - 2r)\underline{v_1} - (\eta\nabla^2 h + s)\underline{v_1} + (\underline{v_1}\cdot\nabla)\underline{v_1} + \rho^{-1}(\nabla p_2 - p_1\nabla h)\\ &= -(\nabla\Omega_2 - \Omega_1\nabla h) + \eta[\nabla^2\underline{v_2} - 2(\nabla h\cdot\nabla)\underline{v_1} - \underline{v_1}\nabla^2 h]\end{aligned}$$

Cancelling $\eta\nabla^2 h\underline{v_1}$ from each side of (21) now yields

$$(22) \qquad (\nabla_t - \eta\nabla^2 - 2r)\underline{v_2} = \underline{s_2} + \underline{\sigma_2}, \quad \text{where}$$

$$(23) \qquad \begin{aligned}\underline{s_2} &= [s - 2\eta\nabla h\cdot\nabla - (\underline{v_1}\cdot\nabla)]\underline{v_1} + (\rho^{-1}p_1 + \Omega_1)\nabla h,\\ \nabla\cdot\underline{v_2} &= (v_1\cdot\nabla)h, \quad \underline{\sigma_2} = -\nabla(\rho^{-1}p_2 + \Omega_2)\end{aligned}$$

Application of $\nabla\cdot$ and $\nabla\times$ to (22) produces a Poisson equation for $\rho^{-1}p_2 + \Omega_2$ in terms of $\underline{v_2}$ and a forced vector reaction diffusion paravorticity equation.

The Poisson equation is evidently

$$(24) \qquad \nabla\cdot[(\nabla_t - \eta\nabla^2 - 2r)\underline{v_2}] + \nabla^2(\rho^{-1}p_2 + \Omega_2) = \nabla\cdot\underline{s_2}.$$

Expansion of $\underline{s_2}$ and the use of many previous identities (and much algebra) leads to

$$(25) \qquad \begin{aligned}\nabla^2(\rho^{-1}p_2 + \Omega_2) &= 2(\underline{v_2}\cdot\nabla)r + r(\underline{v_1}\cdot\nabla)h - 2\eta\Sigma_{i\le j}(\nabla_i\nabla_j h)(\nabla_j v_{1i} + \nabla_i v_{1j})\\ &\quad - \eta\Sigma_{i\le j}(\nabla_i v_{1j})(\nabla_j v_{1i}) + (\rho^{-1}p_1 + \Omega_1)(hr + s),\end{aligned}$$

with a simple dependence on $\underline{v_2}$. Thus p_2 depends on $\underline{v_2}$, $\underline{v_1}$, h, r, s, and p_1. As for $\underline{v_2}$,

$$(26) \qquad \nabla\times[(\nabla_t - \eta\nabla^2 - 2r)\underline{v_2}] = \nabla\times\underline{s_2}, \quad \nabla\cdot\underline{v_2} = (\underline{v_1}\cdot\nabla)h$$

Now $\nabla\times\underline{s_2}$ depends only on $\underline{v_1}$, h, r, s, and p_1, and like $\nabla\cdot\underline{s_2}$ (expanded in (25)) can be expanded in the v_{1j}. Since

$$\nabla\times[(\rho^{-1}p_1 + \Omega_1)\nabla h] = \nabla(\rho^{-1}p_1 + \Omega_1)\times\nabla h,$$

p_1 can be eliminated from $\nabla\times\underline{s_2}$ in favor of $\underline{v_1}$ by using (11), giving $\underline{v_2}$ in terms of $\underline{v_1}$, by a finite but long formula.

As mentioned earlier, the series for $\underline{u}$ cannot generally stop at the first level, but can stop after two levels, although series which stop after three levels are more interesting.

5. Momentum Equations—Level Three and Beyond

The third and higher (or deeper) levels are considered together, because no new types of terms are needed, although the length of the memory tail increases linearly with the level m, but its nature remains linear-bilinear. Suppose that levels, $1,2,\ldots,m-1$ are complete for $\underline{A}_1,\underline{A}_2,\ldots\underline{A}_{m-1}$; or $\underline{v}_1,\underline{v}_2,\ldots,\underline{v}_{m-1}$, and $\rho^{-1}p_1+\Omega_1,\ldots,\rho^{-1}p_{m-1}+\Omega_{m-1}$. After collecting the coefficients of h^{-m}, the mth level equation for $\underline{v}_m$ is

$$(27)\quad \nabla_t\underline{v}_m - mr\underline{v}_m - (\eta\nabla^2 h+s)(m-1)\underline{v}_{m-1}+\Sigma_{\ell=1}^{m-1}(\underline{v}_\ell\cdot\nabla)\underline{v}_{m-\ell}$$
$$-\Sigma_{\ell=1}^{m-2}(m-\ell-1)\underline{v}_{m-\ell-1}(\underline{v}_\ell\cdot\nabla)h=-\nabla(\rho^{-1}p_m+\Omega_m)+(m-1)(\rho^{-1}p_{m-1}+\Omega_{m-1})\nabla h$$
$$+\eta[\nabla^2\underline{v}_m-2(m-1)(\nabla h\cdot\nabla)\underline{v}_{m-1}-(m-1)\underline{v}_{m-1}\nabla^2 h+(m-1)(m-2)\underline{v}_{m-2}(\nabla h)^2].$$

Cancellation of $(m-1)\eta\underline{v}_{m-1}\nabla^2 h$ from both sides of (27), yields

$$(28)\quad (\nabla_t-\eta\nabla^2-mr)\underline{v}_m=\underline{s}_m+\underline{\sigma}_m,\quad \text{where}$$

$$(29)\quad \underline{s}_m=(m-1)s\underline{v}_{m-1}-\Sigma_{\ell=1}^{m-1}(\underline{v}_\ell\cdot\nabla)\underline{v}_{m-\ell}+\Sigma_{\ell=1}^{m-2}(m-\ell-1)\underline{v}_{m-\ell-1}(\underline{v}_\ell\cdot\nabla)h$$
$$+(m-1)(\rho^{-1}p_{m-1}+\Omega_{m-1})\nabla h+\eta(m-1)[-2(\nabla h\cdot\nabla)\underline{v}_{m-1}+(m-2)\underline{v}_{m-2}(\nabla h)^2]$$

$$(30)\quad \underline{\sigma}_m=-\nabla(\rho^{-1}p_m+\Omega_m),\quad \nabla\cdot\underline{v}_m=(m-1)(\underline{v}_{m-1}\cdot\nabla)h.$$

Application of $\nabla\times$ to (28) yields a forced vector-reaction diffusion equation for $\nabla\times\underline{v}_m$, and application of $\nabla\cdot$ to (28) produces

$$(31)\quad \nabla\cdot[(\nabla_t-\eta\nabla^2-mr)\underline{v}_m]=\nabla\cdot\underline{s}_m-\nabla^2(\rho^{-1}p_m+\Omega_m).$$

As in Section 4, $\nabla\cdot\underline{s}_m$ can be manipulated and so finally yields parapressure p_m:

$$(32)\quad (\nabla_t-\eta\nabla^2)(m-1)(\underline{v}_{m-1}\cdot\nabla)h-m(\nabla r)\cdot\underline{v}_m-m(m-1)[(\underline{v}_{m-1}\cdot\nabla)h]r$$
$$=\nabla\cdot\{(m-1)s\underline{v}_{m-1}-2(m-1)\eta(\nabla h\cdot\nabla)\underline{v}_{m-1}+\eta(m-1)(m-2)\underline{v}_{m-2}(\nabla h)^2$$
$$-\Sigma_{\ell=1}^{m-1}(\underline{v}_\ell\cdot\nabla)(\underline{v}_{m-\ell}+\Sigma_{\ell=1}^{m-2}(m-\ell-1)\underline{v}_{m-\ell-1}(\underline{v}_\ell\cdot\nabla)h$$
$$+(m-1)(\rho^{-1}p_{m-1}+\Omega_{m-1})\nabla h\}-\nabla^2(\rho^{-1}p_m+\Omega_m).$$

Note that $\underline{v}_m$ enters only one term in (27), the rest depending only on $\underline{v}_1,\ldots,\underline{v}_{m-1},m,r,h,s$ and $\rho^{-1}p_{m-1}+\Omega_{m-1}$. If $\nabla r=0$, even the $\underline{v}_m$ dependence is absent. As before, $\rho^{-1}p_m+\Omega_m$ can be obtained by a Poisson integral of the remaining terms in (32).

The equation for $\underline{v}_m$ itself is

$$(33)\quad \nabla\times[(\nabla_t-\eta^2-mr)\underline{v}_m]=\nabla\times\underline{s}_m,$$

where $\underline{s}_m$ is defined in (29), which can be solved by the anti-vorticity methods mentioned in sections 3 and 4, and is an equation of the same type as (26). As to termination, if $\underline{v}_m=0$, then $\nabla\times\underline{s}_m=0$, which is a complicated identity relating $\underline{v}_1,\underline{v}_2,\ldots\underline{v}_{m-1}$. Also $\underline{s}_m=-\underline{\sigma}_m=\nabla(\rho^{-1}p_m+\Omega_m)$, from (33). It is logical to set $\rho^{-1}p_m+\Omega_m=$ const to assist in the termination, so $\underline{s}_m=0$, yielding a less complicated relation between the various levels involved, than that obtained from $\nabla\times\underline{s}_m=0$.

For example, if $m = 3$, termination involves the linear first-order system, depending on $\underline{v_1}, h, \rho^{-1}p_2 + \Omega_2$:

$$2s\underline{v_2} - [(\underline{v_1}\cdot\nabla)\underline{v_2} + (\underline{v_2}\cdot\nabla)\underline{v_1}] + \underline{v_1}(\underline{v_1}\cdot\nabla)h + 2(\rho^{-1}p_2 + \Omega_2)\nabla h + 2\eta[-2(\nabla h\cdot\nabla)\underline{v_2} + \underline{v_1}(\nabla h)^2] = 0 \tag{34}$$

This is a first order PDE system for $\underline{v_2}$. However, note that

$$\nabla^2(\rho^{-1}p_2 + \Omega_2) = \nabla\cdot\underline{s_2} - (\nabla_t - \eta\nabla^2)\nabla\cdot\underline{v_2} + 2\nabla\cdot(r\underline{v_2}) \tag{35}$$

also depends linearly on $\underline{v_2}$ and $\nabla\cdot\underline{v_2} = (\underline{v_1}\cdot\nabla)h$, so $\rho^{-1}p_2 + \Omega_2$ can be written as the output of a linear integral operator on $\underline{v_2}$, and all dependence on $\underline{v_2}$, except for $2(\underline{v_2}\cdot\nabla)r$, can be eliminated from the right side of (35). Thus $\underline{v_2}$ can be determined from $\underline{v_1}$ and p_1 in such a way that $\underline{v_3}$ and all later paravelocity terms are zero. Termination conditions for $\underline{v}_{N+1} = \underline{v}_{N+2}\cdots = 0$ are similarly available, though increasingly tedious. Not only has the determination of $\underline{v_m}$ and p_m been reduced to the solution of *exactly* linear differential equations, but also the discovery of terminating velocity series can be so reduced, without recourse to (post-1900) global functional analysis or numerical computation.

REFERENCES

1. J. D. Cole, *On a quasi-linear parabolic equation*, Quart. Jour. Appl. Math. 9 (1951), 225–236.
2. C. R. Doering and J. D. Gibbon, *Applied Analysis of the Navier-Stokes Equations*, Cambridge U.P., Cambridge, U.K., 1995.
3. E. Hopf, *The partial differential equation* $u_t + uu_x = \mu u_{xx}$, Comm. Pure Appl. Mech. 3 (1950), 201–230.
4. O. A. Ladyzhenskaya, *On non-stationary operational equations*, Mat. Sbornik 95:2, 123–158.
5. O. A. Ladyzhenskaya, *The Boundary-Value Problems of Mathematical Physics*, Ch. III, Ch. V, §2, Springer-Verlag, 1985.

Department of Mathematics, University of California, Santa Barbara, CA 93106

Received August 22, 1996
in revised form October 7, 1996

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

ON SET-VALUED FUNCTIONS OF CONVEX TYPE

Elżbieta Sadowska

Presented by J.D. Aczel, F.R.S.C.

Abstract

Let K be a convex cone in $\mathbb{R}^n$, T be a positive constant and W(T) be the class of set-valued functions $F : K \to n(\mathbb{R}^m)$ satisfying (1). It is shown that if $0 < T_1 < T_2 < 1$ or $1 < T_2 < T_1$ then $W(T_2) \subset W(T_1)$. Moreover, if $F \in W(T)$ for some $T > 1$ and $0 \in F(0)$, then $rF(x) = F(rx)$ for all $x \in K$ and $r \in (0, \infty)$.

In [1] J.Matkowski and K.Nikodem presented relations between the classes of real functions defined on the half line and satisfying

$$f(tx + (T-t)y) \leq tf(x) + (T-t)f(y)\ ,\ x, y \in \mathbb{R}_+,\ t \in [0, T],$$

for a fixed $T > 0$. They also gave the form of the solutions of the above inequality for $T > 1$ under the assumption that $f(0) = 0$.

In this paper we present counterparts of those results for set-valued functions.

In the whole paper we will assume, that $K \subset \mathbb{R}^n$ is a convex cone and that F and Φ are set-valued functions from K into nonempty subsets of $\mathbb{R}^m$. Moreover insted of "set-valued function" we will write "s.v. function".

For a given $T > 0$ we will consider the class of s.v. functions satisfying

$$\sum_{i=1}^{n+m+1} t_i F(x_i) \subset F\left(\sum_{i=1}^{n+m+1} t_i x_i\right) \tag{1}$$

for every $x_1, \ldots, x_{n+m+1} \in K$ and all $t_1, \ldots, t_{n+m+1} \in [0, T]$ summing up to T (the sum on the left hand side means the algebraic sum of sets). Let us denote

$$W(T) = \{F : K \to n(\mathbb{R}^m)\ :\ F \textit{ satisfies the condition } (1)\}.$$

Recall that an s.v. function $F : K \to n(\mathbb{R}^m)$ is said to be *convex* if

$$tF(x) + (1-t)F(y) \subset F(tx + (1-t)y),\ \ x, y \in K,\ t \in [0, 1].$$

1991 Mathematics Subject Classification: 26A51,26B25,54C60. Key words and phrases: set valued functions, convex set- valued functions, sadwich theorem.

Thus (cf [2, Theorem 2.3]) $W(1)$ coincides with the family of all convex s.v. functions on K.

Lemma 1 *An s.v. function F belongs to $W(T)$ if and only if there exists a convex s.v. function $\Phi : K \to n(\mathbb{R}^m)$ such that*

$$\Phi(x) \subset F(x) \subset T^{-1}\Phi(Tx), \quad x \in K. \tag{2}$$

Proof: Let $t_i = T\alpha_i$, $\alpha_i \in [0,1]$, for i=1,2,...,n+m+1. Using (1) we obtain

$$\sum_{i=1}^{n+m+1} \alpha_i F(x_i) \subset T^{-1}F\left(T\sum_{i=1}^{n+m+1} \alpha_i x_i\right), \quad x_1,...,x_{n+m+1} \in K.$$

By [3, Theorem 1.1 and Remark 2] there exists a convex s.v. function $H : K \to n(\mathbb{R}^m)$ such that

$$F(x) \subset H(x) \subset T^{-1}F(Tx), \quad x \in K.$$

Putting $\Phi(x) := TH(T^{-1}x)$, for $x \in K$, we can easly check that Φ satisfies condition (2).

The converse implication is obvious.

■

Now we will present two lemmas on convex s.v. functions Φ for which

$$\Phi(x) \subset T^{-1}\Phi(Tx), \quad x \in K, \tag{3}$$

holds for some $T > 0$.

Lemma 2 *If an s.v. function Φ is convex and satisfies condition (3) with a $T > 1$, then*

$$\forall\, T_1, T_2 \in (0,\infty) \quad 0 < T_1 < T_2 \Rightarrow \frac{\Phi(T_1 x)}{T_1} \subset \frac{\Phi(T_2 x)}{T_2}, \quad x \in K.$$

Proof: Let us take T_1 and T_2 such that $0 < T_1 < T_2$. Because $T > 1$, there exists a $k \in \mathbb{N}$ for which $T^k T_1 > T_2$. Hence there exists an $\alpha \in (0,1)$ such that

$$T_2 = \alpha T_1 + (1-\alpha)T_1 T^k. \tag{4}$$

By the convexity of Φ, we get

$$\Phi(T_2 x) \supset \alpha\Phi(T_1 x) + (1-\alpha)\Phi\left(T_1 T^k x\right), \quad x \in K.$$

From (3) it follows that

$$\Phi(x) \subset T^{-k}\Phi(T^k x), \quad x \in K.$$

Hence

$$\Phi(T_2 x) \supset \alpha\Phi(T_1 x) + (1-\alpha)T^k\Phi(T_1 x), \quad x \in K.$$

Because Φ is convex its values are also convex, so we can rewrite this inclusion in the form

$$\Phi(T_2 x) \supset \left(\alpha + (1-\alpha)T^k\right)\Phi(T_1 x), \quad x \in K.$$

Finally, using equality (4) we get the assertion of the lemma.

■

Lemma 3 *If an s.v. function Φ is convex and satisfies condition (3) for a $T \in (0,1)$, then*

$$\forall\ T_1, T_2 (0,\infty) \quad 0 < T_1 < T_2 \Rightarrow \frac{\Phi(T_1 x)}{T_1} \supset \frac{\Phi(T_2 x)}{T_2}, \ x \in K.$$

Proof: The proof of this lemma is similar to the above one. For $0 < T_1 < T_2$ we choose such $k \in \mathbb{N}$ for which $T^k T_2 < T_1$. There also exists an $\alpha \in (0,1)$ such that $T_1 = \alpha T_2 T^k + (1-\alpha)T_2$. And now arguing like in the previous proof we obtain the desired inclusion.

■

Theorem 1

(*i*) *If* $1 < T_1 < T_2$ *then* $W(T_1) \subset W(T_2)$,

(*ii*) *If* $0 < T_1 < T_2 < 1$ *then* $W(T_1) \supset W(T_2)$.

Proof: (*i*) Let $F \in W(T_1)$. By Lemma 1 there exists a convex s.v. function Φ such that condition (2) holds for $T = T_1$; by Lemma 2 it holds for $T = T_2$, too. This means that $F \in W(T_2)$.

The part (*ii*) can be proved in the some way by use of Lemmas 1 and 3.

■

Notice that the class W(1) is not included in any class W(T) where $T \neq 1$. For example a function $F : [0,\infty) \to n(\mathbb{R})$, defined by $F(x) = \{1\}$, belongs to W(1) but does not belong to W(T) for any $T \neq 1$.

Now we will assume, that K is a convex cone with zero and for a given $T > 1$ we will present the form of s.v. functions F belonging to the class $W(T)$ and such that $0 \in F(0)$.

Lemma 4 *Let $K \subset \mathbb{R}^n$ be a convex cone with zero. If an s.v. function $\Phi : K \to n(\mathbb{R}^m)$ is convex and such that $0 \in \Phi(0)$, then*

$$\forall\, x \in K \quad \forall\, T_1, T_2 \in (0,\infty) \quad 0 < T_1 < T_2 \Rightarrow \frac{\Phi(T_1 x)}{T_1} \supset \frac{\Phi(T_2 x)}{T_2}.$$

Proof: Because $0 \in \Phi(0)$ and Φ is convex, we get the following inlusions

$$\alpha\Phi(x) \subset \alpha\Phi(x) + (1-\alpha)\Phi(0) \subset \Phi(\alpha x), \quad \alpha \in [0,1], \; x \in K. \tag{5}$$

For T_1, T_2 satisfying $0 < T_1 < T_2$ there exists an $\alpha \in (0,1)$ such that $T_1 = \alpha T_2$. Using these two facts we obtain

$$T_2^{-1}\Phi(T_2 x) \subset \frac{\Phi(\alpha T_2 x)}{\alpha T_2} = T_1^{-1}\Phi(T_1 x), \; x \in K.$$

which was to be shown. ∎

Theorem 2 *Let $K \subset \mathbb{R}^n$ be a convex cone with zero. If an s.v. function $F : K \to n(\mathbb{R}^m)$ belongs to the class $W(T)$ for some $T > 1$ and $0 \in F(0)$, then F is convex and*

$$\forall\, r \in (0,\infty) \quad \forall\, x \in K \quad rF(x) = F(rx). \tag{6}$$

Proof: Because $F \in W(T)$, by Lemma 1 there exists a convex s.v. function Φ satisfying condition (2); in particular, $0 \in \Phi(0)$. Using Lemma 4 for $T_1 = 1$ and $T_2 = T$ we obtain

$$T^{-1}\Phi(Tx) \subset \Phi(x), \quad x \in K,$$

which together with (2) gives

$$T^{-1}\Phi(Tx) = \Phi(x), \quad x \in K. \tag{7}$$

Applying (2) and (7) we get

$$\Phi(x) \subset F(x) \subset T^{-1}\Phi(Tx) = \Phi(x), \quad x \in K,$$

This means that

$$F(x) = \Phi(x), \quad x \in K, \tag{8}$$

and so, F is convex.

Now we are going to prove the condition (6). By (8) and (5) we have $rF(x) \subset F(rx)$ for $r \in [0,1]$. Let us take an $r > 1$. We can find a $k \in \mathbb{N}$ such that $0 < \frac{r}{T^k} < 1$. Using (5), (3) and (7) we get

$$\frac{r}{T^k}F(x) \subset F\left(\frac{r}{T^k}x\right) = \frac{F(rx)}{T^k}, \quad x \in K,$$

i.e. $rF(x) \subset F(rx)$ for $x \geq 1$. Thus for all $r \in (0,\infty)$ we have the inclusion $rF(x) \subset F(rx)$. The converse inclusion we obtain multiplying the following one by r

$$\frac{1}{r}F(rx) \subset F\left(\frac{1}{r}rx\right) = F(x), \quad for \ \ r \in (0,\infty).$$

■

Corollary 1 *Let $K = [0.\infty)$ and assume that an s.v. function $F : K \to n(\mathbb{R}^m)$ belongs to the class $W(T)$ for some $T > 1$. If $0 \in F(0)$, then there exists a convex set $A \subset \mathbb{R}^m$ such that*

$$F(x) = xA, \quad x \in (0,\infty). \tag{9}$$

Proof: Using Theorem 2 for $x = 1$ we obtain

$$rF(1) = F(r), \quad r \in (0,\infty),$$

i.e. (9) holds with $A = F(1)$. By the convexity of F, the set A is convex, which finishes the proof.

■

Notice that the s.v. function $F : [0,\infty) \to \mathbb{R}$, $F(x) = [0,\infty)$, $x \in [0,\infty)$, belongs to the class W(T) and $0 in F(0)$, but it does not satisfy the condition (9) for $x = 0$.

Remark 1 For an arbitrary convex cone $K \subset \mathbb{R}^n$ with zero, if $F \in W(T)$ for some $T > 1$ and $0 \in F(0)$ then F is subadditive.

Indeed, by the positive homogeneity and the convexity of F we obtain

$$F(x) + F(y) = F\left(\alpha\frac{x}{\alpha}\right) + F\left((1-\alpha)\frac{y}{1-\alpha}\right) =$$

$$= \alpha F\left(\frac{x}{\alpha}\right) + (1-\alpha)F\left(\frac{y}{1-\alpha}\right) \subset F(x+y), \quad x,y \in K.$$

The following example shows that under the assumptions of Theorem 2 the s.v. function F need not to be additive.

Example 1 Let $K = [0,\infty) \times [0,\infty)$ and $F : K \to n(\mathbb{R})$ be defined by the formula

$$F(x,y) = [0, min\{x,y\}], \quad (x,y) \in K.$$

It is easy to check that F is convex and satisfies $2F(x,y) = F(2x,2y)$. So it satisfies the condition (2) with $\Phi = F$ and $T = 2$; so by Lemma 1, $F \in W(2)$. However F is not additive. For instance $F(2,0) + F(0,2) = \{0\}$ and $F((2,0) + (0,2)) = [0,2]$.

Remark 2 The theorems presented above remain true if (see [3, Theorem 1.1 and Remark 2]) in the definition of the classes $W(T)$ we assume that F satisfies (instead of (1)) the following condition

$$\sum_{i=1}^{n+m} t_i F(x_i) \subset F\left(\sum_{i=1}^{n+m} t_i x_i\right),$$

for all $x_1, ..., x_{n+m} \in K$ and all $t_1, ..., t_{n+m} \in [0,T]$ summing up to T and, moreover, that the graph of F is the union of n+m connected subsets of $\mathbb{R}^{n+m}$. In the same way as in the proof of Lemma 1 we can show (using [3, Theorem 1.1]) that also in this case $F \in W(T)$ if and only if there exists a convex s.v. function $\Phi : K \to n(\mathbb{R}^m)$ such that condition (2) holds.

References

[1] **J.MATKOWSKI, K.NIKODEM** : Solutions of some functional inequalities connected with convex functions , *C. R. Math. Rep. Acad. Sci.* Canada 15(3)(1993), 114-118.

[2] **K.NIKODEM:** K-convex and K-concave set-valued functions, *Zeszyty Naukowe Politechniki Lódzkiej* 559 (*Rozprawy Mat.* 114), Lódź 1989.

[3] **E.SADOWSKA:** A sandwich with convexity for set-valued functions , *Mathematica Pannonica* 7/1 (1996), 163-169.

[4] **F.A.VALENTINE:** Convex Sets, McGraw-Hill Book Company, 1969.

Received March 19, 1996

in revised form October 8, 1996

Katedra Matematyki
Politechnika Lódzka
Filia w Bielsku-Białej
ul. Willowa 2
PL-43-309 Bielsko-Biała
Ploland
e-mail: LK@merc.pb.bielsko.pl

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

THE SQUARE CLASSES IN LUCAS SEQUENCES WITH ODD PARAMETERS

Paulo Ribenboim, F.R.S.C and Wayne L. McDaniel.

Abstract. For all odd relatively prime parameters P and Q, $P^2 - 4Q > 0$, we show that the square classes of the Lucas sequences $\{U_n(P, Q)\}$ and $\{V_n(P, Q)\}$ contain at most 3 elements, and explicitly determine those square classes, except for the classes $\{U_m, U_{3m}\}$ and $\{V_m, V_{3m}\}$; in the exceptional case, we prove that there exists an effectively computable constant C such that $m < C$.

1. INTRODUCTION

Let P and Q be non–zero integers, and α and β $(\beta < \alpha)$ be the roots of $X^2 - PX + Q = 0$. The Lucas sequence $\{U_n\}$ and "associated Lucas sequence" $\{V_n\}$ are defined, for $n \geq 0$, by $U_n = U_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, and $V_n = V_n(P, Q) = \alpha^n + \beta^n$, respectively. If there exist non–zero integers x and y such that $x^2 U_m = y^2 U_n$, or equivalently, $U_m U_n = \square$, then we say that U_m and U_n are in the same square class (resp. $V_m V_n$).

Our purpose, here, is to report that for P and Q odd, $\gcd(P, Q) = 1$ and $P^2 - 4Q > 0$, we have explicitly determined all integers m and n, $0 \leq m < n$, $n \neq 3m$ such that $U_m U_n = \square$ and $V_m V_n = \square$; if $n = 3m$, $m > 1$, we have shown that there exists an effectively computable constant C such that if $U_m U_{3m} = \square$ (or $V_m V_{3m} = \square$), then $m < C$. In adddition, we have shown that with a slightly stronger hypothesis, no additional square classes occur when $n = 3m$. In either event, each non–trivial square class of $\{U_n\}$ contains at most 3 elements and each non–trivial square class of $\{V_n\}$ contains at most 2 elements.

2. THE THEOREMS.

We assume that P and Q are odd, $\gcd(P, Q) = 1$ and $P^2 - 4Q > 0$. In addition, we assume, for convenience, that $P > 0$; the results hold for $P < 0$, as well, since $U(P, Q)$ and $U(-P, Q)$ (resp. $V(P, Q)$) differ only in the sign of alternate terms.

THEOREM 1.

(a) If, for $1 \leq m < n$, $U_m U_n = 0$, then $(m, n) = (1, 2), (1, 3), (1, 6), (1, 12), (2, 3), (2, 12), (3, 6)$ or $(5, 10)$, or $n = 3m$, $m > 1$, m odd.

(b1) $U_1 U_n = 0$ iff $U_n = 0$ (see [10]).

(b2) $U_2 U_3 = 0$ iff $P = 0$ and $P^2 - Q = 0$; if $U_2 U_3 = 0$, then $Q \equiv 1 \pmod 4$.

(b3) $U_3 U_6 = 0$ iff $P = 0$ and $P^2 - 3Q = 0$, or $P = 3\square$ and $P^2 - 3Q = 3\square$; if $U_3 U_6 = 0$, then $Q \equiv 3 \pmod 4$.

(b4) $U_5 U_{10} = 0$ iff $P = 5\square$ and $P^4 - 5P^2Q + 5Q^2 = 5\square$; if $U_5 U_{10} = 0$, then $P \equiv Q \equiv 5 \pmod 8$.

(b5) $U_2 U_{12} = 0$ iff $P = 0$, $P^2 - 3Q = 0$, $P^2 - Q = 2\square$, $P^2 - 2Q = 3\square$ and $(P^2 - 2Q)^2 - 3Q^2 = 6\square$; if $U_2 U_{12} = 0$, then $Q \equiv 3 \pmod 4$.

(c1) If $m > 1$ and $U_m U_{3m} = 0$, then m is odd, $3 \nmid m$, $Q \equiv 1 \pmod 4$ and $(-Q|P) = +1$.

(c2) If $m > 1$ and Q are given, and $U_m U_{3m} = 0$, then P is bounded; specifically, $P < |Q + 1|$.

(c3) If $m > 1$ and P are given, and $U_m U_{3m} = 0$, then there exists an effectively computable constant $C > 0$ such that $Q < C$.

(c4) If P and Q are given, and $U_m U_{3m} = 0$, then there exists an effectively computable constant $C > 0$ such that $m < C$.

COROLLARY 1. A square class C of $\{U_n\}$ is non–trivial only if

(1) $C = \{U_1, U_2, U_3\}$ or $\{U_5, U_{10}\}$ when $Q \equiv P \equiv 1 \pmod 4$,

(2) $C = \{U_1, U_3, U_6\}$ when $Q \equiv 1 \pmod 4$ and $P \equiv 3 \pmod 4$,

(3) $C = \{U_1, U_2, U_{12}\}$ or $\{U_3, U_6\}$ when $Q \equiv 3 \pmod 4$, or

(4) $C = \{U_m, U_{3m}\}$, $m > 1$, m odd, $3 \nmid m$, $P < |Q + 1|$, $Q \equiv 1 \pmod 4$, and $(-Q|P) = +1$, for at most a finite set of values of m.

THEOREM 2.

(a) If, for $0 \leq m < n$, $V_m V_n = \square$ then $(m, n) = (0, 3)$ or $(0, 6)$, or $n = 3m$, $m \geq 1$, m odd.

(b1) $V_0 V_3 = \square$ iff $P = 3\square$ and $P^2 - 3Q = 6\square$. If $V_0 V_3 = \square$, then $Q \equiv 1$ or $3 \pmod 8$ and $P \equiv 3 \pmod{24}$.

(b2) $V_0 V_6 = \square$ iff $P^2 - 2Q = 3\square$ and $(P^2 - 2Q)^2 - 3Q^2 = 6\square$. If $V_0 V_6 = \square$, then $Q \equiv 3 \pmod 4$.

(b3) $V_1 V_3 = \square$ iff $P^2 - 3Q = \square$. If $V_1 V_3 = \square$, then $Q \equiv 3 \pmod 8$ and $3 \nmid P$.

(c1) If $m > 1$ and $V_m V_{3m} = \square$, then m is odd, $3 \nmid m$, $Q \equiv 3 \pmod 4$, $3 \nmid P$ and $(-3Q|P) = +1$.

(c2) If $m > 1$ and Q are given, and $V_m V_{3m} = \square$, then P is bounded; specifically, $P < |Q/k + k|$ for $k = \sqrt[5]{0.6} \approx 0.90$.

(c3) If P and Q are given, and $V_m V_{3m} = \square$, then there exists an effectively computable constant $C > 0$ such that $m < C$.

COROLLARY 2. A square class C of $\{V_n\}$ is non–trivial only if

(1) $C = \{V_0, V_3\}$ when $Q \equiv 1$ or $3 \pmod 8$, $3 | P$,

(2) $C = \{V_1, V_3\}$ when $Q \equiv 3 \pmod 8$, $3 \nmid P$,

(3) $C = \{V_0, V_6\}$ when $Q \equiv 3 \pmod 4$, or

(4) $C = \{V_m, V_{3m}\}$, $m > 1$, m odd, $3 \nmid m$, $P < |Q/k + k|$ for $k = \sqrt[5]{0.6}$, $Q \equiv 3 \pmod 4$, and $(-3Q|P) = +1$, for at most a finite set of values of m.

3. THE PROOFS.

Essential to our proofs are the results of [5], [10] and [11]; as in those papers, extensive use of the Jacobi symbol is made. The proof that there exist only a finite number of values of m such that $\{U_m, U_{3m}\}$ (or $\{V_m, V_{3m}\}$) is a square class requires a result proven by Schinzel & Tijdeman [12].

The details of the proofs are contained in [6].

4. COMMENTS ON PREVIOUS RESULTS.

The square classes in Lucas sequences have been previously determined in certain special cases. When $P = 1$ and $Q = -1$, $\{U_n\} = \{F_n\}$ and $\{V_n\} = \{L_n\}$ are the familiar sequences of Fibonacci and Lucas numbers, respectively; Cohn found the square classes containing F_1 (i. e., the class of all squares in $\{F_n\}$) in 1963 [1], and in 1966 through 1972 [2], [3], [4], found all square classes for $\{U_n\}$ and $\{V_n\}$ when $Q = \pm 1$ and P is odd or has certain even values. For an alternate determination of the square classes for $\{F_n\}$ and $\{L_n\}$, see [7]. More recently, Ribenboim and McDaniel found all square classes in $\{U_n(P, Q)\}$ containing $U_1(P, Q)$ for P and Q odd, $\gcd(P, Q) = 1$, $P^2 - 4Q > 0$ [10]. If $P = Q + 1 > 0$, Ribenboim [8] determined the square–classes, for all non–negative Q, of U_n and, when Q is even, of V_n. See, also, [9], for a related result.

REFERENCES

[1] J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* 39 (1964), 537–541.

[2] J. H. E. Cohn, Eight diophantine equations, *Proc. London Math. Soc.* (3) 16 (1966), 153–166.

[3] J. H. E. Cohn, Five diophantine equations, *Math. Scand.* 21 (1967), 61–70.

[4] J. H. E. Cohn, Squares in some recurrent sequences, *Pacific J. Math.* (3) 41 (1972), 631–646.

[5] W. L. McDaniel, Square Lehmer numbers, *Colloquium Mathematicum* (66) (1993), 85–93.

[6] W. L. McDaniel and P. Ribenboim, Square classes in Lucas sequences having odd parameters, (preprint).

[7] P. Ribenboim, Square classes of Fibonacci and Lucas numbers. *Port. Math.* 46 (1989), 159–175.

[8] P. Ribenboim, Square classes of $\frac{a^n - 1}{a - 1}$ and $a^n + 1$, *J. Szechuan Univ.* 26 (1989), 196–199.

[9] P. Ribenboim and W. L. McDaniel, Square classes of Lucas sequences, *Port. Math.* 48 (1991), 469–473.

[10] P. Ribenboim and W. L. McDaniel, The square terms in Lucas sequences, *J. of Number Theory* 58 (1996), 104–122.

[11] A. Rotkiewicz. Applications of Jacobi's symbol to Lehmer's numbers, *Acta Arithmetica* 42 (1983), 163–187.

[12] A. Schinzel and R. Tijdeman, on the equation $y^m = P(x)$, *Acta Arithmetica* 31 (1976): 199–204.

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

Received November 8, 1996

Department of Mathematics and Computer Science
University of Missouri–St. Louis
St. Louis, Missouri 63121
U. S. A.

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

Théorie des Nombres

Sur l'équation $x^p - y^q = 1$ lorsque $p \equiv 5 \bmod 8$

Maurice Mignotte, Strasbourg

Presented by C.L. Stewart, F.R.S.C.

Résumé .— Nous considérons l'équation de Catalan $x^p - y^q = 1$ (avec p, q premiers et $|x|, |y| > 1$). Lorsque $p \equiv 5 \bmod 8$, nous obtenons une majoration de q en fonction de p qui est meilleure que celle connue dans le cas général.

On the equation $x^p - y^q = 1$ when $p \equiv 5 \bmod 8$

Abstract .— We consider Catalan's equation $x^p - y^q = 1$ (with p, q prime and $|x|, |y| > 1$). When $p \equiv 5 \bmod 8$, we prove an upper bound on q in terms of p which is better than the general one.

1. Introduction

En 1843, E. Catalan a posé le problème suivant: existe-t-il des entiers consécutifs autres que 8 et 9 qui soient tous deux des puissances parfaites? Cette question revient à considérer "l'équation de Catalan"

$$x^p - y^q = 1, \qquad \text{avec } p, q \text{ premiers et } |x|, |y| > 1. \tag{1}$$

En 1976, R. Tijdeman [T] a montré que l'équation de Catalan ne possède qu'un nombre fini de solutions non triviales (p, q, x, y). La même année, M. Langevin [La] a obtenu la borne $\max\{p, q\} < 10^{110}$, *cf.* [S-T].

Le résultat de Tijdeman est obtenu en considérant deux formes linéaires de logarithmes et en appliquant des minorations de telles formes. En 1960, Cassels [C] a montré que pour l'équation (1) l'entier x est divisible par q et l'entier y divisible par p; ce résultat implique des relations de la forme $x - 1 = u^q/p$ et $y + 1 = v^p/q$, où u et v sont des entiers, $|u|, |v| > 1$. On considère alors les "formes linéaires"

$$\Lambda_1 = \left| q \log \left| yu^{-p} \right| + p \log p \right|$$

et

$$\Lambda_2 = \left| pq \log |u/v| - p \log p + q \log q \right|.$$

On en déduit respectivement des majorations du type

$$q < C_1 p (\log q)^2 \log p \tag{2}$$

et

$$p < C_2 (\log q)^3. \tag{3}$$

Dans le présent travail, nous supposons $q > p$ et nous nous intéresserons exclusivement aux majorations de q en fonction de p, donc du type (2).

En utilisant les résultats de [L-M-N], le meilleur résultat de la forme (2) est actuellement le suivant (*cf.* [M-R1], relation (2.14))

$$(2') \qquad q < 2.77\, p\,(\log(q/\log p) + 2.333)^2 \log p, \qquad \text{pour } p > 3000.$$

Dans le cas particulier où $p \equiv 3 \pmod 4$, toujours grâce à [L-M-N], en considérant une forme linéaire nouvelle, on a mieux:

$$(2'') \qquad q \leq 4.51\, p \max\{3.46 + \log q, 17\}^2,$$

résultat lui aussi démontré dans [M-R1]. Dans le cas particulier $p \equiv 5 \pmod 8$, on peut encore améliorer un peu la relation (2'), c'est l'objet de la présente note.

Notons que la démonstration de la majoration (2') repose sur la construction d'une forme linéaire de logarithmes qui résulte de la démonstration du premier critère d'Inkeri, [I1]. C'est une démarche semblable que nous suivrons ici, à la différence près que nous utilisons cette fois la démonstration du critère publié en [M], elle-même inspirée de celle du second critère d'Inkeri, [I2].

Pour le lecteur intéressé, signalons qu'une étude complète de l'équation de Catalan (jusqu'en 1992) est l'objet du livre de P. Ribenboim [R]. Notons simplement que d'après les travaux de Lebesgue [Le], Nagell [Na] et Ko Chao [K] on peut supposer $p \geq 5$.

2. Préliminaires algébriques

Comme indiqué plus haut, notre démonstration reprend donc celle de [M]. Pour plus de détails, le lecteur pourra consulter cette note.

On remarque d'abord que le résultat de Cassels cité plus haut implique l'existence d'un entier rationnel w tel que

$$\frac{x^p - 1}{x - 1} = pw^q.$$

Ecrivons $p - 1 = d\ell$, où ℓ est impair et $d = 2^k$. Soit $\zeta = e^{2i\pi/p}$ et soit $L = L_p$ le corps cyclotomique $\mathbf{Q}(\zeta)$. Désignons par g une racine primitive modulo p. Alors le groupe de Galois $\mathrm{Gal}(L/\mathbf{Q})$ est cyclique, engendré par la transformation $\sigma : \zeta \mapsto \zeta^g$. Si $\tau = \sigma^d$ alors $\tau(\zeta) = \zeta^m$ où $m = g^d \bmod p$. Désignons par $K = K_p$ le sous-corps de L_p qui est invariant sous l'action de τ. Alors K est un corps de type CM de degré d et $K = \mathbf{Q}(\xi)$ où $\xi = \zeta + \zeta^m + \cdots + \zeta^{m^{\ell-1}}$, enfin $\mathrm{Gal}(K/\mathbf{Q}) = \{1, \sigma, \ldots, \sigma^{d-1}\}$ et $\sigma^{d/2}$ est la conjugaison complexe. On désigne par h_K le nombre de classes de K.

Posons

$$A(X) = \prod_{j=0}^{\ell-1} (X - \zeta^{m^j}), \qquad \beta = A(1) = \prod_{j=0}^{\ell-1} (1 - \zeta^{m^j}),$$

alors $\prod_{i=0}^{d-1} \sigma^i(\beta) = p$.

Dans le corps K, nous avons la factorisation

$$w^q = \delta_1 \cdots \delta_d, \qquad \delta_i = \sigma^{i-1}\big(A(x)/\beta\big), \quad i = 1, \ldots, d,$$

où les δ sont des entiers de K deux à deux étrangers (voir [I2]). Si $q \nmid h_K$ il existe un entier algébrique α et une unité η de K tels que

$$A(x) = \eta\beta\alpha^q.$$

On suppose désormais $\ell >$, alors les seules racines de l'unité appartenant à K sont ± 1, et comme K est un corps de type CM ceci implique que $\bar{\eta} = \pm\eta$.

Remarquons aussi que

$$\tilde{A}(X) = \prod_{j=0}^{\ell-1}(X - \zeta^{-m^j}) = \prod_{j=0}^{\ell-1}(\zeta^{m^j}X - 1) = -X^\ell \prod_{j=0}^{\ell-1}(X^{-1} - \zeta^{m^j}) = -X^\ell A(1/X),$$

la seconde égalité résultant de la congruence $1 + m + \cdots + m^{l-1} \equiv 0 \pmod{p}$, elle-même conséquence des relations $m^\ell \equiv g^{d\ell} \equiv 1 \pmod{p}$.

En particulier, on a $\tilde{\beta} = \tilde{A}(1) = -A(1) = -\beta$, et, puisque $\bar{\eta} = \pm\eta$, on a aussi $\tilde{A}(x) = \mp\beta\eta\tilde{\alpha}^q$. De plus la preuve de [M] montre que $\tilde{A}(x) \neq A(x)$. D'où les relations

$$\frac{\tilde{A}(x)}{A(x)} = \mp\left(\frac{\tilde{\alpha}}{\alpha}\right)^q = \prod_{j=0}^{\ell-1}\left(\frac{x - \zeta^{m^j}}{x - \zeta^{-m^j}}\right) = \prod_{j=0}^{\ell-1}\left(\frac{1 - \zeta^{m^j}/x}{1 - \zeta^{-m^j}/x}\right) \neq 1. \tag{4}$$

3. La forme linéaire de logarithmes

La relation (4) ci-dessus implique clairement

$$\frac{\tilde{A}(x)}{A(x)} = 1 + O\left(\frac{1}{x}\right).$$

De manière précise, la formule $x - 1 = u^q/p$, où $|u| > 1$ et $q > p$, montre que $|x| > 2^p/p > 6$, ce qui implique $|\log(1 + z/x)| < \frac{2}{|x|}$ pour tout nombre complexe x de module 1 (où log désigne la détermination principale du logarithme) et donc

$$\left|\log\frac{\tilde{A}(x)}{A(x)}\right| < \frac{4\ell}{|x|} < \frac{2p^2}{2^p} < 2. \qquad \text{[Ce qui implique } \tilde{A}(x) \neq -A(x).\text{]}$$

On pose

$$\Lambda = \left|\log\frac{\tilde{A}(x)}{A(x)}\right|,$$

si bien qu'il existe un entier rationnel k, avec $|k| \leq q$, tel que

$$\Lambda = |q\log(\tilde{\alpha}/\alpha) - ki\pi| \neq 0,$$

c'est la forme de logarithmes que nous allons étudier.

Remarquons que le nombre algébrique $\tilde{\alpha}/\alpha$ est racine du polynôme à coefficients entiers

$$\prod_{i=0}^{d-1}\sigma^j(\tilde{\alpha} - \alpha X) = \mathrm{Norm}(\alpha)X^d + \cdots,$$

donc, comme tous les conjugués de ce nombre sont de module un, on a

$$h(\tilde{\alpha}/\alpha) = \frac{1}{d}\log|\mathrm{Norm}(\alpha)| = \frac{\log|w|}{d},$$

puisque $\mathrm{Norm}\,A(x) = \pm\mathrm{Norm}(\beta)\cdot\mathrm{Norm}(\alpha^q) = \pm p w^q$, où h désigne la hauteur logarithmique absolue (définie par exemple en [L-M-N]).

Nous supposons désormais que $p \equiv 5 \pmod 8$, alors $p - 1 = 4\ell$ et donc

$$\Lambda < \frac{4p}{|x|}. \tag{5}$$

En appliquant le Théorème 3 de [L-M-N], on a la minoration

$$\log|\Lambda| \geq -8.87aH^2,$$

où $D = [\mathbf{Q}(\tilde{\alpha}/\alpha) : \mathbf{Q}]/2 = 2$ et

$$a \geq \max\Big\{20,\ 10.98|\log(\tilde{\alpha}/\alpha)| + D\,h(\tilde{\alpha}/\alpha)\Big\},$$

$$H = \max\Big\{17,\ \frac{\sqrt{D}}{10},\ D\log\left(\frac{|k|}{2a} + \frac{q}{68.9}\right) + 2.35D + 5.03\Big\}.$$

D'après les résultats de [M-R1] on sait que $p > 10^5$ et $q > 10^6$, un calcul élémentaire montre ensuite qu'on peut choisir

$$a = 34.5 + 2h(\tilde{\alpha}/\alpha), \qquad H = 5 + 2\log q.$$

Ainsi

$$|\log\Lambda| > -8.87 \times (34.5 + 2h(\tilde{\alpha}/\alpha)) \times (5 + 2\log q)^2. \tag{6}$$

La relation $(x^p - 1)/(x - 1) = pw^q$, compte tenu du calcul de $h(\tilde{\alpha}/\alpha)$ effectué plus haut, donne

$$h(\tilde{\alpha}/\alpha) = \frac{\log|w|}{d} < \frac{p-1}{dq}\log|x| < .25\,\frac{p}{q}\log|x|. \tag{7}$$

Enfin, en [M-R1], §1, on trouve la minoration $|x|^p \geq (2(q-1)p^q)^q$ qui, jointe aux inégalités (5), (6) et (7), fournit la majoration

$$q < 17.75\,p(2.5 + \log q)^2.$$

Considérons maintenant le cas où q divise h_K. On sait (voir [W]) que $h_K = h_K^+ \cdot h_K^-$ où $h_K^+ < p$, donc q divise h_K^-. Les majorations de Louboutin [Lo] montrent que $h_K^- < p\log^2 p$ (et même mieux), donc l'inégalité ci-dessus est encore vérifiée lorsque q divise h_K. Nous avons donc démontré le résultat suivant:

Théorème. *Lorsque $p \equiv 5 \pmod 8$ et $q > p$, l'équation de Catalan $x^p - y^q = 1$ ne peut avoir des solutions non triviales que pour*

$$q < 17.75\,p(2.5 + \log q)^2. \tag{2'''}$$

On vérifie facilement que l'estimation (2''') est meilleure que (2') pour $p > 3800$; pour le domaine qui nous intéresse, c'est à dire pour $p > 10^5$, le gain est d'un facteur supérieur à 1.46.

Références

[C] J.W.S. CASSELS .— On the equation $a^x - b^y = 1$, II ; *Proc. Cambridge Society*, 56, 1960, p. 97–103.

[I1] K. INKERI .— On Catalan's problem ; *Acta Arith.*, 9, 1964, p. 285–290.

[I2] K. INKERI .— On Catalan's conjecture ; *J. Number Th.*, 34, 1990, p. 142–152.

[K] KO CHAO .— On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$; *Sci. Sinica*, 14, 1965, p. 457–460.

[La] M. LANGEVIN .— Quelques applications de nouveaux résultats de van der Poorten, *Sém. Delange-Pisot-Poitou*, 1977/78, Paris, Exp. 4, 7 pages.

[L-M-N] M. LAURENT, M. MIGNOTTE et Y. NESTERENKO .— Formes linéaires en deux logarithmes et déterminants d'interpolation ;
J. Numb. Th., 55, 1995, p. 285–321.

[Le] V.A. LEBESGUE.— Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$; *Nouv. Ann. Math.*, 9, 1850, p. 178–181.

[Lo] S. LOUBOUTIN.— Majorations explicites de $|L(1,\chi)|$ (suite); *C. R. Acad. Sci. Paris*, à paraître.

[M] M. MIGNOTTE .— A criterion on Catalan equation ; *J. Numb. Th.*, 52, p. 280–284, 1995.

[M-R1] M. MIGNOTTE et Y. ROY .— Catalan's equation has no new solution with either exponent less then 10651, Experimental Mathematics, 4, 1995, p. 101–110.

[M-R2] M. MIGNOTTE et Y. ROY .— Minorations pour l'équation de Catalan, Comptes Rendus Acad. Sciences de Paris, soumis pour publication.

[Na] T. NAGELL .— Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$; *Nordsk. Mat. Forenings Skr. (1)*, 2, 1920, 14 pages.

[R] P. RIBENBOIM .— *Catalan's conjecture*; Acad. Press, Boston, 1994.

[S-T] T.N. SHOREY and R. TIJDEMAN .— *Exponential diophantine equations* ; Cambridge University Press, Cambridge, 1986.

[T] R. TIJDEMAN .— On the equation of Catalan ; *Acta Arith.*, 29, 1976, p. 197–209.

[W] L.C. WASHINGTON .— *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

Université Louis Pasteur
Département de mathématique
7, Rue René Descartes
67084, Strasbourg
Tél : 88416301 ; FAX : 88619069
e.mail: mignotte@math.u-strasbg.fr

Received August 29, 1996

C.R. Math. Rep. Acad. Sci. Canada - Vol. XVIII, No. 5, October 1996 octobre

Corrigendum to "On the Diophantine equation $x^4 - py^2 = z^p$" [C. R. Math. Rep. Acad. Sci. Canada 17(1995), no. 2, 61–66]

Zhenfu Cao

Presented by C.L. Stewart, F.R.S.C.

Let p be an odd prime. In the paper "On the Diophantine equation $x^4 - py^2 = z^p$" [1], we proved the following

Theorem 1. If $p \equiv 1 \pmod 4$ and the Bernoulli number $B_{(p-1)/2}$ is not divisible by p, then the Diophantine equation

$$x^4 - py^2 = z^p \tag{1}$$

has no integral solutions x, y, z with $(x, y) = 1$, $p \mid y$ and $2 \mid x$.

The proof of Theorem 1 needs the following result.

Theorem 2([1], Theorem 3). Let $a, k \in \mathbb{Z}$, $a > 0$, $(a, k) = 1$, $a^2 - k > 0$, and $a^2 - k = Db^2$, where D is a square-free positive integer. If $k \equiv 3 \pmod 4$, then

$$\frac{\alpha^p + \beta^p}{\alpha + \beta} \neq z^2, \ z \in \mathbb{Z}, \tag{2}$$

where $\alpha = a + b\sqrt{D}$, $\beta = a - b\sqrt{D}$.

In [1], The proof of Theorem 2 has an error ([1], pp. 64 – 65). Because "for any prime number $p > 5$, $p \equiv 1 \pmod 4$ there exists a positive integer λ such that $\left(\frac{\lambda}{p}\right) = -1$, $p - 4\lambda > 0$" and "$p - 4\lambda(a+1) = 1$" isn't both true.

Here, we give a right proof of Theorem 2.

Let m and n be coprime positive odd integers, $n < m$, and let $E(t) = (\alpha^t + \beta^t)/(\alpha + \beta)$ for $2 \nmid t$. We write the following sequence of equalities

$$\begin{aligned}
m &= 2l_1 n + \varepsilon_1 r_1, \ 0 < r_1 < n, \\
n &= 2l_2 r_1 + \varepsilon_2 r_2, \ 0 < r_2 < r_1, \\
r_1 &= 2l_3 r_2 + \varepsilon_3 r_3, \ 0 < r_3 < r_2, \\
&\cdots\cdots\cdots\cdots \\
r_{s-1} &= 2l_{s+1} r_s + \varepsilon_{s+1} r_{s+1}, r_{s+1} = 1,
\end{aligned}$$

where $\varepsilon_i = \pm 1$, $2 \nmid r_i (i = 1, 2, \cdots, s+1)$. Then we have

Lemma 1([1], Theorem 5). If $k \equiv 3 \pmod 4$, then Jacobi's symbol

$$\left(\frac{E(m)}{E(n)}\right) = \left(\frac{-k}{E(n)}\right)^{\lambda_1}\left(\frac{-k}{E(n)}\right)^{\lambda_2}\cdots\left(\frac{-k}{E(r_s)}\right)^{\lambda_{s+1}}\left(\frac{m}{n}\right),$$

where $\lambda_i = l_i + \dfrac{\varepsilon_i - 1}{2}$ $(i = 1, 2, \cdots, s+1)$.

Now, we also have

Lemma 2. If r and k are odd, $r > 0$, then $\left(\dfrac{-k}{E(r)}\right) = 1$.

Proof. It is easy to see that

$$E(r) \equiv \begin{cases} r \pmod 4, & \text{when } k \equiv 3 \pmod 4, \\ 1 \pmod 4, & \text{when } k \equiv 1 \pmod 4. \end{cases}$$

Since

$$E(r)=\sum_{j=0}^{(r-1)/2}\binom{r}{2j}a^{r-(2j+1)}b^{2j}D^j=\sum_{j=0}^{(r-1)/2}\binom{r}{2j}a^{r-(2j+1)}(a^2-k)^j$$
$$\equiv\sum_{j=0}^{(r-1)/2}\binom{r}{2j}a^{r-(2j+1)}a^{2j}=a^{r-1}\sum_{j=0}^{(r-1)/2}\binom{r}{2j}=(2a)^{r-1}\pmod{k}.$$

Thus
$$\left(\frac{E(r)}{|k|}\right)=\left(\frac{(2a)^{r-1}}{|k|}\right)=1.$$

If $k\equiv 3\pmod 4$, then $\left(\frac{-k}{E(r)}\right)=\left(\frac{E(r)}{-k}\right)=1$

when $k<0$. When $k>0$, we have

$$\left(\frac{-k}{E(r)}\right)=(-1)^{\frac{r-1}{2}}\left(\frac{k}{E(r)}\right)=(-1)^{\frac{r-1}{2}}(-1)^{\frac{k-1}{2}\cdot\frac{r-1}{2}}\left(\frac{E(r)}{k}\right)=1.$$

If $k\equiv 1\pmod 4$, then $\left(\frac{-k}{E(r)}\right)=\left(\frac{|k|}{E(r)}\right)=\left(\frac{E(r)}{|k|}\right)=1.$

This completes the proof of Lemma 2.

From Lemma 1 and Lemma 2, we have

Lemma 3. If $k\equiv 3\pmod 4$, then $\left(\frac{E(m)}{E(n)}\right)=\left(\frac{m}{n}\right)$.

In [2], we proved that if $k\equiv 1\pmod 4$ then

$$\left(\frac{E(m)}{E(n)}\right)=\left(\frac{-k}{E(n)}\right)^{\lambda_1}\left(\frac{-k}{E(n)}\right)^{\lambda_2}\cdots\left(\frac{-k}{E(r_s)}\right)^{\lambda_{s+1}}.$$

Hence, from Lemma 2 we also have

Lemma 4. If $k\equiv 1\pmod 4$, then $\left(\frac{E(m)}{E(n)}\right)=1$.

Proof of Theorem 2. Suppose that $k\equiv 3\pmod 4$ and $E(p)=z^2, z\in Z$. By Lemma 3 we have $1=\left(\frac{E(p)}{E(q)}\right)=\left(\frac{p}{q}\right)$

for every odd q, $p\nmid q$. On the other hand, for a given odd prime p, let q be an odd number such that $\left(\frac{p}{q}\right)=-1$ (It is easy to see that such an odd number q exists). Then $\left(\frac{E(p)}{E(q)}\right)=\left(\frac{p}{q}\right)=-1$ and we get a contradiction. This completes the proof of Theorem 2.

References

[1] Z. Cao, On the Diophantine equation $x^4-py^2=z^2$, *C. R. Math. Rep. Acad. Sci. Canada*, (2), XVII (1995), 61–66.

[2] Z. Cao, Applications of Diophantine equations to Lucas' sequences, *J. of Math.* (PRC), (3), 11(1991), 267–274.

Department of Mathematics
Harbin Institute of Technology
Harbin 150001 P. R. China

Received July 5, 1996

O.I. Bogoyavlenskij	Department of Mathematics & Statistics Queen's University Kingston, Ontario, K7L 3N6, Canada
Z. Cao	Department of Mathematics Harbin Institute of Technology Harbin 150001, P.R. China
A. Grytczuk	Institute of Mathematics Department of Algebra and Number Theory T. Kobarbiński Pedagogical University P65-069 Zielona Góra, Poland
C. Helou	Department of Mathematics Penn State University, Delaware County 25 Yearsley Mill Road Media, PA, USA 19063
R.B. Leipnik	Department of Mathematics University of California Santa Barbara, CA, USA, 93106
W.L. McDaniel	Department of Mathematics and Computer Science University of Missouri-St. Louis St. Louis, MO, USA 63121
M. Mignotte	Université Louis Pasteur Departement de mathématique 7, rue René Descartes F-67084, Strasbourg, France
D. Nour El Abidine	Departement de Mathematique Faculté des Sciences et Techniques de Mohammedia B.P. 146 Morocco
K.B. Ranger	Department of Mathematics University of Toronto Toronto, Ontario, M5S 3G3, Canada
P. Ribenboim	Department of Mathematics Queen's University Kingston, Ontario, K7L 3N6, Canada
E. Sadowska	Katedra Matematyki Politechnicka Lódzka Filia w Bielsku - Bialej ul Willowa 2 PL-43-309 Bielsko-Biala, Poland
A.I. Zayed	Department of Mathematics University of Central Florida Orlando, Florida, USA 32816-6990

CAMEL Listings
Canadian Mathematical Electronic Information Service

Papers published in Comptes Rendus/Mathematical Reports can now be listed electronically on the CAMEL system. Typescripts must be printed in TeX, LaTeX, Postscript or other digital format, and sent by e-mail by the author to *cr@camel.math.ca* or ftp to *camel.math.ca*. An additional page charge of $5 per page is necessary, to be added to the standard page charge. If authors so indicate at the time of submission of their paper to Mathematical Reports, an indication of this listing for their paper can be shown in the printed edition.

Papers listed are available at "*http://camel.math.ca/*".