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

Vol. XVI, Nos. 2, 3 **April-June 1994 avril-juin**

CONTENTS

THE SCHINZEL–TIJDEMAN THEOREM OVER FUNCTION FIELDS

B. BRINDZA, Á. PINTÉR AND J. VÉGSŐ

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

INTRODUCTION

Let $f \in \mathbb{Q}[X]$ be a polynomial with at least two distinct (complex) zeros. In 1976 Schinzel and Tijdeman [6] showed that the equation

$$f(x) = y^z, \text{ in rational integers } x, y, z \text{ with } |y| > 1$$

implies $z < C(f)$ where $C(f)$ is an effectively computable constant depending only on f. For further improvements, generalizations and related results we refer to [1],[2],[8] and [9]. The purpose of this paper is to give an effective analogue of the theorem, mentioned above, in the case when the unknowns x and y lie in an algebraic function field. Our result makes it possible to prove a general theorem on superelliptic equations over finitely generated fields (see Végső [10]).

Let k be an algebraically closed field of characteristic zero and let $\mathbf{K}$ be a finite extension of the rational function field $k(t)$ with genus $g(\mathbf{K})$ and degree d. Moreover, let $M_{\mathbf{K}}$ denote the set of additive valuations of $\mathbf{K}$ with value group $\mathbf{Z}$. The (additive) height of a non-zero element $\alpha \in \mathbf{K}$ and a non-zero polynomial $P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbf{K}[X]$ are defined by

$$H_{\mathbf{K}}(\alpha) = \sum_{v \in M_{\mathbf{K}}} -\min\{0, v(\alpha)\}$$

and

$$H_{\mathbf{K}}(P) = \sum_{v \in M_{\mathbf{K}}} -\min\{0, v(a_0), \dots, v(a_n)\},$$

respectively.

Theorem. *Let $f \in \mathbf{K}[X]$ be a polynomial of degree n with at least two distinct zeros (in an algebraic closure of $\mathbf{K}$). Then the equation*

$$f(x) = y^m \text{ in } x, y \in \mathbf{K}, m \in \mathbf{Z}^+ \text{ with } y \notin k \tag{1}$$

implies

$$m \le 32n^6(H_{\mathbf{K}}(f) + d + g(\mathbf{K})).$$

We note that the unknowns x and y are not necessarily integral over the polynomial ring $k[t]$, and an analogous result over algebraic number fields would have dramatic consequences.

The research of the first author has been supported in part by Grants 1641 and 4055 from the Hungarian National Foundation for Scientific Research. The research of the second author has been supported in part by Grant 4055 from the Hungarian National Foundation for Scientific Research .

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

AUXILIARY RESULTS

To prove our Theorem some preliminaries are needed. Let $\mathbf{L}$ be a finite extension of an algebraic function field $\mathbf{K}$ and $P \in \mathbf{K}[X]$ be a non-zero polynomial of degree n splitting into linear factors over $\mathbf{K}$; that is

$$P(X) = a\prod_{i=1}^{n}(X-\alpha_i), \quad (\alpha_i \in \mathbf{K}, i = 1, \dots, n).$$

For the following simple inequalities we refer to [5] and [7]. For any non-zero $\alpha, \beta \in \mathbf{K}$ and $m \in \mathbf{Z}$ we have

$$\max\{H_{\mathbf{K}}(\alpha\beta), H_{\mathbf{K}}(\alpha+\beta)\} \le H_{\mathbf{K}}(\alpha) + H_{\mathbf{K}}(\beta),$$

$$H_{\mathbf{K}}(\alpha^m) = |\, m \,|\, H_{\mathbf{K}}(\alpha),$$

$$H_{\mathbf{L}}(P) = [\mathbf{L} : \mathbf{K}]\, H_{\mathbf{K}}(P),$$

$$\max\{H_{\mathbf{K}}(a), \sum_{i=1}^{n} H_{\mathbf{K}}(\alpha_i)\} \le H_{\mathbf{K}}(P).$$

Let S be a finite subset of $M_{\mathbf{K}}$ containing all the *infinite valuations*[1] of $\mathbf{K}$. A non-zero $\alpha \in \mathbf{K}$ is called *S-unit* if $v(\alpha) = 0$ for every $v \notin S$.

Lemma 1. (Mason [4]) *Let $\gamma_1, \gamma_2, \gamma_3$ be S-units in $\mathbf{K}$ with*

$$\gamma_1 + \gamma_2 + \gamma_3 = 0.$$

Then

$$H_{\mathbf{K}}(\gamma_1/\gamma_2) \le |\, S \,| + 2g(\mathbf{K}) - 2.$$

where $|\, S \,|$ denotes the cardinality of S.

A similar result had been proved by Győry [3].

For an algebraic function field $\mathbf{K} \subseteq \mathbf{K}' \subseteq \mathbf{L}$ we put $G(\mathbf{K}') = [\mathbf{L} : \mathbf{K}'](g(\mathbf{K}') - 1)$.

Lemma 2. (Mason [5], p.65) *Let $A \in \mathbf{K}[X]$ be a polynomial and α be a zero of A such that $\mathbf{K}(\alpha) \subseteq \mathbf{L}$. Then*

$$0 \le G(\mathbf{K}(\alpha)) - G(\mathbf{K}) \le \frac{3}{2} H_{\mathbf{K}}(A).$$

(The constant $\frac{3}{2}$ can be improved a bit.)

[1] We recall that the extensions of the *degree valuation* of the rational function field $k(t)$ are said to be infinite (cf. Mason [5], Schmidt [7]).

Proof of the Theorem

Let (x, y, m) be an arbitrary, but fixed solution to the equation (1). Furthermore, let $\mathbb{F}$ be the splitting field of f and let f be factorized (over $\mathbb{F}$) as

$$f(X) = a\prod_{i=1}^{k}(X - \alpha_i)^{r_i},$$

where $\alpha_i \neq \alpha_j$ for $i \neq j$. Since

$$[\mathbb{F} : \mathbb{K}]H_{\mathbb{K}}(f) = H_{\mathbb{F}}(f) \geq \sum_{i=1}^{k} r_i H_{\mathbb{F}}(\alpha_i) = \sum_{i=1}^{k} r_i[\mathbb{F} : \mathbb{K}(\alpha_i)]H_{\mathbb{K}(\alpha_i)}(\alpha_i) \geq$$

$$\geq \sum_{i=1}^{k} \frac{r_i}{n}[\mathbb{F} : \mathbb{K}]H_{\mathbb{K}(\alpha_i)}(\alpha_i),$$

we have two (distinct) zeros of f with reasonable "size", that is, we may assume without loss of generality that $H_{\mathbb{K}(\alpha_1)}(\alpha_1) \leq H_{\mathbb{K}}(f)$ and $H_{\mathbb{K}(\alpha_2)}(\alpha_2) \leq nH_{\mathbb{K}}(f)$. Set $\mathbb{L} = \mathbb{K}(\alpha_1, \alpha_2)$ and $f_i(X) = f(X + \alpha_i), i = 1, 2$. For a polynomial $Q \in \mathbb{L}[X]$ we denote by $S(Q)$ the set of (additive) valuations of $\mathbb{L}$ with value group $\mathbb{Z}$ for which there exists a coefficient of Q with non-zero value. As a preparatory step to apply Lemma 1 we derive an upper bound for the cardinality of $S(f_i), i = 1, 2$.

Let $a = a_0^{(i)}, a_1^{(i)}, \ldots, a_n^{(i)}$ denote the coefficients of f_i, $i = 1, 2$. Then by using the *sum formula* we obtain

$$| S(f_i) | \leq \sum_{j=0}^{n} 2H_{\mathbb{L}}(a_j^{(i)}) \leq 2(n+1)H_{\mathbb{L}}(f_i) = 2(n+1)\frac{1}{[\mathbb{F} : \mathbb{L}]}H_{\mathbb{F}}(f_i) \leq$$

$$\leq \frac{2(n+1)}{[\mathbb{F} : \mathbb{L}]}(H_{\mathbb{F}}(a) + \sum_{j=1}^{k} H_{\mathbb{F}}((X + \alpha_i - \alpha_j)^{r_j}) \leq$$

$$\leq \frac{2(n+1)}{[\mathbb{F} : \mathbb{L}]}(H_{\mathbb{F}}(f) + \sum_{j=1}^{k} r_j H_{\mathbb{F}}(\alpha_j) + nH_{\mathbb{F}}(\alpha_i)) \leq$$

$$\leq \frac{2(n+1)}{[\mathbb{F} : \mathbb{L}]}(2H_{\mathbb{F}}(f) + nH_{\mathbb{K}(\alpha_i)}(\alpha_i)[\mathbb{F} : \mathbb{K}(\alpha_i)]) \leq 4(n+1)n^3 H_{\mathbb{K}}(f); \quad i = 1, 2.$$

By taking a valuation $v \notin S(f_i)$ of $\mathbb{L}$ such that $v(x - \alpha_i) \neq 0$ we get two cases to distinguish: $v(x - \alpha_i) < 0$ yields

$$mv(y) = v(f(x)) = v(f_i(x - \alpha_i)) = nv(x - \alpha_i), \ i = 1, 2.$$

Moreover, if $v(x - \alpha_i) > 0$, then

$$mv(y) = v(f_i(x - \alpha_i)) = l_i v(x - \alpha_i)$$

where l_i is the smallest degree occuring in the expression of the polynomial f_i. In both cases we have

(2) $$\frac{m}{n} \le \frac{m}{n} \mid v(y) \mid \le \mid v(x-\alpha_i) \mid, \; i=1,2.$$

The identity

(3) $$(x-\alpha_1)+(\alpha_2-x)+(\alpha_1-\alpha_2)=0$$

can be considered as an S-unit equation where the valuation set S is the smallest set containing all the infinite valuations of $\mathbf{L}$ and the sets $S(\alpha_1-\alpha_2), S(x-\alpha_i), S(f_i), i = 1,2$. (Now, the elements α_1, α_2 are considered as constant polynomials in $\mathbf{L}[X]$.) Applying Lemma 2 twice we get

$$0 \le G_{\mathbf{K}(\alpha_1)} - G_{\mathbf{K}} \le \frac{3}{2} H_{\mathbf{K}}(f)$$

and

$$0 \le G_{\mathbf{L}} - G_{\mathbf{K}(\alpha_1)} \le \frac{3}{2} H_{\mathbf{K}(\alpha_1)}(f) \le \frac{3}{2} n H_{\mathbf{K}}(f),$$

therefore,

$$g(\mathbf{L}) \le [\mathbf{L}:\mathbf{K}] g(\mathbf{K}) + \frac{3}{2}(n+1) H_{\mathbf{K}}(f).$$

If $S \subseteq S(f_1) \cup S(f_2) \cup S(\alpha_1-\alpha_2)$, then Lemma 1 implies

$$H_{\mathbf{L}}\left(\frac{x-\alpha_1}{\alpha_1-\alpha_2}\right) \le \mid S(f_1) \mid + \mid S(f_2) \mid + [\mathbf{L}:\mathbf{K}]d + \mid S(\alpha_1-\alpha_2) \mid + 2g(\mathbf{L}) - 2,$$

and the inequalities

$$m \le m H_{\mathbf{K}}(y) = H_{\mathbf{K}}(f(x)) \le (n+1) H_{\mathbf{K}}(f) + \frac{n(n+1)}{2} H_{\mathbf{K}}(x) \le$$
$$\le (n+1) H_{\mathbf{K}}(f) + \frac{n(n+1)}{2}\left(H_{\mathbf{L}}\left(\frac{x-\alpha_1}{\alpha_1-\alpha_2}\right) + H_{\mathbf{L}}(\alpha_1-\alpha_2) + H_{\mathbf{L}}(\alpha_1)\right)$$

provide the appropriate bound for m.

In the remaining case, when the set

$$S_1 = S \setminus (S(f_1) \cup S(f_2) \cup S(\alpha_1-\alpha_2))$$

is not empty, we have

$$\frac{\mid S \mid}{\mid S_1 \mid} \le 1 + \mid S(f_1) \cup S(f_2) \cup S(\alpha_1-\alpha_2) \mid .$$

It is clear that $\frac{m}{n} \mid S_1 \mid \le 2(H_{\mathbf{L}}(x-\alpha_1) + H_{\mathbf{L}}(x-\alpha_2))$ and

$$H_{\mathbf{L}}(x-\alpha_i) \le H_{\mathbf{L}}\left(\frac{x-\alpha_i}{\alpha_1-\alpha_2}\right) + H_{\mathbf{L}}(\alpha_1-\alpha_2), \; i=1,2.$$

By applying Lemma 1 again we obtain

$$H_{\mathbf{L}}\left(\frac{x-\alpha_i}{\alpha_1-\alpha_2}\right) \le \mid S \mid + 2g(\mathbf{L}) - 2, \; i=1,2,$$

thus

$$2(H_{\mathbf{L}}(x-\alpha_1) + H_{\mathbf{L}}(x-\alpha_2)) \le 4 \mid S \mid + 8g(\mathbf{L}) - 8 + 4H_{\mathbf{L}}(\alpha_1-\alpha_2),$$

and finally a simple calculation completes the proof.

Acknowledgements. The authors are grateful to Prof.K.Győry and the referee for their remarks.

References

[1] B.Brindza, *Zeros of polynomials and exponential diophantine equations*, Compositio Math. 61 (1987), 137–157.

[2] B.Brindza,K.Győry and R.Tijdeman, *The Fermat equation with polynomial values as base variables*, Invent.Math. 80 (1985), 139–151.

[3] K.Győry, *Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains*, Acta Math.Hungar. 42 (1983), 45–80.

[4] R.C.Mason, *On Thue's equation over function fields*, J.Lond.Math.Soc. 24 (1981), 414–426.

[5] R.C.Mason, *Diophantine Equations over Function Fields*, LMS Lecture Notes 96, Cambridge University Press, 1984.

[6] A.Schinzel and R.Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. 31 (1976), 199–204.

[7] W.M.Schmidt, *Thue's equation over function fields*, J.Austral Math.Soc. A 25 (1978), 385–422.

[8] T.N.Shorey and R.Tijdeman, *Exponential Diophantine Equations* , Cambridge University Press, 1986.

[9] J.Turk, *On the difference between perfect powers*, Acta Arith. 45 (1986), 289–307.

[10] J.Végsö, *On superelliptic equations*, Publ.Math.Debrecen 44 (1994), 183–189.

Kossuth Lajos University, Mathematical Institute, Debrecen, P.O.Box 12., 4010-Hungary

Received December 15, 1993

FLATNESS OF POWER SERIES EXTENSIONS CHARACTERIZES DEDEKIND DOMAINS

John T. Condo and David E. Dobbs

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

Abstract. It is proved that a (commutative integral) domain R is a Dedekind domain if and only if $T[[X]]$ is $R[[X]]$-flat for each domain T containing R as a subring.

Recall from [4] that if A is a subring of a (commutative integral) domain B, then $A \subset B$ is said to be LCM-stable in case $rB \cap sB = (rA \cap sA)B$ for all $r, s \in A$. Flatness is a sufficient condition for LCM-stability (cf. [3]); the converse holds for overrings but fails in general [8, Proposition 1.7 and Example 4.8]. As noted in [2], it follows from a result of F. Richman [7, Theorem 4] that a domain R is a Prüfer domain if and only if the polynomial ring $T[X]$ is $R[X]$-flat for each domain T containing R as a subring; equivalently, if and only if $R[X] \subset T[X]$ is LCM-stable for all such T. Our purpose here is to determine the domains R such that the formal power series ring $T[[X]]$ is $R[[X]]$-flat for each domain T containing R as a subring. Henceforth, X denotes an analytic indeterminate.

According to the main result of [2], a domain R is a Dedekind domain if and only if $R[[X]] \subset T[[X]]$ is LCM-stable for each domain T containing R as a subring.

Since flatness entails LCM-stability, it follows that if R is a domain such that $T[[X]]$ is $R[[X]]$ - flat for each domain T containing R as a subring, then R is a Dedekind domain. The following result establishes the converse, and thus achieves the purpose announced above. Its proof makes essential use of the above-cited result from [2].

<u>THEOREM.</u> For a domain R, the following are equivalent:

(1) $R[[X]] \subset T[[X]]$ is LCM-stable for each domain T containing R as a subring;

(2) $T[[X]]$ is $R[[X]]$ - flat for each domain T containing R as a subring;

(3) R is a Dedekind domain.

<u>Proof.</u> By the above comments, it suffices to prove that (3)⇒(2). Let a Dedekind domain R be a subring of a domain T. To prove that $T[[X]]$ is $R[[X]]$ - flat, it suffices to show that $B = T[[X]]_N$ is flat over $A = R[[X]]_N$ for each maximal ideal N of $R[[X]]$. By [6, Theorem 15.1], write $N = (M, X)$ for the corresponding maximal ideal M of R. It is important to note that A is a regular local ring [5, Exer.5, p.121] and, hence, a UFD (cf. [5, Theorem 184]). Without loss of generality, $\dim(A) = 2$; for, otherwise, A would be a local one-dimensional UFD, hence a DVR, and B would be A - flat.

According to the "conductor criterion" for flatness [1, Exer. 22, p.47], it suffices to prove that $(IB : f) \subset (I : f)B$ for each nonzero $f \in A$ and for each nonzero proper ideal I of A. To this end, suppose $h \in B$ satisfies $hf \in IB$; we shall produce $c_j \in A$, $d_j \in B$ such that $c_j f \in I$ and $h = \sum c_j d_j$.

Case 1: $ht(I) = 2$. Then $\sqrt{I} = NR[[X]]_N$, and so $X \in \sqrt{I}$. Hence, $X^n \in I$ for some positive integer n. Since T is R - flat and flatness is a universal property, the base change $R \to R_M[X]/X^nR_M[X]$ leads to the fact that B/X^nB is A/X^nA - flat. If $\overline{(\ )}$ denotes reduction modulo (X^n), then the condition $hf \in IB$ leads to $\overline{h}\overline{f} \in \overline{I}\overline{B}$. As $\overline{B}$ is $\overline{A}$- flat, the conductor criterion for flatness now yields $\overline{a}_j \in \overline{A}$, $\overline{b}_j \in \overline{B}$ such that $\overline{a}_j\overline{f} \in \overline{I}$ and $\overline{h} = \sum \overline{a}_j\overline{b}_j$. Choose a_j (resp., b_j) to be any preimage modulo (X^n) of $\overline{a}_j$ (resp., $\overline{b}_j$); then $h - \sum a_jb_j = X^nb$ for some $b \in B$. Also, writing $I = (f_1, ..., f_k)$ for suitable $f_i \in R[[X]]$, we have $a_{ij} \in A$ such that $\overline{a}_j\overline{f} = \sum_{i=1}^k \overline{a_{ij}}\overline{f_i}$, whence $a_jf - \sum a_{ij}f_i \in X^nA$. Since $f_i, X^n \in I$, we have $a_jf \in I$. As $X^nf \in I$ and $h = \sum a_jb_j + X^nb$, the required c_j, d_j have been presented.

Case 2: $ht(I) = 1$. As above, write $I = (f_1, ..., f_k), f_i \in R[[X]]$. Put $d = \gcd(f_1, ..., f_k) \in A$. Then d belongs to some height 1, hence principal, prime ideal of A. So d is a nonunit. Moreover, without loss of generality, $\gcd(d, f) = 1$. Since $hf \in IB$, we have $hf = \sum \beta_if_i = d\beta$ for suitable $\beta_i, \beta \in B$. Thus, $hf \in fB \cap dB$.

At this point, we invoke the main result of [2]: since R is Dedekind, $R[[X]] \subset T[[X]]$ is LCM-stable. Thus (cf. [8, Proposition 1.6]), $A \subset B$ is also LCM-stable. It follows that $hf \in (fA \cap dA)B$. However, $fA \cap dA = fdA$ since $\gcd(d, f) = 1$ (and A is a UFD), and so $h = d\alpha$ for some $\alpha \in B$.

Next, writing $f_i = g_id$ for suitable $g_i \in A$, we infer $\alpha f = \sum \beta_ig_i = \beta$. Thus with $J = (g_1, ..., g_k) = d^{-1}I$, we have $\alpha \in (JB : f)$. Note that $ht(J) \neq 1$ since $\gcd(g_1, ..., g_k) = 1$, and so by case 1, $\alpha \in (J : f)B$. Therefore, $\alpha = \sum \alpha_j\delta_j$ for some $\alpha_j \in A$, $\delta_j \in B$ such that $\alpha_jf \in J$. Then $\gamma_j = d\alpha_j \in A$ satisfies $\gamma_jf = d(\alpha_jf) \in dJ = I$ and $\sum \gamma_j\delta_j = d\sum \alpha_j\delta_j = d\alpha = h$, as desired. ∎

We find it remarkable that the above proof that (3)⇒(2) needed to invoke the main result from [2]. It would be interesting to find a proof that (3)⇒(2) which would avoid mentioning LCM-stability.

Let n be a positive integer. We do not know which (necessarily Dedekind, hence Noetherian) domains R are characterized by the property that the formal power series ring $T[[X_1, ..., X_n]]$ is $R[[X_1, ..., X_n]]$ - flat for each domain T containing R as a subring. We close with some observations about the n-variable context.

REMARK. (a) If a Noetherian domain T is flat over a Noetherian subring R, then $T[[X_1, ..., X_n]]$ is $R[[X_1, ..., X_n]]$ - flat. For a proof, we may reduce to the case $n = 1$ since power series rings inherit Noetherianness, and this case is handled by [2, Remark 2.12(b)].

(b) If a Dedekind domain R is a subring of a Noetherian domain T, then $T[[X_1, ..., X_n]]$ is $R[[X_1, ..., X_n]]$ - flat. For a proof, (a) may be applied, as R is Noetherian.

(c) If R is a Noetherian domain with quotient field K and if K is a subring of a domain T, then $T[[X_1, ..., X_n]]$ is $R[[X_1, ..., X_n]]$ - flat. For a proof, note via [1, Exer.17(a), p.250] that $T[[X_1, ..., X_n]]$ is $K[[X_1, ..., X_n]]$ - flat. Thus, by the transitivity of flatness, it suffices to show that $K[[X_1, ..., X_n]]$ is $R[[X_1, ..., X_n]]$ - flat. This, in turn, follows from (a), as K is Noetherian and R - flat.

REFERENCES

1. N. Bourbaki, Commutative Algebra, Addison-Wesley, Reading, 1972

2. J.T. Condo, LCM-stability of power series extensions characterizes Dedekind domains, Proc. Amer. Math. Soc., to appear.

3. D.E. Dobbs, On n-flat modules over a commutative ring, Bull. Austral. Math. Soc. 43 (1991), 491-498.

4. R. Gilmer, Finite element factorization in group rings : Lecture Notes Pure Appl. Math. 7, Dekker, New York, 1974.

5. I. Kaplansky, Commutative Rings, second ed., Univ. Chicago Press, Chicago/London, 1974.

6. M. Nagata, Local Rings, Wiley-Interscience, New York/London/Sydney, 1962.

7. F. Richman, Generalized quotient rings, Proc. Amer. Math. Soc. 16 (1965), 794-799.

8. H. Uda, LCM-stableness in ring extensions, Hiroshima Math. J. 13 (1983), 357-377.

Ball State University

Muncie, IN 47306-0490, U.S.A.

Received April 5, 1994

University of Tennessee

Knoxville, TN 37996-1300, U.S.A.

The Diophantine equation $x^4 \pm py^4 = z^p$

Nobuhiro Terai

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

§1 Introduction.

Let p be an odd prime and put $p^* = (-1)^{(p-1)/2}p$. Let d be a square-free positive integer. In [4], Powell proved the following:
Theorem 1 (Powell[4]) (a) If $p \not\equiv \pm 1 \pmod 8$, then the Diophantine equation

$$x^4 + y^4 = z^p$$

has no integral solutions x, y, z with $(x, y) = 1$ and $p \not| xy$.
(b) The Diophantine equation

$$x^4 - y^4 = z^p \text{ (resp. } x^4 - 4y^4 = z^p)$$

has no integral solutions x, y, z with $(x, y) = 1$, $p \not| xyz$ (resp. $p \not| y$).

Powell proved (a) by factoring z^p as $(x^2 + iy^2)(x^2 - iy^2)$ over the Gaussian ring $\mathbb{Z}[i]$. The proof of (b) needs the result concerning the Jacobi symbol used in the proof of the first case of Fermat's Last Theorem for even exponents by Terjanian (cf. Terjanian[8] or Ribenboim[5], p.67).

To generalize Theorem 1, (a), in the previous paper [7] we considered whether the Diophantine equation

$$x^4 + dy^4 = z^p \qquad (1)$$

has integral solutions x, y, z or not, and using the theory of imaginary quadratic fields, we obtained the following (cf. Cao[2]).

Theorem 2 (Terai and Osada[7]) *Let p be an odd prime, $d \not\equiv 3 \pmod 4$ a square-free positive integer, and $h(-d)$ the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. If $p \not\equiv \pm 1 \pmod 8$ and $p \not| h(-d)$, then the Diophantine equation* (1) *has no integral solutions x, y, z with $(x, y) = 1$, $p \not| xy$ and y even.*

If $d = 1$ in (1), it follows unconditionally that $p \not| h(-1)$ and y is even. Therefore Theorem 2 gives a generalization of Theorem 1, (a). The proof of Theorem 2 is based on the following two facts:

(i) Let a, b be relatively prime integers of opposite parity and c an integer. Then the implication

$$a^2 + db^2 = c^p \Rightarrow a + b\sqrt{-d} = (u + v\sqrt{-d})^p \tag{2}$$

holds for some integers u and v.

(ii) A square of odd integers is congruent to 1 modulo 8.

In general, it is difficult to show that the implication (2) holds (especially for $d < 0$). Adachi [1] showed that the implication (2) holds for $d = -p^*$ under some conditions.

In this paper, we consider the Diophantine equation (1) when $d = -p^*$, and prove the following two theorems:

Theorem 3. *If $p \equiv 1 \pmod 4$ and $B_{(p-1)/2} \not\equiv 0 \pmod p$, then the Diophantine equation*

$$x^4 - py^4 = z^p \tag{3}$$

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

Theorem 4. *The Diophantine equation*

$$x^4 + 3y^4 = z^3 \tag{4}$$

has no integral solutions x, y, z with $(x, y) = 1$.

§2 Proof of Theorems.

First we prepare two lemmas:

Lemma 1 (Adachi[1]) *Let p be an odd prime, and a, b relatively prime and of opposite parity. In the case $p \equiv 1 \pmod 4$, we also suppose that the Bernoulli number $B_{(p-1)/2}$ is not divisible by p and b is divisible by p. If $d = -p^*$, then the implication (2) is valid.*

The following lemma is obtained by applying the idea of Terjanian[8] using properties of Jacobi's symbol.

Lemma 2 (Rotkiewicz[6]) *Let α and β be the different zeros of the trinomial $x^2 - Lx + M$, where $L > 0$ and M are rational integers such that $K = L^2 - 4M > 0$ and $(L, M) = 1$. If $2 \mid L$, $M \equiv -1 \pmod 4$ and p is an odd prime, then*

$$L_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} \neq pz^2.$$

Now we use Lemma 1, 2 to prove Theorem 3, 4.

Proof of Theorem 3. Suppose that the Diophantine equation (3) has integral solutions. Then it follows from Lemma 1 that

$$x^2 + \sqrt{p}y^2 = (a + b\sqrt{p})^p.$$

Therefore we have

$$x^2 = a\sum_{j=0}^{(p-1)/2}\binom{p}{2j}a^{p-(2j+1)}b^{2j}p^j = aA,$$

$$y^2 = b\sum_{j=0}^{(p-1)/2}\binom{p}{2j+1}a^{p-(2j+1)}b^{2j}p^j = bB.$$

We first show that $(a, A) = 1, (b, B) = p$ and $p \| B$. From $(x, y) = 1$ and $p \mid y$, we have $p \nmid aA$ and $(a, b) = 1$. Hence since

$$A \equiv pb^{p-1}p^{(p-1)/2} \pmod{a^2} \quad \text{and} \quad B \equiv pa^{p-1} \pmod{b^2p^2},$$

we have $(a, A) = 1$, $p \| B$. Thus it follows from $p \mid y$ that $p \mid b$ and so $(b, B) = p$. Therefore we obtain

$$a = \pm u^2, \quad A = \pm U^2, \quad b = \pm pv^2, \quad B = \pm pV^2$$

for some non-zero integers u, U, v, V.

We next show that a and b are of opposite parity. Suppose that a and b are odd. Then we have

$$A \equiv \sum_{j=0}^{(p-1)/2}\binom{p}{2j} = 2^{p-1} \pmod 2$$

and

$$B \equiv \sum_{j=0}^{(p-1)/2}\binom{p}{2j+1} = 2^{p-1} \pmod 2,$$

so A and B are even, which contradicts $(x, y) = 1$. Thus a and b are of opposite parity from $(a, b) = 1$. Since $A \equiv a^{p-1} + pb^{p-1}p^{(p-1)/2} \pmod{a^2b^2}$ and $a \not\equiv b \pmod 2$, we have

$$\pm U^2 = A \equiv a^{p-1} + pb^{p-1}p^{(p-1)/2} \pmod 4,$$

so

$$\pm U^2 \equiv a^{p-1} + b^{p-1} \equiv 1 \pmod 4.$$

Hence $A = U^2$, so $a = u^2$. Similarly we obtain $B = pV^2$, $b = pv^2$.

Put $\alpha = a + b\sqrt{p}$ and $\beta = a - b\sqrt{p}$. We note that $a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$, since $x \equiv 0 \pmod 2$ and $(a, b) = 1$. Thus we have $L = \alpha + \beta = 2a(> 0) \equiv 0 \pmod 2$, $M = \alpha\beta = a^2 - pb^2 \equiv -1 \pmod 4$ since $p \equiv 1 \pmod 4$, and $(L, M) = 1$.

Since $x^2 + \sqrt{p}y^2 = \alpha^p$ and $x^2 - \sqrt{p}y^2 = \beta^p$, we obtain

$$\begin{aligned} y^2 &= \frac{\alpha^p - \beta^p}{2\sqrt{p}} \\ &= b \cdot \frac{\alpha^p - \beta^p}{2b\sqrt{p}} \\ &= b \cdot \frac{\alpha^p - \beta^p}{\alpha - \beta} \\ &= bB. \end{aligned}$$

Therefore we have $B = \dfrac{\alpha^p - \beta^p}{\alpha - \beta} = pV^2$, which contradicts Lemma 2. This completes the proof of Theorem 3. ∎

Remark 1. No examples of $B_{(p-1)/2} \equiv 0 \pmod p$ are known for $p < 6270713$ (cf. Washington [9], p.82).

Remark 2. If $p \nmid y$ and x is odd, then the Diophantine equation (3) has an integral solution. For example, $(x, y, z, p) = (3, 2, 1, 5)$.

In the same way as the proof of Theorem 3, we obtain the following:

Corollary. *If $p \equiv 1 \pmod 4$ and $B_{(p-1)/2} \not\equiv 0 \pmod p$, then the Diophantine equation*

$$x^4 - p^3y^4 = z^p \tag{5}$$

has no integral solutions x, y, z with $(x, y) = 1$ and x even.

Proof. The Diophantine equation (5) can be written as $(x^2)^2 - p(py^2)^2 = z^p$. It follows from Lemma 1 that

$$x^2 + \sqrt{p} \cdot py^2 = (a + b\sqrt{p})^p.$$

We use the notations in the proof of Theorem 3. Then we have $py^2 = bB$. Since $p \nmid a$ and $B \equiv pa^{p-1} \pmod{b^2p^2}$, we have $p \| B$ and $(b, B/p) = 1$. Thus

$$b = \pm v^2, B = \pm pV^2.$$

By the same argument as the proof of Theorem 3, we obtain $B = \dfrac{\alpha^p - \beta^p}{\alpha - \beta} = pV^2$, which contradicts Lemma 2. This completes the proof of corollary. ∎

Proof of Theorem 4. Suppose that the Diophantine equation (4) has integral solutions. If x and y are odd, then z is even. Hence by (4), we have $4 \equiv 0 \pmod 8$, which is impossible. Thus x and y are of opposite parity since $(x, y) = 1$. Therefore it follows from Lemma 1 that

$$x^2 + \sqrt{-3}y^2 = (s + \sqrt{-3}t)^3$$

for some non-zero integers s, t. Then we have

$$x^2 = s(s^2 - 9t^2)$$

and

$$y^2 = 3t(s^2 - t^2).$$

Since $(x, y) = 1$, we have $(s, 3t) = 1$ and so $(s, s^2 - 9t^2) = 1$. Thus there are integers u, v with $(u, v) = 1$ such that $s = \pm u^2$ and $s^2 - 9t^2 = \pm v^2$. But a congruence mod 3 shows that the – sign must be rejected. Hence

$$s = u^2 \quad \text{and} \quad s^2 - 9t^2 = v^2.$$

Suppose first that $t \equiv 0 \pmod 3$. Then by $(3t, s^2 - t^2) = 1$, we have

$$3t = \pm w^2 \quad \text{and} \quad s^2 - t^2 = \pm r^2.$$

Therefore we obtain

$$u^4 - w^4 = v^2,$$

which has no integral solutions as well known.

Suppose next that $t \not\equiv 0 \pmod 3$. Then by $(3t, s^2 - t^2) = 3$, we have

$$t = \pm w^2 \quad \text{and} \quad s^2 - t^2 = \pm 3r^2.$$

Thus

$$u^4 - 9w^4 = v^2,$$

which has no integral solutions as well known (cf. Dickson [3], p.634). ∎

Remark 3. If $p \equiv -1 \pmod 4$, then $-d = p^* = -p < 0$ and so $K = L^2 - 4M < 0$. Hence in this case we can not apply Lemma 2. But we here treated only the case of $p = 3$, using Lemma 1.

Remark 4. If $(x, y) \neq 1$, then the Diophantine equation (4) has many integral solutions. For example, $(x, y, z) = (2a^3, 2a^3, 4a^4), (7a^3, 14a^3, 49a^4)$. The integral solutions of (4) with $(x, y) \neq 1$ and $0 < x, y < 300$ are given in the table below. The least solution of (4) such that $(x, y) \neq 1$, $x \nmid y$ or $y \nmid x$ is $(x, y, z) = (49923, 33282, 2146689)$. It seems that the condition $(x, y) = 1$ is essential for the Diophantine equation (1) to have no integral solutions.

Table. The integral solutions of (4) with $(x, y) \neq 1$ and $0 < x, y < 300$

x	y	z
2	2	4
7	14	49
16	16	64
54	54	324
56	112	784
128	128	1024
250	250	2500

References

[1] N. Adachi, The Diophantine equation $x^2 \pm ly^2 = z^l$ connected with Fermat's Last Theorem, *Tokyo J. Math.*, (1), **11**(1988), 85-94.

[2] Z. Cao, The Diophantine equation $cx^4 + dy^4 = z^p$, *C.R. Math. Rep. Acad. Sci. Canada*, (5), **XIV**(1992), 231-234.

[3] L.E.Dickson, *History of the Theory of Numbers*, Vol. II, Chelsea, New York 1971.

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

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

[6] A. Rotkiewicz, Applications of Jacobi's symbol to Lehmer's numbers, *Acta Arith.*, XLII(1983), 163–187.

[7] N. Terai and H. Osada, The Diophantine equation $x^4 + dy^4 = z^p$, *C.R. Math. Rep. Acad. Sci. Canada*, (1), XIV(1992), 55–58.

[8] G. Terjanian, Sur l'équation $x^{2p}+y^{2p} = z^{2p}$, *C.R. Acad. Sci. Paris*, **285**(1977), 973-975.

[9] L.C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, 83, Springer-Verlag, 1982.

Nobuhiro Terai
Division of General Education
Ashikaga Institute of Technology
268-1 Omae, Ashikaga, Tochigi 326
Japan

Received January 5, 1994

FREY CURVES OVER PRINCIPAL IDEAL DOMAINS

PAVLOS TZERMIAS

Department of Mathematics, University of California, Berkeley, CA 94720

May 3, 1994

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

ABSTRACT. In his paper [1], G. Frey shows that the existence of a non-trivial integer solution to Fermat's equation is equivalent to the existence of an elliptic curve over Q with certain properties. In this paper, we consider the Fermat equation in a more general form and generalize Frey's argument to obtain a similar statement when the base field is the fraction field of a principal ideal domain of characteristic different than 2.

1. NOTATION

Let p be a prime number such that $p \geq 5$. Let R be a principal ideal domain of characteristic different than 2 and p. Let S denote the set of primes dividing 2 and let F be the fraction field of R.

We consider the Fermat-like equation in six variables $S_1X^p + S_2Y^p + S_3Z^p = 0$. We are intersted in solutions $(S_1, S_2, S_3, X, Y, Z) = (s_1, s_2, s_3, a, b, c)$, where a, b, c are non-zero elements of R and s_1, s_2, s_3 are units in R. We may assume that a, b, c are pairwise coprime. Let $A = s_1a^p$, $B = s_2b^p$, $C = s_3c^p$.

We define an equivalence relation in the set of such solutions as follows:

(s_1, s_2, s_3, a, b, c) is equivalent to $(s'_1, s'_2, s'_3, a', b', c')$

if and only if $\{A, B, C\} = \{uA', uB', uC'\}$ (as sets), for some unit u in R.

We also call a solution (s_1, s_2, s_3, a, b, c) trivial iff a, b, c are units in R. By the unit theorem (see [4]), there are only finitely many equivalence classes of trivial solutions and they are effectively computable.

Given a solution, consider the elliptic curve over F given by

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

(This is non-singular because $2 \neq 0$ in R. Also observe that there is nothing special about the pair (A, B); we could have chosen any other pair instead.)

We have the associated quantities (see [4]):

$c_4 = 16(A^2 + B^2 + AB)$, $\Delta = 16A^2B^2C^2$, $j = c_4^3/\Delta = 2^8(A^2 + B^2 + AB)^3/A^2B^2C^2$.

Let l be a prime of R not in S.

If l does not divide ABC, then we have good reduction at l.

If l divides ABC , then l cannot divide c_4, therefore $v_l(c_4) = 0$ and $v_l(\Delta) > 0$, so the Weierstrass form is minimal at l and we have multiplicative reduction at l.

The reduction type at primes $l \in S$ does not have to be multiplicative. As an example, let R be the ring of integers of $F = Q(\sqrt{-3})$. The field F has class number 1 and, as noted in [3], we have the solution $(1, 1, 1, \zeta, \zeta^{-1}, -1)$, where ζ is a primitive 6th root of 1. Then 2 is inert in R and it is easy to check that the given Weierstrass form of the elliptic curve corresponding to this solution is minimal at 2, therefore the reduction is additive at 2.

In the sequel, we will use S as a prefix whenever we want to describe properties shared by all primes not in S. Therefore, the considerations above give an elliptic curve over F with S-multiplicative reduction.

2. RAMIFICATION OF POINTS OF ORDER p

In order to state and prove the theorem in the next section, we will need the following two propositions:

Proposition 1

Let E be an elliptic curve over R with multiplicative reduction at the prime l. Let p be a rational prime , not divisible by l, and let K_p denote the extension of F obtained by adjoining the coordinates of the points of order p on E. Let λ be a divisor of l in K_p and $K_{p,\lambda}$ the corresponding completion. Also let F_l be the completion of F at l. If $e(/)$ denotes ramification index, then we have $e(K_{p,\lambda}/F_l) = e(F_l(\zeta_p, j^{1/p})/F_l)$, where ζ_p is a primitive pth root of 1.

Proof

Since K_p/F is Galois, it suffices to prove the assertion for the place λ such that $K_{p,\lambda} = F_l(E[p])$. ($E[p]$ is the subgroup of points of order p of E.)

Let q be the F_l-integer such that $j = (1/q) + \sum_{n=0}^{\infty} c_n q^n$, where the coefficients c_n are integers.

Observe that $(jq)^{1/p}$ exists in F_l (apply Hensel's lemma to the polynomial $X^p - jq$ with first approximation equal to 1). Hence $F_l(\zeta_p, q^{1/p}) = F_l(\zeta_p, j^{1/p})$.

We have two cases to consider:

(i) E has split reduction at l. Then, by Tate's theorem (see [4]), we have an isomorphism of $E(K_{p,\lambda})$ and $K^*_{p,\lambda}/ < q >$ as $Gal(\overline{F}_l/K_{p,\lambda})$- modules.

Since $E[p]$ is contained in $E(K_{p,\lambda})$, we conclude that there exist elements ζ_p, $q^{1/p}$ in $K_{p,\lambda}$ and we have

$K_{p,\lambda} = F_l(E[p]) = F_l(\zeta_p, q^{1/p})$, which proves the assertion in this case.

(ii) E has non-split reduction at l. Then, again by Tate's theorem (see [4]), there exists a quadratic unramified extension L of F_l such that E is isomorphic to the Tate curve E_q over L. Let M be the compositum of $K_{p,\lambda}$ and L. Then $E(M)$ and $M^*/ < q >$ are isomorphic $Gal(\overline{F}_l/M)$-modules.

As in part (i), we conclude that there exist elements ζ_p, $q^{1/p}$ in M and $M = L(E[p]) = L(\zeta_p, q^{1/p})$. Since L/F_l is unramified, we get
$e(K_{p,\lambda}/F_l) = e(M/F_l) = e(L(\zeta_p, q^{1/p})/L) = e(F_l(\zeta_p, q^{1/p})/F_l)$, and this completes the proof.

Proposition 2
Let l, p, K_p be as in proposition 1. Let E be an eliptic curve over F having good or multiplicative reduction at l. Then K_p/F is unramified at l if and only if $v_l(j) \geq 0$ or $v_l(j) = 0 \bmod p$.

Proof
If $v_l(j) \geq 0$, then E has good reduction at l. Indeed, if this were not the case, then, by semistability, $v_l(c_4) = 0$ and $v_l(\Delta) > 0$, so $v_l(j) < 0$, which is absurd.
Therefore , by the criterion of Néron-Ogg-Shafarevich, we get that K_p/F is unramified at l.
Now suppose $v_l(j) = 0 \bmod p$ and $v_l(j) < 0$. Then we have multiplicative reduction at l, so it suffices to show that $F_l(\zeta_p, j^{1/p})/F_l$ is unramified, by proposition 1. But this is evidently true, because $v_l(j) = 0 \bmod p$ and p is not divisible by l (see e.g. [2], page 130).
Conversely, suppose that K_p/F is unramified at l and $v_l(j) < 0$. Then we have multiplicative reduction , so we can apply proposition 1. Then $e(F_l(\zeta_p, j^{1/p})/F_l) = 1$, therefore $v_l(j) = 0 \bmod p$ (again by [2]).

3. THE THEOREM

We now return to the Frey curves of section 1. We have the following:

THEOREM
For a prime $p \geq 5$, the following are equivalent:
1. There exist non-zero a, b, c and units s_1, s_2, s_3 in R such that

$$s_1 a^p + s_2 b^p + s_3 c^p = 0.$$

2. There exists an elliptic curve E over F with S-multiplicative reduction and an S-minimal Weierstrass equation $y^2 = x^3 + dx^2 + ex$, where d, e are coprime elements in R, such that:
(i) The points of order 2 are F-rational.
(ii) the field K_p obtained by adjoining the coordinates of the points of order p on E is unramified over F outside the divisors of $2p$.
(iii) $min(0, v_\rho(j) - v_\rho(2^8)) = 0 \bmod p$, for all $\rho \in S$, and $min(0, v_{p_i}(j)) = 0 \bmod p$ for all p_i dividing p.

3. There exists an elliptic curve E over F with S-multiplicative reduction and an S-minimal Weierstrass equation $y^2 = x^3 + dx^2 + ex$, where d, e are coprime elements in R, for which $\Delta/16 = u^2r^{2p}$, where u is a unit and r is in R.

Proof

1 implies 2.

Let the notation be as in section 1. Then $d = B - A$, $e = -AB$. Let $\rho \in S$. If ρ divides $e = -AB$, then it cannot divide d, by coprimality of A, B. Therefore, ρ cannot divide both d and e.

Also if l is a prime of R which does not lie in S, then, by S-minimality and S-multiplicativity of the given Weierstrass equation, we get that l cannot divide both d and e.

Therefore d, e are coprime.

The points of order 2 are $(0,0)$, $(A,0)$ and $(-B,0)$, which are of course F-rational. This proves (i).

Now let l be a prime not dividing $2p$. If l does not divide ABC, then $v_l(j) \geq 0$, so K_p/F is unramified at l, by proposition 2. If l divides ABC, then $v_l(j) = -2p(v_l(a) + v_l(b) + v_l(c))$, so $v_l(j)$ is divisible by p, hence K_p/F is unramified at l, again by proposition 2. This proves (ii).

Also, let $\rho \in S$. If ρ divides ABC, then $v_\rho(j) - v_\rho(2^8) \leq 0$ and $v_\rho(j) - v_\rho(2^8) = 0 \bmod p$ (Since A. B, C are p-powers). Otherwise, if ρ does not divide ABC, then $v_\rho(j) - v_\rho(2^8) \geq 0$. Hence, in any case, $min(0, v_\rho(j) - v_\rho(2^8)) = 0 \bmod p$.

Finally, let p_i be a divisor of p in R. If p_i does not divide ABC , then obviously $v_{p_i}(j) \geq 0$. Otherwise, if p_i divides ABC, we get $v_{p_i}(j) = -2p(v_{p_i}(a) + v_{p_i}(b) + v_{p_i}(c))$. Hence, in any case, p divides $min(0, v_{p_i}(j))$, which proves (iii).

2 implies 3.

The given equation is S-minimal and we have $\Delta = 16e^2(d^2 - 4e)$ and $j = 2^8(d^2 - 3e)^3/(e^2(d^2 - 4e))$, by direct calculation.

So it suffices to show that $e^2(d^2 - 4e)$ is a $2p$-power times the square of a unit.

Now, $e^2(d^2 - 4e)$ is already a square, since it equals the square of the product of the x-coordinates of the points of order 2 on E (it is a square of an element in F and therefore it is a square of an element in R, since it lies in R already).

So it will suffice to show that the valuation of $e^2(d^2 - 4e)$ at every prime l that divides $e^2(d^2 - 4e)$ is a multiple of p.

Let l be such a prime (i.e. l divides $e^2(d^2 - 4e)$).

If l does not divide $2p$, then, by proposition 2 and the fact that K_p/F is unramified at l, we get that $v_l(j) = 0 \bmod p$, hence, $v_l(e^2(d^2 - 4e))$ is divisible by p, by S-semistability.

If $l = p_i$ divides p, then $v_{p_i}(j) < 0$ (by S-semistability), so, by (iii), $v_{p_i}(e^2(d^2 - 4e))$ is divisible by p.

Finally, let $l \in S$, say $l = \rho$.

We have two possibilities:

Suppose ρ divides e. Then, ρ does not divide d (by coprimality of d, e), so ρ does not divide $d^2 - 3e$. Now, by (iii), p divides $v_\rho(j) - v_\rho(2^8)$, i.e. p divides $v_\rho((d^2-3e)^3/(e^2(d^2-4e)))$. Since ρ does not divide $d^2 - 3e$, we get that p divides $v_\rho(e^2(d^2-4e))$.

Suppose ρ does not divide e. Then ρ divides $d^2 - 4e$. Then, obviously ρ cannot divide $d^2 - 3e$ (otherwise, it would also divide e, which is absurd). Again , since, by (iii), p divides $v_\rho((d^2-3e)^3/(e^2(d^2-4e))$, we get that p divides $v_\rho(e^2(d^2-4e))$.

Therefore, $v_l(e^2(d^2-4e))$ is a multiple of p for all primes l of R.

3 implies 1.

Since d and e are coprime, so are $d^2 - 4e$ and e. Therefore, there exist coprime elements v, w and units u_1, u_2 in R such that $d^2 - 4e = u_2 v^{2p}$ and $e = u_1 w^p$. Then $u_1^2 u_2 w^{2p} v^{2p} = u^2 r^{2p}$.

Therefore, $u_1^2 u_2 = u^2$, therefore u_2 is also a square, say $u_2 = u_3^2$.

Then $(d - u_3 v^p)(d + u_3 v^p) = 4e = 4u_1 w^p$. Note that the only possible common prime factor of $d - u_3 v^p$, $d + u_3 v^p$ are in S. Fix $\rho \in S$ for the moment. There exist non-negative integers μ, ν (both of them $\leq p - 1$), units u_4, u_5 and S-coprime elements z_1, z_2 such that

$d - u_3 v^p = u_4 \rho^\mu z_1^p$, $d + u_3 v^p = u_5 \rho^\nu z_2^p$, where $\mu + \nu = v_\rho(4) \bmod p$.

Then

$2d = u_4 \rho^\mu z_1^p + u_5 \rho^\nu z_2^p$ and

$2u_3 v^p = u_5 \rho^\nu z_2^p - u_4 \rho^\mu z_1^p$.

If $\mu + \nu = v_\rho(4) + p$, then both μ and ν are at least $v_\rho(4) + 1$. Then $\rho^{v_\rho(4)+1}$ divides $2d$ and $2u_3 v^p$. Therefore, $\rho^{v_\rho(4)+2}$ divides d^2 and v^{2p}, absurd, since $d^2 - u_2 v^{2p} = 4e$ and d, e are coprime.

Therefore we must have $\mu + \nu = v_\rho(4)$.

Suppose μ is different than ν, say $\mu < \nu$. Then $\mu < v_\rho(2)$ and $\nu > v_\rho(2)$. Then ρ divides z_1, so ρ^ν divides $2d$ and ρ divides e, absurd, since $\nu > v_\rho(2)$ and d, e are coprime.

Therefore, $\mu = \nu = v_\rho(2)$.

This being true for all ρ dividing 2, we conclude that we can write

$d - u_3 v^p = u_6 z_3^p \prod \rho^{v_\rho(2)} = 2u_8 z_3^p$,

$d + u_3 v^p = u_7 z_4^p \prod \rho^{v_\rho(2)} = 2u_9 z_4^p$,

where u_6, u_7, u_8, u_9 are units, z_3, z_4 are S-coprime and the products are taken over all $\rho \in S$.

The above two relations give

$2u_3 v^p = (u_7 z_4^p - u_6 z_3^p) \prod \rho^{v_\rho(2)} = 2(u_9 z_4^p - u_8 z_3^p)$, therefore we get

$u_3 v^p = u_9 z_4^p - u_8 z_3^p$, i.e. we get a solution to the Fermat-like equation of section 1.

This completes the proof.

4. FINAL REMARKS

Let E be an elliptic curve satisfying the third equivalent statement of the theorem. Then the above proof of 3 implies 1 gives a solution S of the Fermat-like equation of section 1.

Let E_S be the Frey curve associated to the solution S.

An easy computation shows that the two curves E and E_S have the same j-invariant. Therefore, E and E_S are isomorphic and, in particular, the isomorphism class of E_S does not depend on S.

Moreover, one can show that two solutions of our Fermat-like equation give rise to isomorphic (over $\overline{F}$) Frey curves if and only if they are equivalent. Therefore:

COROLLARY. There is a bijection between the set of equivalence classes of solutions to the Fermat-like equation and the set of isomorphism classes of elliptic curves satisfying statement 3 of the main theorem.

Also, it is easy to see that, under the bijection of the corollary, equivalence classes of trivial solutions correspond to isomorphism classes of elliptic curves satisfying statement 3 and having good reduction outside S. Therefore, using Shafarevich's theorem (see [4]), we get another efficient algorithm for determining all equivalence classes of trivial solutions.

5. ACKNOWLEDGEMENTS

I would like to thank my advisor, Robert F. Coleman, for suggesting the problem as well as for his continuous encouragement. I am also indebted to Hendrik W. Lenstra, Jr., for his valuable advice.

REFERENCES

1. G. FREY, *Links between stable elliptic curves and certain Diophantine equations,* Ann. Univ. Saraviensis, Ser. Math. 1 (1986), 1-40.
2. A. FRÖHLICH and M. J. TAYLOR, *Algebraic number theory,* Cambridge studies in advanced mathematics, 27 (1993).
3. B. GROSS and D. ROHRLICH, *Some Results on the Mordell-Weil Group of the Jacobian of the Fermat Curve,* Inv. Math. 44 (1978), 201-224.
4. J. SILVERMAN, *The arithmetic of elliptic curves,* Springer-Verlag, GTM 106, (1986).

Received March 5, 1994

ON A CONJECTURE OF ZASSENHAUS IN AN ALTERNATIVE SETTING

EDGAR G. GOODAIRE AND CÉSAR POLCINO MILIES
Presented by V. Dlab, F.R.S.C.

ABSTRACT. H. J. Zassenhaus has suggested that every finite subgroup of normalized units in the integral group ring of a finite group G is conjugate to a subgroup of G. While this conjecture has not been settled for group rings, a reformulation within the context of alternative loop rings has recently been established and is discussed here.

1. Introduction. Let $\mathbf{Z}G$ denote the group ring of a finite group G over the integers. What role does G play in determining the torsion units of $\mathbf{Z}G$? H. J. Zassenhaus has conjectured that every normalized unit in $\mathbf{Z}G$ is a conjugate of an element of G via a unit in the rational group algebra $\mathbf{Q}G$. Several years ago the authors established a variation of this result for alternative loop rings. Specifically, we proved

Theorem 1.1. [5, 3] *Let r be a normalized torsion unit in the integral alternative loop ring $\mathbf{Z}L$ of a finite loop L which is not a group. Then there exist units $\gamma_1, \gamma_2 \in \mathbf{Q}L$ and $\ell \in L$ such that $\gamma_2^{-1}(\gamma_1^{-1} r \gamma_1)\gamma_2 = \ell$.*

A second, far stronger conjecture of Zassenhaus says that every finite subgroup of normalized units of $\mathbf{Z}G$ is conjugate to a subgroup of G, via a unit of $\mathbf{Q}G$. Recently, the authors have shown that here too, with some modification, the conjecture is true for alternative loop rings. We have established, and it is our intent to discuss here, the following theorem.

Theorem 1.2. *If H is a finite subloop of normalized units in an alternative loop ring $\mathbf{Z}L$ which is not associative, then H is isomorphic to a subloop of L. Moreover, there exist units $\gamma_1, \gamma_2, \ldots, \gamma_k$ of $\mathbf{Q}L$ such that*

(1) $$\gamma_k^{-1}(\ldots(\gamma_2^{-1}(\gamma_1^{-1} H \gamma_1)\gamma_2)\ldots)\gamma_k \subseteq L.$$

1991 *Mathematics Subject Classification.* Primary 17D05; Secondary 16S34, 20N05.
This research was supported by the Instituto de Matemática e Estatística, Universidade de São Paulo, by FAPESP and CNPq. of Brasil (Proc. No. 93/4440-0 and 501253/91-2, respectively) and by the Natural Sciences and Engineering Research Council of Canada, Grant No. 0GP0009087.

Corollary 1.3. *If H is a finite subloop of normalized units in* $\mathbf{Z}L$, *then* $|H| \leq |L|$. *If* $|H| = |L|$, *then H is isomorphic to L and there exist units* $\gamma_1, \ldots, \gamma_k \in \mathbf{Q}L$ *such that* $L = \gamma_k^{-1}(\ldots(\gamma_2^{-1}(\gamma_1^{-1}H\gamma_1)\gamma_2)\ldots)\gamma_k$.

2. Definitions and Terminology. An *alternative* ring is one which satisfies the left and right alternative laws

$$x(xy) = x^2y \qquad \text{and} \qquad (yx)x = yx^2.$$

Such rings are nearly associative; for example, the subring generated by any two elements is always associative and also, if three elements of an alternative ring associate in some order, then they too generate an associative subring. Composition algebras provide examples of alternative rings, and examples of particular relevance to this work. A *composition algebra* is an algebra A with 1 over a field F on which there is a multiplicative nondegenerate quadratic form $q\colon A \to F$. By *multiplicative*, we mean that $q(xy) = q(x)q(y)$ for all $x, y \in A$. Since alternative rings satisfy the three *Moufang identities*

$$((xy)x)z = x(y(xz)), \qquad ((xy)z)y = x(y(zy)) \quad \text{and} \quad (xy)(zx) = (x(yz))x,$$

the loop of units in an alternative ring is necessarily a *Moufang loop* which is, by definition, a loop in which any of these (equivalent) identities is valid. In particular, if RL is an alternative loop ring for some commutative and associative ring R and loop L, then L is a Moufang loop (of a very special nature). We refer the reader to the book by Zhevlakov, Slin'ko and Shestakov [8] for a treatment of alternative rings and composition algebras, to Pflugfelder's text [7] for an introduction to Moufang loops, and to two papers in the literature [2, 1] for the basic properties of loops which have alternative loop rings.

In an alternative loop ring RL, the map $\epsilon\colon RL \to R$ which sends $\sum \alpha_\ell \ell$ to $\sum \alpha_\ell$ is a homomorphism. Thus $\epsilon(\gamma^{-1}\ell\gamma) = \epsilon(\ell) = 1$ for any $\ell \in L$ and unit γ. So, if we hope to establish (1), it is clear that we must restrict ourselves to subloops H whose elements are *normalized* in the sense that $\epsilon(h) = 1$ for all $h \in H$.

3. Sketch of the Proof of Theorem 1.2. Let H be a finite subloop of normalized units in an alternative loop ring $\mathbf{Z}L$. In a proof of the isomorphism theorem for alternative loop rings over $\mathbf{Z}$ [4], the authors constructed a map ρ from the normalized torsion units of $\mathbf{Z}L$ to L. Restricted to H, this map turns out to be a one-to-one homomorphism, thus H is isomorphic to a subloop of L. What is more difficult is to establish an equation of the form (1). For this, we show that there exist units γ_i in the rational loop algebra $\mathbf{Q}L$ such that

$$(2) \qquad \gamma_k^{-1}(\dots(\gamma_2^{-1}(\gamma_1^{-1}\alpha\gamma_1)\gamma_2)\dots)\gamma_k = \rho(\alpha).$$

for all $\alpha \in H$. We consider the three possibilities: (i) H is an abelian group, (ii) H is a nonabelian group, and (iii) H is a Moufang loop which is not associative.

If H is an abelian group, we show that H is generated by a single element and elements in the centre of $\mathbf{Z}L$ and then appeal to Theorem 1.1. Cases (ii) and (iii) are more delicate. Here we use the fact that the alternative loop algebra $\mathbf{Q}L$ is the direct sum of simple alternative algebras and observe that it is sufficient to establish (2) in each simple component. Since the associative components are fields, as we are able to show, and since the ℓ of Theorem 1.1 is, in fact, $\rho(r)$, each element of H and its image under ρ have equal images in the associative components. Thus we need consider only those components which are not associative.

Now an alternative loop algebra has an involution (anti-automorphism of period 2) $\alpha \mapsto \alpha^*$ such that $\alpha\alpha^*$ is central for any α. From this, one can show that $n(\alpha) = \alpha\alpha^*$ induces a multiplicative quadratic form on each simple component of $\mathbf{Q}L$. This form turns out to be non-degenerate, so each simple component is a composition algebra. Let A be such a component and $\pi\colon \mathbf{Q}L \to A$ be the natural projection. Let $L_0 = \rho(H)$.

If H is not associative, we show that each of $\pi(H)$ and $\pi(L_0)$ generate A and that ρ induces an automorphism of A. By a theorem of Jacobson [6], any automorphism of a composition algebra is the product of *reflections* (maps of the form $x \mapsto \gamma^{-1}x\gamma$), so we have the result in case (iii).

The most difficult case is that in which H is a nonabelian group. Here we let x and y be noncommuting elements of L_0 and let B be the subalgebra of $\mathbf{Q}L$ generated by x and y. Similarly, we consider the subalgebra $\hat{B}$ of $\mathbf{Q}L$ generated by $\hat{x}$ and $\hat{y}$, the preimages under ρ of x and y respectively. It can be shown that $\rho\colon H \to L_0$ extends to a ring isomorphism $\hat{B} \to B$ which induces a ring isomorphism $\pi(\hat{B}) \to \pi(B)$. We show that this map extends to an automorphism of the composition algebra A which, by the theorem of Jacobson already mentioned, is the product of reflections. Thus the proof is complete.

References

1. Orin Chein and Edgar G. Goodaire, *Loops whose loop rings are alternative*, Comm. Algebra 14 (1986), no. 2, 293–310.
2. Edgar G. Goodaire, *Alternative loop rings*, Publ. Math. Debrecen 30 (1983), 31–38.
3. Edgar G. Goodaire and César Polcino Milies, *Isomorphisms and units in alternative loop rings*, C. R. Math. Rep. Acad. Sci. Canada IX (1987), no. 5, 259–263.
4. ———, *Isomorphisms of integral alternative loop rings*, Rend. Circ. Mat. Palermo XXXVII (1988), 126–135.
5. ———, *Torsion units in alternative loop rings*, Proc. Amer. Math. Soc. 107 (1989), 7–15.
6. N. Jacobson, *Composition algebras and their automorphisms*, Rend. Circ. Mat. Palermo VII (1958), 55–80.
7. H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Heldermann Verlag, Berlin, 1990.
8. K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, and A. I. Shirshov, *Rings that are nearly associative*, Academic Press, New York, 1982, Translated by Harry F. Smith.

Memorial University of Newfoundland, St. John's, Newfoundland, Canada A1C 5S7
E-mail address: edgar@morgan.ucs.mun.ca

Universidade de São Paulo, Caixa Postal 20570—Ag. Iguatemi, 01452-990 São Paulo, Brasil
E-mail address: polcino@ime.usp.br

Received March 29, 1994

MINIMUM NUMBER OF STAGES FOR LOW-ORDER EXPLICIT RUNGE–KUTTA–NYSTRÖM PAIRS

Fadi MALEK, P. W. SHARP and Rémi VAILLANCOURT *

Presented by T.E. Hull, F.R.S.C.

Abstract. Second-order initial value problems with the first derivative absent can be solved using explicit Runge–Kutta–Nyström pairs. We report that the minimum number of stages for pairs of order $(p-1, p)$, $p = 4, 5, 6$, is respectively $4, 6, 6$ if the first stage of the next step is as the last stage of the previous step, and $4, 5, 6$ otherwise.

Résumé. Les paires de formules explicites du type Runge–Kutta–Nyström résolvent les équations différentielles du second ordre, où la première dérivée est absente. On montre que le nombre minimum de stages des paires d'ordre $(p-1, p)$, $p = 4, 5, 6$, est respectivement $4, 6, 6$ si le premier stage du pas suivant utilise le dernier stage du pas précédent, sinon ce nombre est $4, 5, 6$.

AMS Subject Classification: 65L05. **CR Categories:** G.1.7

Key words: Ordinary differential equations, special second-order equations, explicit Runge–Kutta–Nyström pairs.

1. Introduction

Explicit Runge–Kutta–Nyström (RKN) pairs are designed to solve directly second-order systems of non-stiff ordinary differential equations of the form

$$y'' = f(x, y), \qquad y(x_0) = y_0, \quad y'(x_0) = y'_0, \tag{1.1}$$

where $f : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ and the first derivative is absent, without reducing (1.1) to a system of first-order equations.

RKN pairs consist of at least three formulae: two formulae of different orders for the solution, y, and one formula for the derivative, y'. The derivative-formula and one of the solution-formulae are used to advance the approximations. The second solution-formula is used to estimate the local error in the solution. Pairs often have a second derivative-formula. This is used to estimate the local error in the derivative.

Pairs with three formulae require fewer stages than pairs with four formulae. However, the numerical testing of Dormand, El-Mikkaway and Prince [1] suggests that the local error in

* Each author was partly supported by the Natural Sciences and Engineering Research Council of Canada. The work of the second and third authors was also partly supported, respectively, by the Information Technology Research Centre of Ontario and the Centre de recherches mathématiques of the Université de Montréal.

the derivative should be controlled to ensure reliability of the pair. Because of this evidence, we report on pairs which use four formulae.

As for Runge–Kutta pairs, RKN pairs are usually derived with as few stages as is practicable. Table 1 lists the previously known or newly found minimum number of stages required for pairs that consist of $(p-1)$st- and pth-order formulae for the solution and derivative (the references for the known results are given in Section 3; the new pairs are listed in the Appendix). The number of stages is listed for two general types of pairs: those that re-use the last stage on the next step, and those that do not. We refer to the first type as $(p-1,p)$F pairs and to the second type as $(p-1,p)$NF pairs. The letter F stands for FSAL (First Same As Last) and NF stands for Non-FSAL.

Table 1. *The minimum number of stages for $(p-1,p)$ pairs, $p=4,5,6$.*

p	4	5	6
$(p-1,p)$NF	4	5	6
$(p-1,p)$F	4	6	6

It is proved in [2] that the number of stages listed in Table 1 is the minimum possible. Proofs are by contradiction. For each value of p it is assumed that a pair exists with one stage fewer than the one given in Table 1. Then it is shown that either the order conditions for the derivative-formulae cannot be satisfied or that the $(p-1)$st- and pth-order derivative-formulae are the same. In this note, we give the proof for the case $(5,6)$.

2. Definitions and order conditions

Explicit Runge–Kutta–Nyström pairs, which use four formulae, generate approximations to $y(x_i)$ and $y'(x_i)$ according to the formulae

$$y_{i+1} = u_i + h_i u_i' + h_i^2 \sum_{j=1}^{s} b_j f_j, \qquad y'_{i+1} = u_i' + h_i \sum_{j=1}^{s} b'_j f_j, \tag{2.1}$$

$$\hat{y}_{i+1} = u_i + h_i u_i' + h_i^2 \sum_{j=1}^{s} \hat{b}_j f_j, \qquad \hat{y}'_{i+1} = u_i' + h_i \sum_{j=1}^{s} \hat{b}'_j f_j, \tag{2.2}$$

where $h_i = x_{i+1} - x_i$ and

$$f_1 = f(x_i, u_i), \quad f_j = f\left(x_i + h_i c_j, u_i + h_i c_j u_i' + h_i^2 \sum_{k=1}^{j-1} a_{jk} f_k\right), \qquad j = 2, \ldots, s.$$

The two formulae in (2.1) are of order p and the two formulae in (2.2) are of order $p-1$. If the numerical approximations are advanced from x_i to x_{i+1} using the order-$(p-1)$ formulae, then $u_i = \hat{y}_i$, $u_i' = \hat{y}_i'$. If the numerical approximations are advanced using the order-p formulae, then $u_i = y_i$, $u_i' = y_i'$.

The order conditions for the $(p-1)$st-order derivative consist of the quadrature conditions

$$\sum_{i=1}^{s} \hat{b}'_i c_i^k = \frac{1}{k+1}, \qquad k = 0, 1, \ldots, p-2, \tag{2.3}$$

and the non-quadrature conditions

$$\sum_{i=1}^{s} \hat{b}'_i S^q_{i,k}(a,c) = 0, \qquad k = 1, \ldots, N_q - 1, \quad q = 1, \ldots, p-1, \tag{2.4}$$

where N_q is the number of order conditions of the order q. The $S^q_{i,k}$ for order conditions up to the order six are listed in Table 2, where repeated j indices imply summation and

$$Q_{i,k} := \frac{c_i^{k+2}}{(k+1)(k+2)} - \sum_{j=1}^{i-1} a_{ij} c_j^k, \qquad i = 2, \ldots, s. \tag{2.5}$$

Table 2. *The $S^q_{i,k}(a,c)$ of orders one through six.*

q	$S^q_{i,k}$			
1, 2, 3	none			
4	Q_{i1}			
5	$c_i Q_{i1}$	Q_{i2}		
6	$c_i^2 Q_{i1}$	$c_i Q_{i2}$	Q_{i3}	$a_{ij} Q_{j1}$

The order conditions for the pth-order derivative-formula consist of the quadrature conditions

$$\sum_{i=1}^{s} b'_i c_i^k = \frac{1}{k+1}, \qquad k = 0, 1, \ldots, p-1, \tag{2.6}$$

and the non-quadrature conditions

$$\sum_{i=1}^{s} b'_i S^q_{i,k}(a,c) = 0, \qquad k = 1, \ldots, N_q - 1, \quad q = 1, \ldots, p. \tag{2.7}$$

For a FSAL pair, c_s must be one, b_s must be zero and

$$a_{s,j} = b_j, \qquad j = 1, \ldots, s-1. \tag{2.8}$$

By the definition of a pth-order solution-formula, the weights b_j, $j = 1, \ldots, s$, satisfy the quadrature conditions

$$\sum_{i=1}^{s} b_i c_i^k = \frac{1}{(k+1)(k+2)}, \qquad k = 0, \ldots, p-2. \tag{2.9}$$

Equations (2.9) then imply that $Q_{s,k} = 0$ for $k = 0, \ldots, p-2$. This means that the non-quadrature order conditions for an s-stage $(p-1,p)$F pair are the same as those for an $(s-1)$-stage $(p-1,p)$NF pair. We use this observation to shorten the non-existence proof for the pairs of order $(4,5)$.

For convenience, we shall take $c_i^0 = 1$ even when $c_i = 0$.

3. Results

Four-stage $(3,4)$F pairs exist (see [3], for example). We state that three-stage $(3,4)$NF pairs do not exist.

THEOREM 1. *No three-stage* $(3,4)$ RKN *pairs exist.*

Six-stage $(4,5)$F pairs exist (see [3], for example). We state that four-stage $(4,5)$NF and five-stage $(4,5)$F pairs do not exist. A new five-stage $(4,5)$NF pair is given in Table A.1 in the Appendix.

THEOREM 2. *No four-stage* $(4,5)$NF *nor five-stage* $(4,5)$F RKN *pairs exist.*

Seven-stage $(5,6)$F pairs exist (see [4] for example). New six-stage $(5,6)$F and NF pairs are given respectively in Tables A.2 and A.3 in the Appendix. We show by contradiction that five-stage $(5,6)$ pairs do not exist. One step in the proof uses Theorem 2.

THEOREM 3. *No five-stage* RKN *pairs of order* $(5,6)$ *exist.*

PROOF. We assume that a pair exists and consider the non-quadrature order conditions $c_i^k Q_{i1}$ in the first column of Table 2, namely

$$(3.1.k) \qquad \hat{b}'_2 c_2^k Q_{21} + \hat{b}'_3 c_3^k Q_{31} + \hat{b}'_4 c_4^k Q_{41} + \hat{b}'_5 c_5^k Q_{51} = 0, \qquad k = 0, 1.$$

$$(3.2.k) \qquad b'_2 c_2^k Q_{21} + b'_3 c_3^k Q_{31} + b'_4 c_4^k Q_{41} + b'_5 c_5^k Q_{51} = 0, \qquad k = 0, 1, 2,$$

If the rank of the coefficient matrix of the four linear equations (3.1.0) and (3.2.0)–(3.2.2) in the four unknowns Q_{i1} is four, we must have $Q_{i1} = 0$, $i = 2, \ldots, 5$. But if $Q_{21} = 0$, then $c_2 = 0$, and the method reduces to a four-stage pair for which we know that such $(4,5)$-pairs do not exist by Theorem 2.

Hence these four equations must be linearly dependent. Thus there exist $\alpha, \beta, \gamma, \delta$, not all zero, such that

$$(3.3.i) \qquad \alpha \hat{b}'_i + \beta b'_i + \gamma b'_i c_i + \delta b'_i c_i^2 = 0, \qquad i = 2, \ldots, 5.$$

Multiplying the ith equation by c_i^k for $k = 1, 2, 3$, and summing over i, we obtain, from the quadrature conditions (2.3) and (2.6), the system

$$(3.4) \qquad \begin{bmatrix} \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \\ \frac{1}{4} & \frac{1}{5} & \frac{1}{6} \end{bmatrix} \begin{bmatrix} \alpha + \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Since the determinant of the coefficient matrix is not zero, this system has the unique solution $(\alpha+\beta,\gamma,\delta)=(0,0,0)$. Hence $\alpha=-\beta\neq 0$, for otherwise no pair exists. However (3.3.i) imply that $b'_i=\hat{b}'_i$, $i=2,\ldots,5$. Thus, by (2.3) and (2.6) with $k=0$, $b'_1=\hat{b}'_1$. Hence no such pair exists. ▮

Appendix

The appendix contains the Butcher tableaus of a five-stage (4,5)NF pair, a six-stage (5,6)F pair and a six-stage (5,6)NF pair. These pairs are not intended to be optimal pairs from each class, but they only confirm the existence of at least one pair with the required number of stages.

Table A.1. A five-stage (4,5)NF pair.

$\frac{1}{6}$	$\frac{1}{72}$				
$\frac{3}{10}$	$\frac{459}{23000}$	$\frac{72}{2875}$			
$\frac{2}{5}$	$\frac{41}{2875}$	$\frac{189}{2875}$	0		
$\frac{2}{3}$	$\frac{1145}{29187}$	$\frac{203}{6486}$	$\frac{385}{2538}$	0	
$\hat{b}$	$-\frac{19}{36}$	$\frac{155}{84}$	$-\frac{35}{36}$	$-\frac{5}{28}$	$\frac{1}{3}$
b	$\frac{17}{18}$	$-\frac{125}{28}$	$\frac{3325}{396}$	$-\frac{275}{56}$	$\frac{47}{88}$
$\hat{b}'$	$-\frac{19}{36}$	$\frac{31}{14}$	$-\frac{25}{18}$	$-\frac{25}{84}$	1
b'	$\frac{17}{18}$	$-\frac{75}{14}$	$\frac{2375}{198}$	$-\frac{1375}{168}$	$\frac{141}{88}$

Table A.2. A six-stage (5,6)F pair. An entry of the form (a,b) represents the algebraic number $a+b\sqrt{5}$.

$\frac{1}{2}$	$\frac{1}{8}$					
1	$\frac{1}{6}$	$\frac{1}{3}$				
$(\frac{1}{2},-\frac{1}{10})$	$(\frac{11}{150},-\frac{1}{50})$	$(\frac{13}{150},-\frac{1}{30})$	$(-\frac{1}{100},\frac{1}{300})$			
$(\frac{1}{2},\frac{1}{10})$	$(\frac{13}{300},\frac{1}{100})$	$(\frac{7}{150},-\frac{1}{150})$	$(\frac{1}{100},-\frac{1}{300})$	$(\frac{1}{20},\frac{1}{20})$		
1	$\frac{1}{12}$	0	0	$(\frac{5}{24},\frac{1}{24})$	$(\frac{5}{24},-\frac{1}{24})$	
$\hat{b}$	$\frac{1}{12}$	0	-2	$(\frac{5}{24},\frac{1}{24})$	$(\frac{5}{24},-\frac{1}{24})$	2
b	$\frac{1}{12}$	0	0	$(\frac{5}{24},\frac{1}{24})$	$(\frac{5}{24},-\frac{1}{24})$	0
$\hat{b}'$	$\frac{1}{12}$	0	$-\frac{11}{12}$	$\frac{5}{12}$	$\frac{5}{12}$	1
b'	$\frac{1}{12}$	0	$(-\frac{1}{6},\frac{1}{20})$	$\frac{5}{12}$	$\frac{5}{12}$	$(\frac{1}{4},-\frac{1}{20})$

Table A.3. A six-stage (5, 6)NF pair. An entry of the form (a, b) represents the algebraic number $a + b\sqrt{5}$.

$\frac{1}{12}$	$\frac{1}{288}$					
$(\frac{1}{2}, \frac{1}{10})$	$(-\frac{1}{4}, -\frac{11}{100})$	$(\frac{2}{5}, \frac{4}{25})$				
1	$(1, -\frac{1}{5})$	$(-\frac{113}{89}, \frac{189}{445})$	$(\frac{137}{178}, -\frac{20}{89})$			
$(\frac{1}{2}, -\frac{1}{10})$	$(\frac{1}{5}, -\frac{1}{25})$	$(-\frac{101}{445}, \frac{139}{2225})$	$(\frac{63}{356}, -\frac{129}{1780})$	0		
$(\frac{1}{2}, \frac{1}{10})$	$(-\frac{13}{48}, -\frac{37}{1200})$	$(-\frac{113}{89}, \frac{189}{445})$	$(\frac{137}{178}, -\frac{20}{89})$	0	$(-\frac{101}{445}, \frac{139}{2225})$	
$\hat{b}$	$\frac{1}{12}$	0	$(\frac{17}{24}, -\frac{17}{120})$	0	$(\frac{5}{24}, \frac{1}{24})$	$(-\frac{1}{2}, \frac{1}{10})$
b	$\frac{1}{12}$	0	$(-\frac{7}{24}, \frac{7}{120})$	0	$(\frac{5}{24}, \frac{1}{24})$	$(\frac{1}{2}, -\frac{1}{10})$
$\hat{b}'$	$\frac{1}{12}$	0	$\frac{17}{12}$	$\frac{1}{12}$	$\frac{5}{12}$	-1
b'	$\frac{1}{12}$	0	$-\frac{7}{12}$	$\frac{1}{12}$	$\frac{5}{12}$	1

REFERENCES

[1] J. R. Dormand, M. E. A. El-Mikkawy and P. J. Prince, *Higher order embedded Runge-Kutta-Nyström formulae*, IMA J. Num. Anal., 8 (1987) 423–430.

[2] F. Malek, *Formules de type Runge-Kutta-Nyström*, M.Sc. Thesis, University of Ottawa, Ottawa, Canada K1N 6N5, 1992.

[3] J. R. Dormand, M. E. A. El-Mikkawy and P. J. Prince, *Families of Runge-Kutta-Nyström formulae*, IMA J. Num. Anal., 8 (1987) 235–250.

[4] D. G. Bettis and M. K. Horn, *Embedded pairs of Runge-Kutta-Nyström algorithms of order two through six*, manuscript, Texas Institute of Computational Mechanics, Univ. of Texas at Austin, 1978.

Department of Computer Science, University of Ottawa, Ottawa, Canada K1N 6N5.
Department of Mathematics and Statistics, New Zealand University, Aukland, New Zealand.
Departments of Computer Science and Mathematics, University of Ottawa, Ottawa, Canada K1N 6N5.

Received April 12, 1994

ON THE DIAMETER OF THE ATTRACTOR OF AN IFS

Serge Dubuc Raouf Hamzaoui

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

Abstract

We investigate methods for the evaluation of the diameter of the attractor of an IFS. We propose an upper bound for the diameter in n-dimensional space. In the case of an affine IFS, we indicate how this upper bound can be calculated.

Key Words: attractors, diameter, fractals.
AMS *Subject Classifications*: 58F12, 28A80

1 Introduction

Apart from its theoretical interest, the evaluation of the diameter of the attractor of an iterated function system (IFS) is useful in many algorithms. Dubuc-Elqortobi [3] have considered adaptive methods to reduce the computations in the deterministic algorithm [1] and Hepting-Prusinkiewicz-Saupe [5] have proposed an algorithm that renders the geometry of the space which contains an attractor characterizing each point according to its distance to the attractor. In these methods it is assumed that the diameter of the attractor or at least an upper bound is known. However, no clue was provided on how to determine this diameter although it is clear that computer graphic tests can lead to good approximations. In this paper, we propose a class of upper bounds for the diameter of the attractor of an IFS in a complete metric space. The existence of a smallest such upper bound is proved in n-dimensional space. If the IFS is affine, we suggest a method which enables us to compute this smallest upper bound. Finally, we show that in a particular case the diameter of the attractor is equal to the diameter of the convex hull of the set of fixed points determined by the IFS.

2 Approximation of the diameter of an IFS

We recall first some basic results of IFS theory. Let (X, d) be a complete metric space. The class of all non-empty closed bounded subsets of X is a complete metric space for the Hausdorff metric h [7]. Given N contractions $f_1, f_2, \ldots, f_N : X \to X$, the finite set $F = \{f_1, f_2, \ldots, f_N\}$ is called an iterated function system or IFS. Let $L(f_i)$ denote the Lipschitz constant of the contraction f_i, $i = 1, 2, \ldots, N$. The following theorem can be found in Hutchinson [6].

Theorem 1 *Let $F = \{f_1, f_2, \ldots, f_N\}$ be an IFS of the complete metric space (X, d). Then there exists a unique non-empty compact set $\mathcal{A}$ called attractor of the IFS such that $\mathcal{A} = F(\mathcal{A}) = \bigcup_{i=1}^{N} f_i(\mathcal{A})$.*

Lemma 2 *Let $F = \{f_1, f_2, \ldots, f_N\}$ be an IFS of the complete metric space (X, d) with attractor $\mathcal{A}$. Let E be a non-empty closed bounded set such that $f_i(E) \subset E$ for each i. Then $\mathcal{A} \subset E$.*

A proof is given in [4].

Proposition 3 *Let $F = \{f_1, f_2, \ldots, f_N\}$ be an IFS of the complete metric space (X, d) with attractor $\mathcal{A}$. Then for any $x \in X$, $\mathcal{A} \subset B(x, r_x)$, where $r_x = \max_{1 \le i \le N} \frac{d(x, f_i(x))}{1 - L(f_i)}$.*

Proof. If x_0 is in the closed ball $B(x, r_x)$, then for every $i \in \{1, 2, \ldots, N\}$, $f_i(x_0) \in B(x, r_x)$. This is a consequence of the following inequalities

$$\begin{aligned} d(f_i(x_0), x) &\le d(f_i(x_0), f_i(x)) + d(f_i(x), x) \\ &\le L(f_i) r_x + d(f_i(x), x) \\ &\le r_x. \end{aligned}$$

Thus, $f_i\{B(x, r_x)\} \subset B(x, r_x)$ which implies that $\mathcal{A} \subset B(x, r_x)$ by Lemma 2. □

Proposition 4 *Let $F = \{f_1, f_2, \ldots, f_N\}$ be an IFS of $(\mathbb{R}^n, d)$. We define $\Phi : \mathbb{R}^n \to \mathbb{R}$ by $\Phi(x) = r_x$. Then Φ is continuous and has a global minimum.*

Proof. Φ is clearly continuous. Let Ω_1 be the fixed point of f_1. For each x not contained in $B(\Omega_1, r_{\Omega_1})$

$$\begin{aligned} \Phi(\Omega_1) &< d(x, \Omega_1) && (1) \\ &\leq \Phi(x), && (2) \end{aligned}$$

where the inequality (2) is justified by the fact that $\Omega_1 \in \mathcal{A} \subset B(x, r_x)$. Since Φ is continuous on the compact $B(\Omega_1, r_{\Omega_1})$, it reaches on this set a lower bound which is also the global minimum due to (2). □

We deduce from Proposition 4 that from all balls $B(x, r_x)$ that contain the attractor, there is at least one with smallest diameter. This diameter is our best upper bound for the diameter of the attractor.

From now on we shall consider only affine IFSs of n-dimensional space, i.e., IFSs such that the contractions are affine transformations of $\mathbb{R}^n$.

What can be said about the nature of the set of points at which the minimum of the function Φ is reached ?

Proposition 5 *The set of solutions of the minimization problem* $\inf_{u\in\mathbb{R}^n} \Phi(u)$ *is a closed convex set and consists of a unique point if the function* Φ *is strictly convex over* $\mathbb{R}^n$.

Proof. We note first that Φ is convex. This results from the convexity of each function $x \to \frac{d(x, f_i(x))}{1-L(f_i)}$ which is clear since

$$\begin{aligned} d(x, f_i(x)) &= \|x - f_i(x)\| && (3) \\ &= \|A_i x + B_i\|, && (4) \end{aligned}$$

where A_i is a linear map and B_i is a vector. Let S be the set of solutions of the minimization problem $\inf_{u\in\mathbb{R}^n} \Phi(u)$. We know from Proposition 4 that $S \neq \emptyset$. Moreover, S is closed since Φ is continuous. If both x and y attain $m = \inf_{u\in\mathbb{R}^n} \Phi(u)$, then

$$m \leq \Phi(\lambda x + (1-\lambda)y) \leq \lambda\Phi(x) + (1-\lambda)\Phi(y) = m, \quad (5)$$

so $\lambda x + (1-\lambda)y$ also attains m. Hence S is convex. Now if Φ is strictly convex and $x \neq y$, then for $\lambda = 1/2$ the second inequality in (5) is strict and leads to the contradiction $m < m$. □

Let us see how to approximate the diameter of an attractor in Euclidean space. We will consider two approaches. The first one is experimental. It consists of drawing an approximation of the attractor and the assumption that the diameter of the obtained set is a good evaluation of the real diameter. This is motivated by the following proposition.

Proposition 6 *Let $F = \{f_1, f_2, \dots, f_N\}$ be an IFS with attractor A. Then for any non-empty bounded set E*

$$|\delta(A) - \delta(F^n(E))| \leq 2\frac{L^n}{1-L}h(E, F(E))$$

where $L = \max_{1\leq i\leq N} L(f_i)$.[1]

Proof. This is an immediate consequence of a result in Berger [2] which states that the function diameter is Lipschitz with constant 2. □

The second approach is to compute the minimum of the function Φ. We explain in an example how this can be done. The dragon is the attractor of the IFS $\{f_1, f_2\}$, where $f_1(x,y) = (1/2x + 1/2y, -1/2x + 1/2y)$ and $f_2(x,y) = (-1/2x + 1/2y + 1, -1/2x - 1/2y)$. For a given point $u(x,y)$ we determine the value of $\Phi(u) = \max_{1\leq i\leq 2} \frac{d(u, f_i(u))}{1-L(f_i)}$. We know that $L(f_i) = \sqrt{\max_{1\leq j\leq 2} \lambda_j}$, where the $\lambda_j s$ are the eigenvalues of $A_i^T A_i$ and A_i is the matrix associated to f_i. Thus $L(f_1) = L(f_2) = \sqrt{2}/2$. By comparing $d(u, f_1(u))$ and $d(u, f_2(u))$ we find that

$$\Phi(u) = \begin{cases} \frac{d(u,f_1(u))}{1-\sqrt{2}/2} & \text{if } (x-3/4)^2 + (y+1/4)^2 \leq 1/8 \\ \frac{d(u,f_2(u))}{1-\sqrt{2}/2} & \text{otherwise} \end{cases}$$

Instead of the minimization problem $\inf_{u\in R^2} \Phi(u)$, we can consider the equivalent one $\inf_{u\in R^2} \Phi^2(u)$. The function Φ^2 has no critical points inside or outside the circle defined by the equation $(x-3/4)^2 + (y+1/4)^2 = 1/8$. On the circle the critical points are solutions of the Lagrangian system

$$\begin{cases} \frac{\partial F(x,y)}{\partial x} = 0 \\ \frac{\partial F(x,y)}{\partial y} = 0 \\ (x-3/4)^2 + (y+1/4)^2 = 1/8 \end{cases}$$

where $F(x,y) = x^2/2 + y^2/2 - \lambda\{(x-3/4)^2 + (y+1/4)^2 - 1/8\}$. These solutions are $x = 3(\sqrt{5}/20 + 1/4)$, $y = -(\sqrt{5}/20 + 1/4)$ and $x = -3(\sqrt{5}/20 - 1/4)$, $y = (\sqrt{5}/20 - 1/4)$. By comparing the value of Φ at these points we deduce that $\inf_{u\in R^2} \Phi(u) = \frac{(\sqrt{5}-1)/4}{1-\sqrt{2}/2}$. Thus the diameter of the dragon is less than $\frac{\sqrt{5}-1}{2-\sqrt{2}}$.
In the general case and for an IFS $F = \{f_1, f_2, \dots, f_N\}$, we determine the N domains

[1] We recall that h is the Hausdorff metric. By $\delta(A)$ we denote the diameter of a set A.

$D_1, D_2, \ldots, D_N$ defined by

$$D_i \begin{cases} \frac{d(u,f_i(u))}{1-L(f_i)} \geq \frac{d(u,f_1(u))}{1-L(f_1)} \\ \frac{d(u,f_i(u))}{1-L(f_i)} \geq \frac{d(u,f_2(u))}{1-L(f_2)} \\ \ldots \\ \frac{d(u,f_i(u))}{1-L(f_i)} \geq \frac{d(u,f_{i-1}(u))}{1-L(f_{i-1})} \\ \ldots \\ \frac{d(u,f_i(u))}{1-L(f_i)} \geq \frac{d(u,f_N(u))}{1-L(f_N)} \end{cases}$$

The function $\Phi(u)$ is equal to $\frac{d(u,f_i(u))}{1-L(f_i)}$ on D_i. We find the critical points of $\Phi^2(u)$ which is a differentiable function on every D_i. The study is made separately in the interior and on the boundary of D_i. We calculate the value of Φ at the critical points and retain those that minimize Φ.

The following proposition says that there is a special case where the diameter of the attractor is equal to the diameter of a finite set.

Proposition 7 *Let $F = \{f_1, f_2, \ldots, f_N\}$ be an affine IFS with attractor $\mathcal{A}$. Let Ω_i denote the fixed point of f_i, and let $\mathcal{O}$ be the convex hull of $\{\Omega_1, \Omega_2, \ldots, \Omega_N\}$. If $f_j(\Omega_i) \in \mathcal{O}$ for all $i, j \in \{1, 2, \ldots, N\}$, then the diameter of $\mathcal{A}$ is equal to the diameter of $\mathcal{O}$.*

Proof. Since all the fixed points Ω_i are contained in the attractor, we have $\delta(\mathcal{O}) \leq \delta(\mathcal{A})$. The condition $f_j(\Omega_i) \in \mathcal{O}$ implies that $f_j(\mathcal{O}) \subset \mathcal{O}$. Thus $\mathcal{A} \subset \mathcal{O}$ which shows that $\delta(\mathcal{O}) \geq \delta(\mathcal{A})$. □

Example *The diameter of the Sierpinski gasket is equal to the diameter of the triangle whose vertices are the fixed points of the three contractions.*

The computation of the diameter of a finite set in Euclidean space is a common problem in computational geometry. Efficient algorithms are given in Preparata and Shamos [8].

Acknowledgement. The authors are grateful to the referee for his comments on the proof of Proposition 5 and to Dr. Amitava Datta for proof reading the manuscript. The second author would like to thank Prof. Dietmar Saupe for helpful discussions.

References

[1] Barnsley, M. F., *Fractals Everywhere*, Academic Press, San Diego, 1988.

[2] Berger, M. , *Géométrie,* Vol 2, Nathan, Paris Cedic, 1977.

[3] Dubuc, S. and Elqortobi, A., *Approximations of fractal sets,* J. Comput. Appl. Math. 29 (1990) 79-89.

[4] Hamzaoui, R., *Représentations graphiques relatives aux systèmes de fonctions itérées du plan,* M. Sc. Thesis, University of Montreal, 1993.

[5] Hepting, D., Prusinkiewicz, P. and Saupe, D., *Rendering methods for iterated function systems,* in: *Fractals in the Fundamental and Applied Sciences,* H.-O. Peitgen, J. M. Henriques, L. Peneda (eds.), North-Holland, Amsterdam, 1991.

[6] Hutchinson, J., *Fractals and self-similarity,* Indiana Univ. Math. J. 30 (1981) 713-747.

[7] Kuratowski, K., *Topology,* Vol 1, Academic Press, New York, 1966.

[8] Preparata, F. P. and Shamos, M. I., *Computational Geometry: An Introduction,* Springer-Verlag, New York, 1985.

S. Dubuc: Département de mathématiques et de statistique, Université de Montréal, C. P. 6128, Montréal, Québec, H3C 3J7, Canada

R. Hamzaoui: Institut für Informatik, Universität Freiburg, Rheinstr. 10-12, 79104 Freiburg, Germany

Received April 13, 1994

ASYMPTOTIC BEHAVIOR OF THE DAVEY–STEWARTSON SYSTEM

Marisela Guzmán-Gómez

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

Abstract: This paper is devoted to the study of the asymptotic behavior of the Davey–Stewartson system that models gravity-capillary waves.

1. Introduction

We consider the initial value problem for the Davey–Stewartson system (DSS):

$$iu_t + \delta u_{xx} + u_{yy} = \lambda |u|^2 u + bu\varphi_x, \quad t \in \mathbb{R}, \quad (x,y) \in \mathbb{R}^2, \tag{1.1$_a$}$$

$$\varphi_{xx} + m\varphi_{yy} = \frac{\partial}{\partial x}(|u|^2), \tag{1.1$_b$}$$

with the initial condition

$$u(x,y,0) = u_0(x,y). \tag{1.1$_c$}$$

The Davey–Stewartson system appears as envelope equations in modulation of water waves at the surface of a three dimensional flow [1,2,3]. The parameters δ, λ, b and m depend on the fluid depth, surface tension, gravity and wavenumber and can assume both signs; δ and λ can be normalized such that $|\delta| = |\lambda| = 1$. The boundary conditions depend on the sign of m. For $m > 0$, u and φ vanish at infinity while for $m < 0$, the boundary conditions are of radiation type.

A detailed discussion of the well posedness or finite time blow-up for DSS according to the values of the parameters is presented in Ghidaglia & Saut [4].

The purpose of this paper is to study the asymptotic behavior of global solutions of DSS and to prove that when $t \to \pm\infty$ u tends to a solution of the associated linear equation and φ tends to 0. For certain values of the parameters we also show the existence of the scattering operators $\Omega_+ : u_+ \to u_-$ and $\Omega_- : u_- \to u_+$, as bijections of the Hilbert space $\Sigma = \{v \in L^2(\mathbb{R}^2) : \|v\|_2 + \|Dv\|_2 + \|xv\|_2 < \infty\}$ or of a neighborhood of zero in $L^2(\mathbb{R}^2)$.

A large amount of literature has been devoted to the study of the scattering theory of the Nonlinear Schrödinger equation (NLS) with power nonlinearity $|u|^{p-1}u$ in $\mathbb{R}^n$. We refer to [6] for complete references. In [5] Ginibre & Velo proved the existence of the scattering operator for NLS equation in Σ with $\lambda \geq 0$ and $1 + \frac{4}{n} < p < 1 + \frac{2}{n-2}$. When $\frac{n+2+\sqrt{n^2+12n+4}}{2n} < p \leq 1 + \frac{4}{n}$ the construction of the scattering operator in a neighborhood of zero in $H^1(\mathbb{R}^2)$ was studied by Strauss [8] and in general by Tsutsumi [11]. For $p > 1 + \frac{2}{n}$ Tsutsumi and Yajma [10] proved asymptotic freedom of NLS equation in $L^2(\mathbb{R}^2)$ for initial conditions in Σ.

In this paper we obtain similar results for DSS. The study is based on the invariance of the system under some transformations. We use this idea not only when $\delta = 1$ and $m > 0$ where it is a simple consequence once solutions in $C(\mathbb{R},\Sigma)$ are established, but also when $\delta=1$ and $m<0$ where only weak solutions are obtained and for solutions in $C(\mathbb{R},L^2(\mathbb{R}^2))$ when $\delta=-1$ and $m>0$. Decay of solutions of DSS has been studied by Tsutsumi [9] who constructs weak solutions of DSS that decay in L^p.

2. Notation and Basic Results

$W^{m,p}(\mathbb{R}^2)$ denote the Sobolev Space of functions equipped with the usual norm: $\|u\|_{m,p}=(\Sigma_{0\le|k|\le m}\int|D^k u|^p)^{1/p}$ and $H^s(\mathbb{R}^2)=W^{s,2}(\mathbb{R}^2)$, $\|u\|_p=\|u\|_{L^p}$, $\|v\|_\Sigma^2=\|v\|_2^2+\|\nabla v\|_2^2+\|xv\|_2^2$. $H^1_w(\mathbb{R}^2)$ refers to $H^1(\mathbb{R}^2)$ endowed with its weak topology; $C_b(\mathbb{R}^2)$ is the set of bounded continuous functions.

The system can be classified as elliptic–elliptic, elliptic–hyperbolic, hyperbolic–elliptic and hyperbolic–hyperbolic according to the respective signs of (δ,m): $(+,+)$, $(+,-)$, $(-,+)$, $(-,-)$. We first recall some results due to Ghidaglia & Saut [4] concerning existence of global solutions.

If any one of the following hypotheses $(h1)$, $(h2)$, or $(h3)$ is satisfied there exists a global solution (u,φ) of (1.1):

a) $u_0\in H^1(\mathbb{R}^2)$, $m>0$, $\delta=1$ and $\lambda\ge max\{-b,0\}$ $\quad(h1)$

b) $u_0\in H^1(\mathbb{R}^2)$, $m<0$, $\delta=1$ and $\left[\frac{2|b|}{\sqrt{-m}}+max\{-\lambda,0\}\right]\|u_0\|_2^2<1$ $\quad(h2)$

c) $u_0\in L^2(\mathbb{R}^2)$, $m>0$ and $\|u_0\|_2$ "small enough" $\quad(h3)$

Under hypothesis $(h1)$, the solution is unique with u and $\nabla\varphi\in C(\mathbb{R},H^1(\mathbb{R}^2))$; if $(h2)$ is true, $u\in C(\mathbb{R},H^1_w(\mathbb{R}^2))$ and $\varphi\in L^\infty(\mathbb{R},C_b(\mathbb{R}^2))$; when $(h3)$ is satisfied the solution is unique with u and $\nabla\varphi\in C(\mathbb{R},L^2(\mathbb{R}^2))$. In all the above solutions the mass is conserved, $\|u(t)\|_2=\|u_0\|_2$, while the energy $\mathcal{E}=\int\{\delta|u_x|^2+|u_y|^2+\frac{\lambda}{2}|u|^4+\frac{b}{2}(\varphi_x^2+m\varphi_y^2)\}\,dxdy$ is conserved by solutions of DSS that satisfy $(h1)$. Under hypothesis $(h2)$ one can construct weak solutions such that the inequality $\mathcal{E}(t)\le\mathcal{E}(0)$ is verified.

Under hypothesis $(h1)$ or $(h2)$ and if the solution satisfies the inequality $\mathcal{E}(t)\le\mathcal{E}(0)$ then $\|\nabla u(t)\|_2$ is bounded.

We also have :

$$\int\{\varphi_x^2+m\varphi_y^2\}dxdy\le\|u\|_4^4,\quad \text{if}\quad m>0 \tag{2.1}$$

$$\left|\int\{\varphi_x^2+m\varphi_y^2\}dxdy\right|\le\frac{1}{2\sqrt{-m}}\||u|_x^2\|_1^2\quad\text{and}\quad\|\varphi\|_\infty\le\||u|_x^2\|_1^2\quad\text{if}\quad m<0. \tag{2.2}$$

If $m>0$, DSS is equivalent to the integral equation $u(t)=S(t)u_0-i\int S(t-\tau)F(\tau)d\tau$ where $S(t)$ stands for the evolution operator of the linear equation $iu_t+\delta u_{xx}+u_{yy}=0$ given by $S(t)=\frac{1}{it}e^{i(\delta x^2+y^2/4t)}$, $F(v)=\lambda|v|^2v+bvK(|v|^2)$ and K the integral operator that solves $\varphi_x=K(|u|^2)$ from $(1.1)_b$.

In the next section we study the long time behavior of global solutions of DSS.

3. Asymptotic Behavior of Solutions with data in Σ and $L^2(\mathbb{R}^2)$.

Theorem 3.1. *Let m, δ and λ be as in $(h1)$.*

a) For initial condition $u_0 \in \Sigma$, there exist unique scattering states $u_\pm \in \Sigma$ such that the solution (u,φ) of (1.1) satifies:

$$\|u_\pm - S(-t)u(t)\|_\Sigma \to 0, \quad \|\nabla\varphi(t)\|_2 \to 0 \quad as \quad t \to \pm\infty \tag{3.1}$$

and for any $p > 2$ there exists a positive constant C_p such that:

$$\|u(t)\|_p \le C_p t^{\frac{2}{p}-1}. \tag{3.2}$$

b) For any $u_+ \in \Sigma$, there exists a unique $u_0 \in \Sigma$ such that the solution (u,φ) of (1.1) satisfies

$$\|u_+ - S(-t)u(t)\|_\Sigma \to 0 \quad and \quad \|\nabla\varphi(t)\|_2 \to 0 \quad as \quad t \to +\infty. \tag{3.3}$$

c) For any $u_- \in \Sigma$, there exists a unique $u_0 \in \Sigma$ such that the solution (u,φ) of (1.1) satisfies

$$\|u_- - S(-t)u(t)\|_\Sigma \to 0 \quad and \quad \|\nabla\varphi(t)\|_2 \to 0 \quad as \quad t \to -\infty. \tag{3.4}$$

Theorem 3.2. *Let m, δ, λ and u_0 as $(h2)$. If $u_0 \in \Sigma$ there exist scattering states $u_\pm \in L^2(\mathbb{R}^2)$ such that a solution (u,φ) of (1.1) satisfies*

$$\|u_\pm - S(-t)u(t)\|_2 \to 0 \quad and \quad \|\varphi(t)\|_\infty \to 0 \quad as \quad t \to \pm\infty \tag{3.5}$$

and for any $p > 2$ there exists a positive constant C_p such that (3.2) is satisfied.

Theorem 3.3. *Let $m > 0$.*

a) There exists $\epsilon > 0$ such that if $\|u_0\|_2 < \epsilon$ there are scattering states $u_\pm \in L^2(\mathbb{R}^2)$ with $\|u_\pm\|_2 < \epsilon$ such that the solution (u,φ) of (1.1) satisfies $\lim_{t \to \pm\infty} \|u(t) - S(t)u_\pm\|_2 = 0$.

b) There exists $\epsilon > 0$ such that given a scattering state $u_+ \in L^2(\mathbb{R}^2)$ with $\|u_+\|_2 < \epsilon$ there exists a unique initial condition $u_0 \in L^2(\mathbb{R}^2)$ with $\|u_0\|_2 < \epsilon$ such that the solution (u,φ) satisfies $\lim_{t\to+\infty} \|u(t) - S(t)u_+\|_2 = 0$.

c) There exists $\epsilon > 0$ such that given a scattering state $u_- \in L^2(\mathbb{R}^2)$ with $\|u_-\|_2 < \epsilon$ there exists a unique initial condition $u_0 \in L^2(\mathbb{R}^2)$ with $\|u_0\|_2 < \epsilon$ such that the solution (u,φ) satisfies $\lim_{t\to-\infty} \|u(t) - S(t)u_-\|_2 = 0$.

Remark. Theorem 3.1b) and c) imply that the wave operators $W_\pm : u_\pm \to u_0$ are well defined as mappings from Σ to Σ. Theorem 3.1a) implies that $W_\pm$ are one-to-one and onto and one can construct the scattering operator $W_+^{-1}W_- : u_- \to u_+$ in the elliptic-elliptic case; similarly theorem 3.3 implies the existence of the scattering operator in a neighborhood of zero in $L^2(\mathbb{R}^2)$ in the hyperbolic-elliptic and elliptic-elliptic cases.

We will use the invariance of DSS under the transformations:

$$\mathcal{T}(u,\varphi)=(v,\psi) \quad \text{with} \quad u(x,y,t)=\frac{1}{2it}e^{i(\delta x^2+y^2)/4t}\overline{v}\left(\frac{x}{2t},\frac{y}{2t},\frac{1}{4t}\right), \varphi(x,y,t)=\frac{1}{2t}\psi\left(\frac{x}{2t},\frac{y}{2t},\frac{1}{4t}\right);$$

$$\mathcal{F}_{t_0}(u(x,y,t),\varphi(x,y,t))=(u(x,y,t+t_0),\varphi(x,y,t+t_0))$$

i.e if (u,φ) satisfies DSS, (v,ψ) also satisfies DSS with the new variables $X=\frac{x}{2t}$, $Y=\frac{y}{2t}$, $T=\frac{1}{4t}$. Note that $\mathcal{T}^2=\text{Id}$.

Lemma 3.1. Let $(v,\psi)=\mathcal{T}(u,\varphi)$, X=(X,Y), x=(x,y).

$$a) \quad \|v(T)\|_2=\|u(t)\|_2 \tag{3.6}$$

$$b) \quad \|\nabla v(T)\|_2=\|\mathbf{x}S(-t)u(t)\|_2=\|\mathbf{x}u(t)+2it\nabla u(t)\|_2 \tag{3.7}$$

$$c) \quad \|\mathbf{X}v(T)+2iT\nabla V(T)\|_2=\|\nabla u(t)\|_2 \tag{3.8}$$

$$d) \quad \|v(T)\|_p=t^{1-\frac{2}{p}}\|u(t)\|_p \tag{3.9}$$

$$e) \quad \|\psi_X\|_2^2=16t^4\|\varphi_x\|_2^2. \tag{3.10}$$

The proof is a direct consequence of the definition of the transformation $\mathcal{T}$.

Proposition 3.1. If u_0, m, λ and b are as in $(h1)$, with in addition $u_0\in\Sigma$, then (u,φ) solution of (1.1) satisfies $u\in C(\mathbb{R},\Sigma)$.

Proof: Let (u,φ) the unique solution of (1.1), take $v(x,y,1/2)=-ie^{i(\delta x^2+y^2)/2}\overline{u}_o(x,y)$ as the initial condition and get (v,ψ) the solution of DSS with $v\in C(\mathbb{R},H^1(\mathbb{R}^2))$. Let $(U,\eta)=\mathcal{T}(v,\psi)$; by uniqueness of solutions of DSS, $u(x,y,t)=U(x,y,t+1/2)$. All of these solutions satisfy the conservation of the energy.

Then by (3.8),(3.9) and (3.10), (U,η) satisfies the pseudo-conformal equality:

$$\|\mathbf{x}U(x,y,t)+2it\nabla U(t)\|_2^2+\frac{\lambda}{2}t^2\|U(t)\|_4^4+8bt^4\int(\eta_x^2+m\eta_y^2)=\text{constant} \tag{3.11}$$

then U and u belongs to $C(\mathbb{R},\Sigma)$. ∎

Proof of theorem 3.1a):

Let us prove (3.1) when $t\to+\infty$ (the case $t\to-\infty$ is identical). Let (u,φ) the unique solution of (1.1) in $C(\mathbb{R},\Sigma)$ and (v,ψ) the solution of DSS with initial condition at $t=1/2$ defined by $v(x,y,1/2)=\mathcal{T}(u(x,y,1/2))$; $v\in C(\mathbb{R},\Sigma)$, then $v(0)=v_0\in\Sigma$ and $\lim_{T\to0}\|v(T)-v_0\|_\Sigma=0$. By uniqueness $(v,\psi)=\mathcal{T}(u,\varphi)$. The solution of the linear Schrödinger equation $S(T)v_0$ satisfies $\lim_{T\to0}\|S(T)v_0-v_0\|_\Sigma=0$, thus $\lim_{T\to0}\|v(T)-S(T)v_0\|_\Sigma=0$.

Let $w(t)=\mathcal{T}(S(T)v_0)$; $w(t)$ is also solution of the linear Schrödinger equation. Thus $w(t)=S(t)w(0)$ with $w(0)\in\Sigma$. By (3.6), (3.7), (3.8) :

$$\|u(t)-w(t)\|_2=\|v(T)-S(T)v_0\|_2,$$

$$\|\nabla u(t)-\nabla w(t)\|_2\le T\|\nabla v(T)-\nabla S(T)v_0\|_2+\|\mathbf{X}v(T)-\mathbf{X}S(T)v_0\|_2,$$

$$\|xS(-t)(u(t)-w(t))\|_2 = \|\nabla(v(T)-S(T)v_0)\|_2,$$

then $\|S(-t)(u(t)-w(t))\|_\Sigma \leq \|v(T)-S(T)v_0\|_\Sigma$ because $S(t)$ is unitary in $H^1(\mathbb{R}^2)$. Define $u_+ = w(0)$; $u_+ \in \Sigma$ is the scattering state satisfying (3.1).

Using the conservation of the energy, $\|v(T)\|_{H^1}$ remains bounded. By (3.9) and Sobolev embedding theorem $L^p(\mathbb{R}^2) \subset H^1(\mathbb{R}^2)$ for $p > 2$, then:

$$\|u(t)\|_p = t^{\frac{2}{p}-1}\|v(T)\|_p \leq C_p t^{\frac{2}{p}-1}\|v(T)\|_{H^1} \leq C_p t^{\frac{2}{p}-1}.$$

Estimate (3.2) follows; (2.1) and (3.2) imply that:

$$\|\nabla\varphi(t)\|_2^2 \leq \|u\|_4^2 \leq C(1+t)^{-1}. \quad \blacksquare$$

Proof of Theorem 3.1b):

Given $u_+ \in \Sigma$, define $v_+(T) = \mathcal{T}(S(t)u_+)$; $S(t)u_+$ as well as $v_+(T)$ is a solution of the linear Schrödinger equation, let $v(T)$ be the solution of DSS with initial condition $v_+(0) \in \Sigma$; then $v(T)$ and $v_+(T)$ are in $C(\mathbb{R},\Sigma)$ and

$$\|v(T)-v_+(T)\|_\Sigma \leq \|v(T)-v_+(0)\|_\Sigma + \|v_+(T)-v_+(0)\|_\Sigma,$$

therefore $\lim_{T\to 0^+}\|v(T)-v_+(T)\|_\Sigma = 0.$

Define $u_{1/2} = \mathcal{T}^{-1}(v(1/2))$, $u_{1/2} \in \Sigma$ and there exists (u,φ) that satisfies DSS with $u(1/2) = u_{1/2}$. $u_0 = u(0)$ is the desired initial condition. By lemma 3.1, $\|S(-t)u(t)-u_+\|_\Sigma \leq \|v(T)-v_+(T)\|_\Sigma$, then (3.3) is obtained. $\blacksquare$

Proof of theorem 3.2:

If $u_0 \in \Sigma$, m, λ and b are as in $(h2)$ take $v(x,y,1/2) = -ie^{i(x^2+y^2)/2}\overline{u}_0(x,y)$ as the initial condition and get $(v(x,y,t),\psi(x,y,t))$ a global weak solution of DSS with $v \in C(\mathbb{R},H^1_\omega(\mathbb{R}^2))$ and $\psi \in L^\infty(\mathbb{R},C_b(\mathbb{R}^2))$ that satisfy:

$$\|\nabla v(t)\|_2^2 + \frac{\lambda}{2}\|v(t)\|_4^4 + \frac{b}{2}\left\{\int \psi_x^2 + m\psi_y^2\right\} \leq \mathcal{E}(1/2) \tag{3.11}$$

Let $(U,\eta) = \mathcal{T}(v,\psi)$ and $(u,\varphi) = \mathcal{F}_{1/2}(U,\eta)$ defined for $t \geq 0$, then (u,φ) is also a solution of DSS and $u(x,y,0) = U(x,y,1/2) = \mathcal{T}(v(x,y,1/2)) = u_0$.

$v \in C(\mathbb{R}_+,H^1_\omega(\mathbb{R}^2))$ implies that $v(T) \to v_0$ as $T \to 0^+$ with respect to the weak* topology of $H^1(\mathbb{R}^2)$, i.e., for any $\mathcal{G} \in H^{-1}(\mathbb{R}^2)$, $\mathcal{G}(v(T)) \to \mathcal{G}(v_0)$, as $T \to 0^+$.

Now, define $\mathcal{G}_f(g) = \langle g,f\rangle\ \forall g \in H^1(\mathbb{R}^2)$, where $\langle\ ,\ \rangle$ is the usual inner product in $L^2(\mathbb{R}^2)$, then:

$$\lim_{T\to 0^+}\mathcal{G}_f(v(T)) = \mathcal{G}_f(v_0) \qquad \forall\ f \in H^1(\mathbb{R}^2)$$

equivalently,

$$\lim_{T\to 0^+}\langle v(T),f\rangle = \langle v_0,f\rangle \qquad \forall f \in H^1(\mathbb{R}^2).$$

Let $\mathcal{P}$ be the linear operator $\mathcal{P} : H^1(\mathbb{R}^2) \to \mathbb{C}$ defined by $\mathcal{P}(f) = \lim_{T\to 0^+}\langle v(T), f\rangle$. $\mathcal{P}$ is a bounded linear operator from a dense subspace of $L^2(\mathbb{R}^2)$, therefore it can be extended to $L^2(\mathbb{R}^2)$ and

$$\lim_{T\to 0^+}\langle v(T), f\rangle = \langle v_0, f\rangle \qquad \forall f \in L^2(\mathbb{R}^2).$$

Also, $\lim_{T\to 0^+}\|v(T)\|_2 = \|v_0\|_2$ and thus $\lim_{T\to 0^+}\|v(T) - v_0\|_2 = 0$.

Define $U_+(t) = \mathcal{T}(S(T)v_0)$, then $U_+(t) = S(t)U_+(0)$ and by (3.6) :

$$\|U(t) - U_+(t)\|_2 = \lim_{T\to 0^+}\|v(T) - S(T)v_0\|_2 \le \|v(T) - v_0\|_2 + \|v_0 - S(T)v_0\|_2 \to 0 \quad \text{when} \quad T \to 0^+.$$

Let $u_+ = S(1/2)U_+(0)$, then

$$\lim_{t\to+\infty}\|u(t) - S(t)u_+\|_2 = \lim_{t\to+\infty}\|u(t-1/2) - S(t-1/2)u_+\|_2$$
$$= \lim_{t\to+\infty}\|U(t) - S(t)U_+(0)\|_2 = 0.$$

Inequality (2.2) together with the Cauchy-Schwartz inequality and (3.11) imply that when $t \to +\infty$:

$$\|\varphi(t)\|_\infty \le C\frac{1}{t}\|\psi(T)\|_\infty \le C\frac{1}{t}\||v|_x^2\|_1^2 \le C_1\frac{1}{t}\|v(T)\|_2^2\|\nabla v(T)\|_2^2 \le \frac{C_2}{t}. \quad ∎$$

The proof of theorem 3.3 is similar to that of theorem 3.1.

References

[1] Ablowitz, M.J. & Segur, H., *J.Fluid Mech.* ,92(1979), 691-715.
[2] Davey, A. & Stewartson, K., *Proc. Roy. Soc. A.* ,388 (1974), 101-110.
[3] Djordjevic, V.D. & Redekopp, L.G., *J.Fluid Mech.* ,79(1977), 703-714.
[4] Ghidaglia, J.M. & Saut, J.C., *Nonlinearity* , 3(1990), 475-506.
[5] Ginibre, J., & Velo, G., *J. Funct. Anal.* 32(1979), 1-71.
[6] Ginibre, J., Ozawa, T., *Commun. Math. Phys.* ,151(1993), 619-645.
[8] Strauss, W., *J. Funct. Anal.*,41(1981), 110-133.
[9] Tsutsumi, M., Decaying of weak solutions to the Davey-Stewartson System *(preprint).*
[10] Tsutsumi, Y.,& Yajma, K., *Bull. of the Am. Math. Soc.* ,11(1984), 186-188.
[11] Tsutsumi, Y., *Ann. Inst. Henri Poincaré*, 43(1985), 321-347.

Department of Mathematics
University of Toronto
Toronto, Ont., CAN. M5S 1A1

Received May 11, 1994

SOME PROPERTIES OF α-BLOCH FUNCTIONS

LOU ZENGJIAN

ABSTRACT. We give the continuity of B^α and B_0^α, predual space of B^α, also a new characterisation of B^α and B_0^α which are real extensions for ones of B and B_0.

Presented by P.G. Rooney, F.R.S.C.

1. Introduction

Let $D = \{z : |z| < 1\}$ denote the open unit disc in the complex plane. For an analytic function f on $D(f \in H(D))$, $0 \le \alpha < \infty$. The α-Bloch space B^α is the set of all functions $f \in H(D)$ for which

$$\sup_z (1 - |z|^2)^\alpha |f'(z)| < \infty$$

little α-Bloch space, B_0^α, consists of all functions $f \in H(D)$ for which

$$\lim_{|z|\to 1} (1 - |z|^2)^\alpha |f'(z)| = 0$$

It is known that B^α is a Banach space under the norm $|f(0)| + \|f\|_{B^\alpha}$, and $B_0^\alpha \subset B^\alpha$. When $\alpha = 1$, we have $B^\alpha = B$ and $B_0^\alpha = B_0$, where B and B_0 are Bloch space and little Bloch space respectively(see [1, 4–11] for an account of the theory of B^α and B_0^α).

We set $\varphi_a(z) = (a - z)/(1 - \bar{a}z)$ to be a canonical Möbius map of D onto D determined by $a \in D$ and $D(a, r) = \{z \in D : |\varphi_a(z)| < r\}$ a pseudohyperbolic disk with center $a \in D$ and radius $r \in [0, 1]$. Suppose that $g(z, a) = log|\varphi_a(z)|$ is the Green function of D with logarithmic singularity at $a \in D$.

Hardy and Littlewood have proved that([5] [2]): for $0 < \alpha < 1$, $B^\alpha = Lip(1-\alpha)$, $B_0^\alpha = Lip^*(1-\alpha)$. We know that Lip$\beta$ can be used to describe the dual space of Hardy space H^p for $0 < p < 1$([2]). So we see B^α and B_0^α are very important in the theory of Hardy spaces.

In this paper constants are denoted by C which may indicate a different constant from one occurrence to the next.

2. Continuity of B^α and B_0^α.

1980 *Mathematics Subject Classification* (1985 *Revision*). 30D45, 30D50.
Key words and phrases. α-Bloch function, little α-Bloch function, predual space, continuity, Carleson measure.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Theorem 2.1. *Let $0 < \alpha, \beta < \infty$. then*

(a) $B^\alpha \subset B^\beta$, $B_0^\alpha \subset B_0^\beta$

(b) $\bigcup_{\alpha<\beta} B_0^\alpha = \bigcup_{\alpha<\beta} B^\alpha$

(c) $\bigcap_{\alpha<\beta} B_0^\beta = \bigcap_{\alpha<\beta} B^\beta$

Proof. (a). From $f \in B^\alpha$, we have

$$\lim_{|z|\to 1} |f'(z)|(1-|z|^2)^\beta \leq \|f\|_{B^\alpha} \lim_{|z|\to 1} (1-|z|^2)^{\beta-\alpha} = 0$$

Hence $B_0^\alpha \subset B^\alpha \subset B_0^\beta \subset B^\beta$.

(b). $\bigcup_{\alpha<\beta} B_0^\alpha \subseteq \bigcup_{\alpha<\beta} B^\alpha$ is obvious. Now we suppose $f \in \bigcup_{\alpha<\beta} B^\alpha$, then there exists $\alpha \in (0, \beta)$, such that $f \in B^\alpha$. For $\alpha' \in (\alpha, \beta)$, from the proof of (a) we know $f \in B_0^{\alpha'}$, so $f \in \bigcup_{\alpha<\beta} B_0^\alpha$ and $\bigcup_{\alpha<\beta} B_0^\alpha = \bigcup_{\alpha<\beta} B^\alpha$

(c). $\bigcap_{\alpha<\beta} B_0^\beta \subseteq \bigcap_{\alpha<\beta} B^\beta$ is obvious. Suppose $\beta \in (\alpha, \infty), f \in \bigcap_{\alpha<\beta} B^\beta$, then there exists $\beta' \in (\alpha, \beta)$, we have $f \in B^{\beta'}$, so from the proof of (a), $f \in B_0^\beta$ and hence $f \in \bigcap_{\alpha<\beta} B_0^\beta$. □

Theorem 2.2. *Let $0 < \alpha, \beta < \infty$, then*

(a) $\bigcup_{\alpha<\beta} B^\alpha \subsetneqq B^\beta$, $\bigcup_{\alpha<\beta} B_0^\alpha \subsetneqq B_0^\beta$,

(b) $\bigcap_{\alpha<\beta} B^\beta \supsetneqq B^\alpha$, $\bigcap_{\alpha<\beta} B_0^\beta \supsetneqq B_0^\alpha$,

Proof. We only prove (i): $\bigcup_{\alpha<\beta} B_0^\alpha \neq B_0^\beta$, (ii): $\bigcap_{\alpha<\beta} B^\beta \neq B^\alpha$,

(i). Taking $f(z) = \sum_{k=0}^\infty \frac{z^{2^k}}{k 2^{k(1-\beta)}}$, From Theorem 1 of [10] $f \notin B_0^\alpha$ for $\alpha < \beta$, but $f \in B_0^\beta$. So $\bigcup_{\alpha<\beta} B_0^\alpha \neq B_0^\beta$.

(ii). Taking $g(z) = \sum_{k=0}^\infty \frac{k z^{2^k}}{2^{k(1-\alpha)}}$. From Theorem 1 of [10], $f \in B^\beta$ for all $\alpha < \beta$, but $f \notin B^\alpha$. So $\bigcap_{\alpha<\beta} B^\beta \neq B^\alpha$. □

3. Predual space of B^α.

In [1], it was shown that the predual of Bloch space can be identified as

$$G_1(1) = \{f \in H(D) : \int_0^1 M_1(r, f') < \infty\}$$

where $M_p(r, f) = (\frac{1}{2\pi} \int_0^{2\pi} |f(re^{i\theta})|^p d\theta)^{1/p}$.

We extend the result to B^α, that is

Theorem 3.1. *Let $0 < \alpha \leq 1$, then the predual space of B^α is isomorphic to*

$$G_1(\alpha) = \{f \in H(D) : \int_0^1 (1-r)^{1-\alpha} M_1(r, f') dr < \infty\}$$

endowed with the norm $\|f\|_{G_1(\alpha)} = |f(0)| + \int_0^1 (1-\alpha)^{1-\alpha} M_1(r, f')dr$.

Proof. Let $\varphi \in (G_1(\alpha))^*$, $a_n = \varphi(z^n)$ and $f(z) = \sum_{n=0}^{\infty} a_n z^n$. It is easy to see that, for $0 < s < 1$,

$$\varphi(g(\tau z)) = \sum_{n=0}^{\infty} b_n \tau^n \varphi(z^n) = \sum_{n=0}^{\infty} a_n b_n \tau^n$$

So

$$\varphi(g) = < f, g > = \lim_{r \to 1} \sum_{n=0}^{\infty} a_n b_n r^n \quad (g \in G_1(\alpha))$$

Since

$$f'(\tau) = \sum_{n=0}^{\infty} n a_n \tau^{n-1} = < f(z), \frac{z}{(1-\tau z)^2} > = \varphi(\frac{z}{(1-\tau z)^2})$$

therefore

$$\begin{aligned}\|\frac{z}{(1-\tau z)^2}\|_{G_1(\alpha)} &= \frac{1}{2\pi}\int_0^1 (1-r)^{1-\alpha}\int_0^{2\pi} |\frac{1+\tau z}{(1-\tau z)^3}| d\theta dr \\ &\leq \int_0^1 (1-r)^{1-\alpha} \frac{1+|\tau|r}{1-|\tau|r}(\frac{1}{2\pi}\int_0^{2\pi} \frac{1}{|1-\tau z|^2} d\theta)dr \\ &\leq \int_0^1 \frac{(1-r)^{1-\alpha}}{(1-|\tau|r)^2} dr \leq C(1-|\tau|^2)^{-\alpha}\end{aligned}$$

Hence from $\|\varphi\|_{G_1(\alpha)^*} = \sup_{g \neq 0} \frac{|\varphi(g)|}{\|g\|_{G_1(\alpha)}}$, we obtain

$$|f'(\tau)| \leq \|\varphi\|_{G_1(\alpha)^*} \|\frac{z}{(1-\tau z)^2}\|_{G_1(\alpha)} \leq C(1-|\tau|^2)^{-\alpha}\|\varphi\|_{G_1(\alpha)^*}$$

Thus $f \in B^\alpha$; the choice $g(z) = z^n (n = 0, 1, \ldots)$ shows that $f \in B^\alpha$ is uniquely determined by $\varphi \in G_1^*(\alpha)$.

Conversely let $g(z) = \sum_{n=0}^{\infty} a_n z^n \in B^\alpha$ and $f(z) = \sum_{n=0}^{\infty} b_n z^n \in G_1(\alpha)$. Then define $\varphi(r) = \sum_{n=1}^{\infty} a_n b_n r^{n-1}$ for $0 < r < 1$. we shall show that $\{\varphi(r) : 0 < r < 1\}$ is a Cauchy net. From the equality

$$2(n+1)n \int_0^1 (1-s^2)s^{2n-1} ds = 1, \quad n \geq 1$$

we have

$$\begin{aligned}\varphi(r) &= 2\int_0^1 (1-s^2)(\sum_{n=1}^{\infty} n b_n (rs)^{n-1}(n+1)a_n s^n)ds \\ &= \frac{1}{\pi}\int_0^1 (1-s^2)\int_0^{2\pi} f'(rse^{i\theta})G'(se^{i\theta})e^{-i\theta} d\theta ds \qquad (1)\end{aligned}$$

where $G(z) = z(g(z) - g(0))$, so $G'(z) = zg(z) + \int_0^r g'(se^{i\theta})e^{i\theta} ds$ for $z = re^{i\theta}$, which implies that $G \in B^\alpha$.

Using (1) we get

$$\begin{aligned}
&|\varphi(r)-\varphi(R)| \\
&=\left|\frac{1}{\pi}\int_0^1\int_0^{2\pi}(1-s^2)(f'(rse^{i\theta})-f'(Rse^{i\theta}))G'(se^{-i\theta})e^{-i\theta}d\theta ds\right| \\
&\le C\int_0^1(1-s)^{1-\alpha}M_1(s,f_r'-f_R')ds \quad (f_r(z)=f(rz))
\end{aligned}$$

So $|\varphi(r)-\varphi(R)|\to 0$ as $r,R\to 1$ by a simple application of the Lebesgue Convergence Theorem. Now we define the linear functional $\psi(f)=\lim_{r\to 1}\varphi(r)$. Its boundedness follows from (1)

$$|\psi(f)|\le \sup_{0<r\le 1}\int_0^1(1-s)^{1-\alpha}M_1(s,f')ds$$

The theorem is proved. □

4. Carleson measure characterization of B^α and B_0^α functions.

Setting

$$S(w,t)=\{z\in D:|w|\le|z|<|w|+(1-|w|)t,|arg\frac{z}{w}|\le(1-|w|)t\}$$

we have

$$t^2(1-|w|)^2\le|S(w,t)|\le 3t^2(1-|w|)^2. \quad |w|\ge\frac{1}{2}$$

A positive measure μ on D is called a Carleson type measure if there exist constants C and $t:0<t\le 1$, such that $\mu(S(w,t))\le C(1-|w|)t$ for all $w\in D$. μ is called a vanishing Carleson type measure if $\lim_{|w|\to 1}\frac{\mu(S(w,t))}{(1-|w|)t}=0$.

It is obvious that Carleson measure(vanishing Carleson measure) is a Carleson type measure (vanishing Carleson type measure) for $t=1$(see [4, 6] for more on Carleson measure).

In this section we consider measure $\mu_{\alpha,\beta,p,f}, 0<\beta,p<\infty, 0\le\alpha<\infty, f\in H(D)$, defined by $d\mu_{\alpha,\beta,p,f}(z)=|D^\beta f(z)|^p(1-|z|^2)^{p(\alpha+\beta-1)-1}dm(z)$. where $D^\beta f(z)$ is the fractional derivative of $f(z)=\sum_{n=0}^\infty a_n z^n$ defined by $D^\beta f(z)=\sum_{n=0}^\infty(n+1)^\beta a_n z^n$. We give Carleson type measure characterization of α-Bloch functionsand vanishing Carleson type measure characterization of little α-Bloch functions,that is

Theorem 4.1. *Let $f\in H(D)$ and $0<\beta,p<\infty, 0\le\alpha<\infty$, then*

(a) $f\in B^\alpha$ if and only if $\mu_{\alpha,\beta,p,f}$ is a Carleson type measure.

(b) $f\in B_0^\alpha$ if and only if $\mu_{\alpha,\beta,p,f}$ is a vanishing Carleson type measure.

To prove the theorem we need the following lemmas.

Lemma 1([6]). *For $z \in D$ and $r : 0 < r < 1$, if $(r + \frac{z}{4})/(1 + \frac{rz}{4}) < |z| < 1$ then there exist $w \in D$ and $\rho : 0 < \rho < 1$, such that $D(z, r) \subset S(w, \rho)$.*

Lemma 2. *Let $0 < p, \beta < \infty, 0 \le \alpha < \infty, 0 < r < 1, 1 < \delta < \infty$, and $f \in H(D)$. then the following are equivalent*

(a) $f \in B^\alpha$

(b) $\sup_z |D^\beta f(z)|(1 - |z|^2)^{\alpha+\beta-1} < \infty$

(c) $\sup_u \int_D |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)-2}(1 - |\varphi_u(z)|^2)^\delta dm(z) < \infty$

Proof. We denote (a) is equivalent to (b) by $(a) \leftrightarrow (b)$. The proof of $(a) \leftrightarrow (b)$ and $(a) \leftrightarrow (c)$ is similar respectively to that of Theorem 2.1 and Theorem 2.3 of [8], so we omit the detail. □

Lemma 3. *Let $0 < p, \beta < \infty, 0 \le \alpha < \infty, 0 < r < 1, 1 < \delta < \infty$, and $f \in H(D)$. then the following are equvalent*

(a) $f \in B_0^\alpha$

(b) $|D^\beta f(z)|(1 - |z|^2)^{\alpha+\beta-1} \to 0, \quad |z| \to 1$

(c) $\int_D |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)-2}(1 - |\varphi_u(z)|^2)^\delta dm(z) \to 0, |u| \to 1$

Proof. The proof of $(a) \leftrightarrow (b)$ follows from [3, Theorem 6(ii)]. $(a) \leftrightarrow (c)$ is similar to that of Theorem 2.4 of [8], so we omit the detail. □

Proof of theorem 4.1. (a). If $f \in B^\alpha$. Fix $t : 0 < t < \frac{1}{2}$. By Lemma 2 we have

$$\begin{aligned}
\mu_{\alpha,\beta,p,f}(S(w,t)) &= \int_{S(w,t)} |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)-1} dm(z) \\
&\le \sup_z |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)} \int_{S(w,t)} (1 - |z|^2)^{-1} dm(z) \\
&\le \sup_z |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)} \frac{S(w,t)}{(1 - |w|)(1 - t)} \\
&\le \sup_z |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)} t(1 - |w|)
\end{aligned}$$

Here we used that $1 - |z|^2 > (1 - |w|)(1 - t)$, for $z \in S(w, t)$. Hence $\mu_{\alpha,\beta,p,f}$ is a Carleson type measure.

If $\mu_{\alpha,\beta,p,f}$ is a Carleson type measure, then for each $w \in D$, there exist constant C and $t : 0 < t \le 1$, such that $\mu_{\alpha,\beta,p,f}(S(w,t)) \le C(1 - |w|)t$.

If $t = 1$, then $\mu_{\alpha,\beta,p,f}$ is a Carleson measure; by [4, P.239, Lemma 3.3]

$$\sup_u \int_D |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)-2}(1 - |\varphi_u(z)|^2) dm(z) < \infty$$

therefore $f \in B^\alpha$ by Lemma 2($(a) \leftrightarrow (c)$).

If $t \neq 1$, for $u \in D : r_0 < |u| (r_0 = \frac{4+3\pi}{12+\pi})$, there exists $r = \frac{t}{4-t} (0 < t < 1)$ such that

$$\frac{\pi}{4} < \frac{r + \frac{\pi}{4}}{1 + \frac{r\pi}{4}} < \frac{4 + 3\pi}{12 + \pi} < |u| < 1$$

From the Lemma 1 and its proof there exist $w = \frac{|u|-r}{1-r|u|} e^{i\arg u} \in D$ and $t = \frac{4r}{1+r}$, such that $D(u, r) \subset S(w, t)$. So

$$\begin{aligned} &\int_{D(u,r)} |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)-2} dm(z) \\ &\leq \int_{S(w,t)} (1 - |z|^2)^{-1} d\mu_{\alpha,\beta,p,f}(z) \\ &\leq \frac{\mu_{\alpha,\beta,p,f}(S(w,t))}{(1 - |w|)(1 - t)} \\ &\leq C \frac{(1 - |w|)t}{(1 - |w|)(1 - t)} = \frac{Ct}{1 - t} \end{aligned}$$

and

$$\sup_{r_0 < |u|} \int_{D(u,r)} |D^\beta f(z)|^p (1 - |z|^2)^{p(\alpha+\beta-1)-2} dm(z) < \infty$$

Then (a) follows from Lemma 2.

(b). Using Lemma 3 instead of Lemma 2, the proof is similar to that of (a). □

REFERENCES

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

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

[3] T. M. Flett, *The dual of an inequality of Hardy and Littlewood and some related inequalities*, J. Math. Annal. Appl., 38(1972), 746-765.

[4] J. Garnett, *Bounded analytic functions*, Acad. Press, New York, 1981.

[5] G. H. Hardy and J. E. Littlewood, *Some properties of fractional integralsII*, Math Z., 34(1932), 403-439.

[6] W. L. Hasi, *A unfied portrayal of a certain amount of function spaces*, Northeastern Math. J., 8(1992), 77-82.

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

[8] Z. J. Lou, *Carleson measure characterization of Bloch functions*, Acta Math.(to appear)

[9] Z. J. Lou, *On Bloch functions*, C. R. Math. Rep. Acad. Sci. Canada, XV(6)(1993), 278-280.

[10] S. Yamashita, *Gap series and α-Bloch functions*, Yokohama Math. J., 28(1980), 31-36.

Department of Mathematics, Qufu Normal University, Qufu Shandong 273165 People's Republic of China

Received May 26, 1994

A NOTE ON THE STRONG LAW OF LARGE NUMBERS OF TRIANGULAR ARRAYS

Fuchun Huang, Peili Wang and Xueren Ding

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

Abstract A necessary and sufficient condition is given for almost sure convergence of triangular arrays with a common distribution.

If X_n, $n \geq 1$ are independent identically distributeds random variables, $S_n = \sum_1^n X_i$ and $\mathbf{E}X_1$ exists, then the Kolmogorov strong law of large numbers ensures $S_n/n \to \mathbf{E}X_1$ almost surely. But this result can not extend directly to triangular arrays. That is, given a triangular array of independent random variables (all defined on a common probability space) such that its nth row consists of n independent and identically distributed random variables $X_{n1}, \ldots, X_{nn}$ according to a common distribution F with mean zero, $S_{nn} = \sum_{j=1}^n X_{nj}$, it is a question whether or not

$$\frac{S_{nn}}{n} \longrightarrow 0 \quad a.s. \tag{*}$$

In [1], J.H. Romano and A.F. Siegel give an example to show that (*) may fail to hold if F has only first finite moment of zero. Their counterexample is an F, that is a *symmetric* distribution and $F(t) = 1 - \frac{1}{2t^2}$ if $t > 1$. Then, using an inequality of Feller (see [2], p. 149), they proved

$$\sum_{n=1}^{\infty} P\left(\frac{S_{nn}}{n} > 1\right) = \infty.$$

So, by the Borel-Cantelli Lemma, $P\left(\frac{|S_{nn}|}{n} > 1 \text{ infinitely often}\right) = 1$, therefore S_{nn}/n diverges almost surely. They also proved that if F has mean zero and a fourth finite moment μ_4, then $S_n/n \xrightarrow{a.s.} 0$, regardless of the row structure. Indeed,

$$\sum_{n=1}^{\infty} P\left(|\frac{S_{nn}}{n}| > \epsilon\right) \leq \sum_{n=1}^{\infty} \frac{\mathbf{E}|S_{nn}/n|^4}{\epsilon^4} < \infty, \qquad \forall \epsilon > 0.$$

So by the Borel-Cantelli Lemma, (*) holds.

In this note we prove the following

THEOREM. *(*) holds if and only if F has mean zero and a second finite moment.*

Proof. By the famous Hsu-Robbins theorem (see [3], p. 363), we know that

$$\sum_{n=1}^{\infty} P\left(\frac{|S_n|}{n} > \epsilon\right) < \infty, \qquad \epsilon > 0, \tag{**}$$

if and only if $EX_{11} = 0$, $EX_{11}^2 < \infty$. If (**) holds, then by the Borel-Cantelli lemma, (*) holds. Else if (**) does not hold, since S_{nn}, $n = 1, 2, \ldots$ are independent random variables, by the Borel-Cantelli lemma for independent events, $P\left(\frac{|S_{nn}|}{n} > 1 \text{ infinitely often}\right) = 1$. However, since F has mean zero, by the usual weak law of large numbers, $S_{nn}/n \xrightarrow{P} 0$, so S_{nn}/n diverges almost surely, that is (*) does not hold. This completes the proof of the theorem.

Noting that (**) means the complete convergence of S_{nn}/n, we have

Corollary. $\frac{S_{nn}}{n} \xrightarrow{c} 0$ if and only if $\frac{S_{nn}}{n} \xrightarrow{a.s.} 0$.

So, though the complete convergence is much stronger than the almost sure convergence in general, the two convergences are equivalent in the case of triangular arrays with common distribution.

Note added in proof: An article by W.E. Pruitt "Summability of independent random variables", J. Math. Mech. 15 (1966), 769-776, contains the "if" part of the present Theorem in a very general form.

Reference

[1] J.H. Romano and A.F. Siegel (1986), Counterexamples in probability and statistics, Wadsworth, Inc., Belmont.

[2] W. Feller (1971), An introduction to probability theory and its applications, Vol. 2, 2nd ed., Wiley, New York.

[3] Y.S. Chow and H. Teicher (1978), Probability theory, Springer-Verlag, New York.

Fuchun Huang,
Institute of Appl. Math., Academia Sinica, P.O. Box 2734, Beijing 100080, CHINA
Peili Wang and Xueren Ding,
Dept. of Math., Tianjin University, Tianjin 300072, CHINA.

Received April 8, 1994

ROUND-OFF STABILITY OF ITERATIONS ON PRODUCT SPACES

S. L. SINGH, S. N. MISHRA and V. CHADHA

Presented by M.A. Akcoglu, F.R.S.C.

ABSTRACT Ostrowski's result [Z. Angew. Math. Mech. 47(1967),77-81; MR35#7560] on the stability of Picard sequence of iterates for Banach contraction is extended to Matkowski contraction on product spaces.

Keywords: Stable iteration, Banach contraction, Matkowski contraction, fixed point.

Mathematics Subject Classifications(1991):65D15,41A25,47H10,54H25.

1.INTRODUCTION. In computing, a solution of an equation is usually approximated by an iterating sequence $\{x_n\}$, say. In practice, because of rounding off or discretization of the function, an approximate sequence is used in place of the sequence $\{x_n\}$. In general, the approximate sequence and the sequence $\{x_n\}$ need not converge to the same point (see, for instance, Harder-Hicks [2],p.704). Alexander M. Ostrowski [6] appears to be the first to investigate sufficient conditions concerning the stability of iteration procedures for contracting maps (see Theorem 2.1 below). Recently Harder-Hicks [2] and Rhoades [8] have obtained similar results for maps satisfying certain contractive conditions. The purpose of this paper is to extend Ostrowski's (now classical) theorem to Matkowski contraction systems on a finite product of metric spaces.

2. PRELIMINARIES. Let (Y, d) be a metric space and $T : Y \to Y$.

For a point x_0 in Y, let

(*) $$x_{n+1} = f(T, x_n)$$

denote some iteration procedure. Let the sequence $\{x_n\}$ be convergent to a fixed point p of T. Let $\{y_n\}$ be an arbitrary sequence in Y, and set

$$\epsilon_n = d(y_{n+1}, f(T, y_n)), \quad n = 0,1,2,\ldots.$$

If $\lim_{m\to\infty} \epsilon_n = 0$ implies that $\lim_{n\to\infty} y_n = p$, then the iteration process defined in (*) is said to be T-stable or stable with respect to T (see Harder-Hicks [2], Rhoades [8]).

In 1967, Ostrowski [6] obtained the following first result on T-stability (see Harder-Hicks [2] and Istrăţescu [3], p.101, wherein Ostrovski (1964) should be corrected to Ostrowski (1967)):

THEOREM 1. *Let (Y, d) be a complete metric space and $T : Y \to Y$ such that T is a Banach contraction, that is,*

(2.1) $$d(Tx, Ty) \le k\, d(x, y)$$

for all $x, y \in Y$; where $k<1$ is a nonnegative number. Let p be the fixed point of T. Let x_0 be an arbitrary point in Y and put

$$x_{n+1} = Tx_n, \; n = 0, 1, 2, \ldots\ldots$$

Let $\{y_n\}$ be a sequence in Y, and $\epsilon_n = d(y_{n+1}, Ty_n)$, $n = 0, 1, 2, \ldots$. Then, for $n = 0, 1, 2, \ldots$,

$$\text{(1)}\quad d(p, y_{n+1}) \le d(p, x_{n+1}) + k^{n+1}d(x_0, y_0) + \sum_{j=0}^{n} k^{n-j}\epsilon_j.$$

Also

$$\text{(2)}\quad \lim_{n\to\infty} y_n = p \text{ if and only if } \lim_{n\to\infty} \epsilon_n = 0.$$

REMARK 1. The last relation (2) says that the functional iteration (*) given by the Picard sequence of iterates, i.e., $x_{n+1} = f(T, x_n) = Tx_n$ is stable with respect to Banach contraction T. Further, since in the case of Banach contraction, $d(x_n, p) \le k^n d(x_0, Tx_0)/(1-k)$, (1) gives an upper bound for the error in estimating $d(y_n, p)$.

In all that follows, we generally follow the following notations of Matkowski [5] (see also Czerwik [1], Matkowski [4], Reddy-Subrahmanyam [7] and Singh-Gairola [9]).

$$\text{(2.2)}\qquad c_{ik}^{(0)} = \begin{cases} a_{ik} & \text{for } i \ne k, \\ 1 - a_{ik} & \text{for } i = k, \end{cases} \qquad i, k = 1, 2, \ldots, n,$$

and $c_{ik}^{(t)}$ are defined recursively by

$$\text{(2.3)}\qquad c_{ik}^{(t+1)} = \begin{cases} c_{11}^{(t)}\, c_{i+1,k+1}^{(t)} + c_{i+1,1}^{(t)}\, c_{1,k+1}^{(t)}, & \text{for } i \ne k \\ c_{11}^{(t)}\, c_{i+1,k+1}^{(t)} - c_{i+1,1}^{(t)}\, c_{1,k+1}^{(t)}, & \text{for } i = k, \end{cases}$$

$$i, k = 1, \ldots, n-t-1, \qquad t = 0, 1, \ldots, n-2.$$

If $n = 1$, we define $c_{11}^{(0)} = a_{11}$.

Matkowski [5, p. 9] has shown that the system of inequalities $\sum_{k=1}^{n} a_{ik}\, r_k < r_i$, $i = 1, 2, \ldots, n$, has a solution $r_i > 0$, $i = 1, 2, \ldots n$, if and only if

$$\text{(2.4)}\qquad c_{ii}^{(t)} > 0,\; i=1, \ldots, n-t,\; t=0, \ldots, n-1;\; n \ge 2$$

holds. Moreover, *there exists a positive number $h < 1$* such that

$$\text{(2.5)}\qquad \sum_{k=1}^{n} a_{ik}\, r_k \le hr_i, \quad i = 1, 2, \ldots n,$$

for some positive numbers $r_1, r_2, \ldots, r_n$, (see Czerwik [1] and Singh-Gairola [9, p. 795]). Indeed, such an h may be found by

$$\text{(2.6)}\qquad h = \max_i \Big(r_i^{-1} \sum_{k=1}^{n} a_{ik}\, r_k\Big).$$

Let (X_i, d_i), $i = 1, 2, \ldots, n$, *be metric spaces,*

$$X := X_1 \times X_2 \times \ldots \times X_n ,$$

and $x^m := (x_1^m, \ldots, x_n^m)$, $x_i^m \in X_i$, $i = 1, \ldots, n$; $m = 0, 1, 2, \ldots$.
Also $x := (x_1, \ldots, x_n)$, $x_i \in X_i$, $i = 1, \ldots, n$.

Matkowski's theorem [4-5] is as follows:

THEOREM 2. *Let* (X_i, d_i), $i = 1, 2, \ldots, n$, be complete metric spaces and

$T_i : X \to X_i$, $i = 1, 2, \ldots, n$, *be such that*

$$(2.7) \qquad d_i(T_i x, T_i y) \le \sum_{k=1}^{n} a_{ik}\, d_k(x_k, y_k)$$

for every $x_k, y_k \in X_k$, $i, k = 1, \ldots, n$, *where* a_{ik} *are nonnegative numbers defined in (2.2) such that (2.3) and (2.4) hold. Then the system of equations*

$$(2.8) \qquad x_i = T_i x, \quad i = 1, \ldots, n$$

has exactly one solution $p = (p_1, \ldots, p_n)$ *such that* $p_i \in X_i$, $i = 1, \ldots, n$. *For any arbitrarily fixed* $x^0 \in X$, *the sequence of successive approximations*

$$(2.9) \qquad x_i^{m+1} = T_i x^m, \quad i = 1, \ldots, n,$$

converges and

$$(2.10) \qquad p_i = \lim_{m\to\infty} x_i^m , \quad i = 1, \ldots, n.$$

The above theorem is usually known as the Matkowski contraction principle (Mcp). Further, $T := (T_1, \ldots, T_n)$ satisfying (2.7), (2.2)-(2.4) is called Matkowski contraction (see Reddy-Subrahmanyam [7] and Singh-Gairola [9]). If $p \in X$ is a solution of (2.8), then p is called a fixed point of $T := (T_1, \ldots, T_n)$.

We shall need the following lemma due to Harder and Hicks [2].

LEMMA. *If* c *is a real number such that* $0 < |c| < 1$ *and* $\{b^j\}$ *is a sequence of real numbers such that* $b^j \to 0$ *as* $j \to \infty$, *then*

$$\lim_{m\to\infty} \left(\sum_{j=0}^{m} c^{m-j} b^j\right) = 0.$$

3. STABILITY RESULTS. The following stability theorem shows that the functional iteration for $T := (T_1, \ldots, T_n)$ defined by (2.9) is T-stable whenever T fulfills the requirements of the Mcp.

THEOREM 3. *Let* (X_i, d_i) *be a complete metric space and* $T_i : X \to X_i$, $i = 1, \ldots, n$, *such that* $T := (T_1, \ldots, T_n)$ *is a Matkowski contraction. Let* $p = (p_1, \ldots, p_n)$ *be the fixed point of* T. *Let* $x^0 = (x_1^0, \ldots, x_n^0)$ *be an arbitrary point in* X, *and put*

$$x_i^{m+1} = T_i x^m , \ m = 0, 1, \ldots, \ i = 1, \ldots, n.$$

Let $\{y_i^m\}$ *denote an arbitrary sequence in* X_i, $i = 1, \ldots, n$, *and set*

$\epsilon_i^m = d_i(y_i^{m+1}, T_i y^m)$, $m = 0, 1, \ldots, i = 1, \ldots, n$.
Then, for $m = 0, 1, \ldots,$ *and* $i = 1, 2, \ldots, n$,

(I) $$d_i(p_i, y_i^{m+1}) \le d_i(p_i, x_i^{m+1}) + h^{m+1} r_i + \sum_{j=0}^{m} h^{m-j} \epsilon_i^j,$$

where $r_i \ge d_i(x_i^0, y_i^0)$ *are some positive numbers and* h *is defined by (2.6). Also*

(II) $\lim_{m\to\infty} y_i^m = p_i$ *if and only if* $\lim_{m\to\infty} \epsilon_i^m = 0$.

PROOF. For any m,

(3.1) $$d_i(p_i, y_i^{m+1}) \le d_i(p_i, x_i^{m+1}) + d_i(T_i x^m, T_i y^m) + d_i(T_i y^m, y_i^{m+1})$$

$$\le d_i(p_i, x_i^{m+1}) + \sum_{k=1}^{n} a_{ik} d_k(x_k^m, y_k^m) + \epsilon_i^m, \quad i = 1, \ldots, n.$$

Now we estimate the middle term on the right hand side of (3.1). From the homogeneity of the system (2.5), we may assume without any loss of generality (indeed, if necessary increasing the values of r_i, $i = 1, \ldots, n$) that $d_i(x_i^0, y_i^0) \le r_i$, for some positive numbers r_i, $i = 1, \ldots, n$ satisfying (2.5). Then

$$d_i(x_i^1, y_i^1) \le d_i(x_i^1, T_i y^0) + d_i(T_i y^0, y_i^1)$$

$$= d_i(T_i x^0, T_i y^0) + \epsilon_i^0 \le \sum_{k=1}^{n} a_{ik} r_k + \epsilon_i^0 \le h r_i + \epsilon_i^0.$$

Analogously $d_i(x_i^2, y_i^2) \le h(h r_i + \epsilon_i^0) + \epsilon_i^1 = h^2 r_i + h\epsilon_i^0 + \epsilon_i^1$.
Inductively $d_i(x_i^m, y_i^m) \le h^m r_i + h^{m-1}\epsilon_i^0 + h^{m-2}\epsilon_i^1 + \ldots + h\,\epsilon_i^{m-2} + \epsilon_i^{m-1}$.

$$\therefore \sum_{k=1}^{n} a_{ik}\, d_k(x_k^m, y_k^m) \le h^{m+1} r_i + \sum_{j=0}^{m-1} h^{m-j}\epsilon_i^j.$$

Its substitution in (3.1) establishes (I).

To prove (II), first assume $y_i^m \to p_i$ as $m \to \infty$, $i = 1, \ldots, n$. Then, for any i,

$$\epsilon_i^m = d_i(y_i^{m+1}, T_i y^m)$$
$$\le d_i(y_i^{m+1}, p_i) + d_i(T_i p, T_i y^m)$$
$$\le d_i(y_i^{m+1}, p_i) + \sum_{k=1}^{n} a_{ik} d_k(p_k, y_k^m)$$
$$\le d_i(y_i^{m+1}, p_i) + \left(\sum_{k=1}^{n} a_{ik}\right).\max\{d_1(p_1, y_1^m), \ldots, d_n(p_n, y_n^m)\}.$$

Since each $d_i(p_i, y_i^m) \to 0$ as $m \to \infty$, $\lim_{m\to\infty} \epsilon_i^m = 0$.

Now suppose $\epsilon_i^m \to 0$ as $m \to \infty$. Since the Mcp guarantees the existence of exactly one solution of (2.8) and, by hypothesis, p is a solution of (2.8), the sequence $\{x_i^m\}$ converges to p_i, $i = 1,\ldots,n$, (cf. (2.9)-(2.10)). Recall that $0 < h < 1$ (cf. (2.5)). Thus, from (I),

$$\lim_{m\to\infty} d_i(p_i, y_i^{m+1}) \le \lim_{m\to\infty} \left(\sum_{j=0}^{m} h^{m-j}\epsilon_i^j\right).$$

Since $\{\epsilon_i^j\}_{j=0}^{\infty}$ is convergent to zero, an appeal to the lemma of Harder and Hicks establishes (II).

COROLLARY. Theorem 1.

Proof. Take $(Y, d) = (X_i, d_i)$, $T = T_i$ $i = 1,\ldots,n$, and $n = 1$ with $a_{11} = k$, $d(x_0, y_0) = r_1$ in Theorem 3.

REFERENCES

1. S. Czerwik, A fixed point theorem for a system of multivalued transformations, Proc. Amer. Math. Soc. 55(1976),136-139.
2. A. M. Harder and T. L. Hicks, Stability results for a fixed point iteration procedures, Math. Japon. 33(1988), no.5,693-706.
3. V. I. Istrăţescu,Fixed Point Theory, D. Reidel Publishing Co.,Dordrecht: Holland, 1981.
4. J. Matkowski, Some inequalities and a generalization of Banach's Principle, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 21(1973),323-324.
5. J. Matkowski, Integrable solutions of functional equations, Dissertationes Mat. Vol.CXXVIII (Rozprawy), Warszawa, 1975.
6. A. M. Ostrowski, The round-off stability of iterations, Z. Angew. Math. Mech. 47(1967),77-81.
7. K. B. Reddy and P. V. Subrahmanyam, Altman's contractors and fixed points of multivalued mappings. Pacific J. Math. 99(1982), no.1, 127-136.
8. B. E. Rhoades, Fixed point theorems and stability results for fixed point iteration procedures. Indian J. Pure Appl. Math. 21(1990),1-9.
9. S. L. Singh and U. C. Gairola, A general fixed point theorem, Math. Japon. 36(1991),no.4,791-801.

Singh : Department of Mathematics
Gurukula Kangri University, Hardwar 249404 INDIA

Mishra : Department of Mathematics,University of Transkei
Private Bag XI UNITRA, UMTATA,Transkei, Southern Africa

Chadha : Department of Mathematics,University of Wisconsin,Eau Claire,WI-54702, U.S.A.

Received April 25, 1994

CORRIGENDUM TO AN APPROACH TO WIEFERICH'S CONDITION

C.R. Math. Rep. XIII, No. 2 April 1991

M. Yamada

Recently, I became aware that the following sentence had been dropped between L.7 of P. 91:

"If u^p replaces u as a new u, then $(u+1)u^{-1}F_1(u) \equiv 0 \pmod{p^2}$."

This line should be inserted.

2-3-41 Nishihara
Mito, Ibaraki, 310
Japan

Received May 20, 1994

Mailing Addresses (continued from p. 111)

P.W. Sharp	Department of Mathematics and Statistics New Zealand University Auckland, New Zealand
S.L. Singh	Department of Mathematics Gurukula Kangri University Hardwar, 249 404, India
N. Terai	Division of General Education Ashikaga Institute of Technology 268-1 Omae, Ashikaga, Tochigi, 326, Japan
P. Tzermias	Department of Mathematics University of California Berkeley, CA, 94720, U.S.A.
R. Vaillancourt	Department of Computer Science and Mathematics University of Ottawa Ottawa, Ontario, K1N 6N5, Canada
J. Végső	Kossuth Lajos University Mathematical Institute Debrecen, P.O. Box 12, H-4010, Hungary
D. Xueren	Department of Mathematics Tianjin University Tianjin, 300072, China
M. Yamada	2-3-41 Nishihara Mito, Ibaraki 310, Japan

Mailing Addresses

B.Brindza	Kossuth Lajos University Mathematical Institute Debrecen, P.O. Box 12, H-4010, Hungary
V. Chadha	Department of Mathematics University of Wisconsin Eau Claire, WI, 54702, U.S.A.
J.T. Condo	Department of Mathematics Ball State University Muncie, IN, 43706-0490, U.S.A.
D.E. Dobbs	Department of Mathematics University of Tennessee Knoxville, TN, 37996-1300, U.S.A.
S. Dubuc	Departement de mathematiques et de statistique Université de Montréal, C.P. 6128, Montréal, Quebec, H3C 3J7, Canada
H. Fuchun	Institute of Applied Mathematics Academia Sinica P.O. Box 2734, Beijing 100080, China
E.G. Goodaire	Department of Mathematics Memorial University of Newfoundland St. John's, Newfoundland, A1C 5S7, Canada
M. Guzman-Gomez	Department of Mathematics University of Toronto Toronto, Ontario, Canada M5S 1A1
R. Hamzaoui	Institut für Informatik Universitat Freiburg Rheinstr. 10-12 D79104 Freiburg, Germany
Z. Lou	Department of Mathematics Qufu Normal University Qufu, Shandong 273165, P.R. China
F. Malek	Department of Computer Science University of Ottawa Ottawa, Ontario, Canada K1N 6N5
C.P. Milies	Universidade de Sao Paulo Caixa Postale 20570 Ag. Iquatemi 01452-990 Sao Paulo, Brazil
S.N. Mishra	Department of Mathematics University of Transkei Private Bag XI UNITRA, Transkei Southern Africa
W. Peili	Department of Mathematics Tianjin University Tianjin, 300072, China
A. Pintér	Kossuth Lajos University Mathematical Institute Debrecen, P.O. Box 12, H-4010, Hungary