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

Vol. X, No. 2 April 1988 avril

CONTENTS

An Artin Conjecture for Two Term Recurrence Sequences

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

Let $\{0,1,f_2,f_3,\cdots\}$ be defined by a two-term integer recurrence relation and let $\ell(p)$ be the first positive n with $f_n \equiv 0 \bmod p$. In this note we use the reasoning behind Artin's conjecture on primitive roots to conjecture the density of primes p for which $\ell(p)$ is as large as possible. This conjecture may be thought of as a reciprocity law involving these densities and the densities occuring in the Artin conjecture.

§1. Recurrence Sequences Modulo p

Let D be a square-free integer and let $K = \mathbb{Q}(\sqrt{D})$. Let $\mathcal{O}_K$ be the ring of algebraic integers in K, let α be a non-rational algebraic integer in $\mathcal{O}_K$, and let σ be the non-trivial automorphism of K/Q. Let $T=\alpha+\sigma(\alpha)$ be the trace of α and $N=\alpha\sigma(\alpha)$ be the norm of α. We define a sequence of integers

$$f_n = \frac{\alpha^n - \sigma(\alpha^n)}{\alpha - \sigma(\alpha)} \tag{1}$$

Lemma 1.1 *Suppose* $T \neq 0$. *Then the sequence* $\{f_n\}$ *satisfies the integer recurrence relation* $f_{n+2} = Tf_{n+1} - Nf_n$, $f_0 = 0$, $f_1 = 1$. *Furthermore, any such two-term integer recurrence relation is given by* (1) *for appropriate* D *and* α *as long as* T^2-4N *is not a square.*

Proof: The first part follows from the definition of f_n and the fact that both α and $\sigma(\alpha)$ are roots of $X^2-TX+N=0$. For the second part, let D be the square-free part of T^2-4N and let α be a root of X^2-TX+N lying in $\mathbb{Q}(\sqrt{D})$. □

Let $u=\alpha/\sigma(\alpha)$. The sequence f_n is periodically zero if and only if u is a root of unity. We will want to exclude these cases, so we will *assume that u is not a root of unity.* This is not very restrictive since $u \notin \mathbb{Q}$ and u lies in a quadratic extension of Q. Thus u is either a third, fourth, or sixth root of unity and $D=-1$ or $D=-3$, see [5].

Let $p \in \mathbb{Z}$ be a prime. We are interested in the first time that p divides an element of our sequence. We therefore define

Definition 1.2 $\ell(p)$ is the least positive integer n such that $p|f_n$.

If $p \nmid (\alpha-\sigma(\alpha))$ in $\mathcal{O}_K$, then $p|f_n$ if and only if $\alpha^n-\sigma(\alpha^n) \equiv 0 \bmod p\mathcal{O}_K$. Let V be the norm of $\alpha-\sigma(\alpha)$. Suppose $p \nmid VN$. Then α is a unit mod $p\mathcal{O}_K$ and $p \nmid (\alpha-\sigma(\alpha))$. Thus $p|f_n$ if and only if $u^n \equiv 1 \bmod p\mathcal{O}_K$.

Let Δ denote the discriminant of K and $\chi(p) = \left(\frac{D}{p}\right)$ be the Legendre symbol.

Proposition 1.3 *Assume* $p \nmid VN\Delta$. *Let* $N_p:(\mathcal{O}_K/p\mathcal{O}_K)^\times \to \mathbb{F}_p^\times$ *be the local norm map defined by* $N_p(\beta+p\mathcal{O}_K)=\beta\sigma(\beta)+p\mathbb{Z}$. *Let* G_p *be the kernel of* N_p. *Then* G_p *is cyclic of order* $p-\chi(p)$ *and* u *defines an element in* G_p *whose order is* $\ell(p)$.

Proof: Since $p \nmid \Delta$, D is a unit modulo p. Thus $\{n^2-Dm^2|m,n\in\mathbb{Z}\}$ represents every residue class modulo p. Hence N_p is surjective, and

$|G_p|=\frac{1}{p-1}|(\mathcal{O}_K/p\mathcal{O}_K)^\times|$. If $\chi(p)=-1$, then $p\mathcal{O}_K$ is prime and $|(\mathcal{O}_K/p\mathcal{O}_K)^\times|=$

p^2-1. Thus $|G_p|=p+1$ and, being a subgroup of the group of units of a finite field, G_p is cyclic. If $\chi(p)=1$, then $p\mathcal{O}_K=P_1P_2$ for two prime ideals P_1 and P_2 of $\mathcal{O}_K$ with $\sigma(P_1)=P_2$. Thus $(\mathcal{O}_K/p\mathcal{O}_K)^\times \cong (\mathcal{O}_K/P_1)^\times \times (\mathcal{O}_K/P_2)^\times \cong \mathbb{F}_p^\times \times \mathbb{F}_p^\times$. If $\beta\in G_p$, then $\beta=\sigma(\beta)^{-1}$, so G_p lies in $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ as the set of elements of the form (x,x^{-1}), which is a cyclic subgroup of order $p-1$. Since u has (global) norm 1, $u+p\mathcal{O}_K\in G_p$ as long as $p\nmid N$, and the proposition follows from the preceding discussion. □

Suppose $p|\Delta$ but $p\nmid VN$. Then $p=2$, which ramifies, $\mathrm{Im}(N_2)=\mathbb{F}_2^\times$, and $|G_2|=4$. But $u=\alpha^2/N$ represents an element in G_2^2, which is cyclic of order 2. We are not particularly concerned with this case, but it completes the proof of the following corollary due to Lucas [5],[6].

Corollary 1.4 $\ell(p)|(p-\chi(p))$ *if* $p\nmid VN$. □

Since $\ell(p)|p-\chi(p)$ for all but possibly finitely many p, we can ask for the *density* of primes with $\ell(p)=p-\chi(p)$. Let $\pi(N)$ denote the number of primes less than or equal to N. We are then interested in computing the (hypothetical) limit $\rho(\alpha)$ defined by

$$\rho(\alpha)=\lim_{N\to\infty}\frac{1}{\pi(N)}|\{\text{primes } p\le N \text{ with } \ell(p)=p-\chi(p)\}|.$$

We see that, if $\rho(\alpha)$ exists, it may be interpreted as the density of primes for which u represents a generator of G_p. It seems reasonable to assume that, for any fixed α, the residue class of u in G_p is "random" as long as α is not a square and u is not a root of unity. This is reminiscent of the Artin Conjecture, see [1],[2],[3],and [4]. The reasoning which follows is strongly based on [4].

§2. Computation of $\rho(\alpha)$.

From now on we will assume that u is neither a square nor a root of unity in K. Since $u=\alpha^2/N$, N is not a square. We let $\bar{u}$ denote the class of u in G_p.

Suppose $\bar{u}$ does not generate G_p. Then $\bar{u}$ has a q^{th} root in G_p and hence in $\mathcal{O}_K/p\mathcal{O}_K$ for some prime factor q of $p-\chi(p)$. Thus if L_q is the splitting field of the polynomial X^q-u over K, then $p\mathcal{O}_K$ splits completely in L_q.

Conversely, if $p\mathcal{O}_K$ splits completely in L_q, then $\bar{u}$ is a q^{th} power modulo $p\mathcal{O}_K$ and hence not a generator of G_p.

Thus $\ell(p)=p-\chi(p)$ precisely if $p\mathcal{O}_K$ splits completely in some field $L_q=K(\sqrt[q]{u},\zeta_q)$ where q is a prime satisfying

$$p \equiv \chi(p) \bmod q$$

(2)

$$\bar{u}^{\left(\frac{p-\chi(p)}{q}\right)} \equiv 1 \quad \bmod p\mathcal{O}_K$$

We now refer to the analyses in [1],[2], and [4] which show how to account for the fact that the various L_q need not be linearly independent. For k a positive square-free integer with prime factorization $k=q_1q_2\cdots q_t$ we let L_k be the compositum $L_{q_1}L_{q_2}\cdots L_{q_t}$. The analyses lead us to conjecture that $\rho(\alpha)$ exists and

$$\rho(\alpha) = \sum_{k=1}^{\infty} \mu(k)/n(k) \tag{3}$$

where $1/n(k)$ is the proportion of primes p satisfying (2) which split completely in L_k, $n(1)=1$, and μ is the Möbius μ-function.

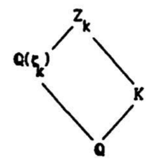
The numbers n(k) may be computed following [4]. Let h be the largest integer such that u is an h^{th} power. (The existence of h follows from the finiteness of the class number.) We let $k_1=k/(h,k)$ and define $H_k=K(\sqrt[k_1]{\bar{u}},\zeta_k)$. Then $n(k)=[H_k:K]$, see [4].

Now H_k is a Kummer extension of the cyclotomic extension $Z_k=K(\zeta_k)$. Furthermore, $[Z_k:K]=\varphi(k)$ unless $K\subset Q(\zeta_k)$. This happens if and only if $\Delta|k$, see [7]. Since k is square-free and $\Delta=4D$ if $D\not\equiv 1 \bmod 4$, this happens if and only if $D|k$ and $D\equiv 1 \bmod 4$. In this case $[Z_k:K]=\varphi(k)/2$.

Next, $[H_k:Z_k]=k_1$ unless u has a q^{th} root in Z_k for some prime q dividing k_1, see [4]. Since Z_k is abelian over K, q must be 2. Thus $[H_k:Z_k]=k_1$ unless $\sqrt{\bar{u}}\in Z_k$ and k_1 (and hence k) is even, in which case $[H_k:Z_k]=k_1/2$.

Lemma 2.1 *Let* N_0 *be the square-free part of* $ND/(D,N)^2$. *Then* $\sqrt{\bar{u}}\in Z_k$ *if and only if* $N_0\equiv 1 \pmod 4$ *and* $N_0|k$.

Proof: Since $u=\alpha^2/N$ is N_0 times a square, the lemma follows as above if $Z_k=Q(\zeta_k)$. If not, we have a diagram of field extensions



Since $\sqrt{D}\notin Q(\zeta_k)$, $[Z_k:Q]=2\varphi(k)$. Hence $[Z_k:K]=\varphi(k)$, and as both are cyclotomic extensions we have $Gal(Z_k/K)\cong Gal(Q(\zeta_k)/Q)$. Therefore both fields have the same number of distinct quadratic subfields. It follows that for any square-free integer M with $(M,D)=1$, $\sqrt{M}\in Z_k$ if and only if $\sqrt{M}\in Q(\zeta_k)$. Thus the lemma also holds if $Z_k=Q(\zeta_k)$. □

We conclude that $n(k)=k_1\varphi(k)/\epsilon(k)\delta(k)$ where

$$(4) \qquad \varepsilon(k) = \begin{cases} 2 & \text{if } D|k \text{ and } D \equiv 1 \bmod 4 \\ 1 & \text{otherwise} \end{cases}$$

$$\delta(k) = \begin{cases} 2 & \text{if } 2N_0|k \text{ and } N_0 \equiv 1 \bmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

This completes the conjectured formula (3) for $\rho(\alpha)$. Our next step is to write down a product formula for $\rho(\alpha)$.

§3. The Product Formula.

If $k = q_1 q_2 \cdots q_t$, then $k\varphi(k) = \prod_{i=1}^{t} q_i(q_i - 1)$. If $q_i | h$, then $q_i | (h,k)$, so

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} = \sum_{k=1}^{\infty} \frac{\mu(k)(h,k)}{k\varphi(k)} = \prod_{q \text{ prime}} \left(1 - \frac{(q,h)}{q(q-1)}\right) = \prod_{q|h}\left(1 - \frac{1}{q-1}\right) \prod_{q \nmid h}\left(1 - \frac{1}{q(q-1)}\right)$$

provided $\varepsilon(k) = \delta(k) = 1$ for all k. We therefore define

$$P(h) = \prod_{q|h}\left(1 - \frac{1}{q-1}\right)\prod_{q \nmid h}\left(1 - \frac{1}{q(q-1)}\right)$$

and ask for a correction factor if D or N_0 are congruent to 1 mod 4. In general we have

$$\rho(\alpha) = \sum_{D \nmid k, 2N_0 \nmid k} \frac{\mu(k)(h,k)}{k\varphi(k)} + 2\sum_{D|k, 2N_0 \nmid k} \frac{\mu(k)(h,k)}{k\varphi(k)} + 2\sum_{D \nmid k, 2N_0 | k} \frac{\mu(k)(h,k)}{k\varphi(k)} + 4\sum_{D|k, 2N_0|k} \frac{\mu(k)(h,k)}{k\varphi(k)} =$$

$$\sum_{\text{all } k} \frac{\mu(k)(h,k)}{k\varphi(k)} + \sum_{D|k} \frac{\mu(k)(h,k)}{k\varphi(k)} + \sum_{2N_0|k} \frac{\mu(k)(h,k)}{k\varphi(k)} + \sum_{\mathrm{lcm}(D,2N_0)|k} \frac{\mu(k)(h,k)}{k\varphi(k)}$$

which can be best written as a product after defining a factor $C(h,m)$ for any $m \in \mathbb{Z}$ by

$$C(h,m) = \begin{cases} 1 - \mu(|m|)\prod_{q|m, q|h}\left(1 - \frac{1}{q-2}\right)\prod_{q|m, q \nmid h}\left(\frac{1}{q^2 - q - 1}\right) & \text{if } m \equiv 1 \bmod 4 \\ 1 & \text{if } m \not\equiv 1 \bmod 4 \end{cases}$$

As can be verified by the patient reader, we then end up with

Conjecture 3.1 $\rho(\alpha) = P(h)(1 + C(h,D) + C(h,2N_0) + C(h,\mathrm{lcm}(D,2N_0)))$.

In particular, $\rho(\alpha)$ *is a rational multiple of* $\prod_{q \text{ prime}}\left(1 - \frac{1}{q(q-1)}\right)$.

These arguments are hueristic in nature but can likely be made precise using the Riemann hypothesis for number fields as in [4]. Recently Heath-Brown has proved the Artin conjecture for all but possibly two primes [3], but his methods do not yield density results.

§4 Towards a reciprocity law.

Suppose that $M \in \mathbb{Z}$ is a non-square with square-free part M_0 and that h is the largest positive integer such that M is an h^{th} power. We define $\rho(M)$ to be the density of primes p for which M is a primitive root - i.e. for which M represents a generator of $\mathbb{Z}/p\mathbb{Z}$. Hooley's result in [4] (assuming the Riemann hypothesis for number fields) is

Proposition 4.1 $\rho(M) = P(h)(1 + C(h,M_0))$. □

Returning to our situation, suppose our conjecture 3.1 is true and that $D \equiv 3 \bmod 4$. Then $2|N$ and hence $N_0 \not\equiv 1 \bmod 4$, so

$$\rho(\alpha) = P(h)(1 + C(h,D)) = \rho(D^h) \tag{5}$$

with $\rho(D^h)$ defined as above. This is a sort of reciprocity law equating the the density of primes with $\ell(p) = p - \chi(p)$ for an exact h^{th} power $\alpha \in K = \mathbb{Q}(\sqrt{D^h})$ with the density of primes for which D^h is a primitive root when $D \equiv 3 \bmod 4$. (Note: both are zero if h is even). This law is only valid as a density statement - the sets of primes involved are different. For example, if $D=3$ and $\alpha = 1+\sqrt{3}$, then $\ell(19) = 9 = 19 - \chi(19)$ but 3 *is* a primitive root mod 19.

Another case where (5) is valid is when $D>0$, $D \equiv 1 \bmod 4$, and $\alpha = \beta^t$ for a fundamental unit $\beta \in \mathcal{O}_K$. Then $h=t$ and $N_0 = N = -1$ is not congruent to 1 mod 4. The Fibonacci numbers fall under this case with $d=5$, $t=1$, and $\beta = \frac{1}{2}(1+\sqrt{5})$.

The correct formulation of a reciprocity law for all D and α and perhaps for arbitrary abelian extensions is an open problem.

Robby Robson, Department of Mathematics, Oregon State University, Corvallis, Oregon, 97331-4605, U.S.A.

References

[1] *The collected papers of Emil Artin.* Addison Wesley, Reading, Mass. (1965). Introduction by S. Lang and J. Tate.

[2] Goldstein, L. J. : Density questions in algebraic number theory. Amer. Math. Monthly 78 (1971) 343-351.

[3] Heath-Brown, D.R.: Artin's conjecture for primitive roots. Quart. J. Math. Oxford (2) 37 (1986) 27-38.

[4] Hooley, C.: On Artin's conjecture. J. für die Reine u. Ang. Math. 225 (1967) 209-220

[5] Lehmer D. H. : An extended theory of Lucas' functions. Ann. of Math (2) 31 (1930) 419-448. Theorem 1.9.

[6] Lucas: Théorie des fonctions numériques simplement périodiques. Amer. J. of Math. 1 (1878) 184-240, 289-321.

[7] Weiss E.: *Algebraic number theory.* McGraw Hill, New York, N.Y. (1963). Chapter 7.

Subject Classification: 10A35, 10A10, 10L10.

Key Words: two-term recurrence relation, Artin conjecture, primitive roots, Fibonacci numbers.

Received August 24, 1987

Proper Differences of Non-Square Powerful Numbers

R.A. Mollin and P.G. Walsh

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

A powerful number is a positive integer n satisfying the property that p^2 divides n whenever the prime p divides n. An integer m is said to be a proper difference of powerful numbers whenever $m = P - Q$ where P and Q are powerful numbers and g.c.d. $(P,Q) = 1$. Although attempts have been made in the literature to prove that every non-zero integer is a proper difference of two non-square powerful numbers, the answers are incomplete. The purpose of this note is to settle the issue.

Introduction

In [7], Mollin and Walsh settled the question for odd integers and provided an effective algorithm for finding the proper differences. In [5] (see also [4] for a summary) McDaniel showed that all non-zero integers are a difference of non-square powerful numbers, but his differences are not proper in general. In particular, in his consideration of the case $n \equiv 0 \pmod 4$, the differences are never proper. It is worthy of note that if proper differences are not required then, for the case $n \equiv 0 \pmod 4$, the result is immediate from the Mollin-Walsh result [6].

In [6] Mollin and Walsh attempted to settle the remaining case; i.e., they wanted to show that every even integer is a proper difference of non-square powerful numbers. Unfortunately, there is a gap in their proof. The problem is as follows. If n is the given even integer then we choose an odd integer $m > n$, relatively prime to n, such that $B = m(m - n)$ is not a perfect square,

$m \equiv 5 \pmod 8$ if $n \equiv 2 \pmod 4$, and $m \equiv 3 \pmod 8$ if $n \equiv 0 \pmod 4$. Let $(x,y) = (T,U)$ be the minimal positive integer solution of $x^2 - By^2 = 1$. Now, they require that for some such B, g.c.d. $(U,B) = 1$. They incorrectly invoke [9, Theorem, p. 57] to achieve this end.

Therefore, to show once and for all that every non-zero integer is a proper difference of two non-square powerful numbers in infinitely many ways we provide a general and complete solution (including a repair of the aforementioned gap in [6]). We also give an effective algorithm for finding these differences and examples to illustrate it. Observe that it suffices to prove the result for either one of n or $-n$.

Proper Non-Square Differences

The key to the general solution of the "proper difference" problem is the following result which is of interest in its own right.

Theorem 1.

Let n be a non-zero integer and let r and s be non-square positive integers. Suppose that the following three conditions are satisfied:

(1) *The diophantine equation* $rx^2 - sy^2 = \pm n$ *has a positive solution in integers* $(x,y) = (A,B)$ *with g.c.d.* $(Ar, Bs) = 1$.

(2) *The diophantine equation* $x^2 - rsy^2 = \pm 1$ *has a positive solution in integers* $(x,y) = (T,U)$ *with g.c.d.* $(U, rs) = 1$.

(3) For positive integers k, let:

$(A\sqrt{r} + B\sqrt{s})(T + U\sqrt{rs})^k = A_k\sqrt{r} + B_k\sqrt{s}$, with $k \equiv -TA(UBs)^{-1} \pmod r$ and $k \equiv -TB(UAr)^{-1} \pmod s$. Then the following two conditions are satisfied:

(4) $A_k \equiv 0 \pmod r$ and $B_k \equiv 0 \pmod s$ with g.c.d. $(rA_k, sB_k) = 1$, for any positive integer k.

(5) $(A_k/r)^2r^3 - (B_k/s)^2s^3 = \pm n$ for all positive integers k.

In other words (4) and (5) say that n is a proper difference of two non-square powerful numbers in infinitely many ways.

Proof. Let $(T+U\sqrt{rs})^k = T_k + U_k\sqrt{rs}$. It is easy to see that

$A_k = AT_k + BsU_k$ and

$B_k = BT_k + ArU_k$. By [7, Lemma, p.34] $A_k = AT_k + BsU_k \equiv AT^k + BskT^{k-1}U \equiv T^{k-1}[AT + BskU] \pmod r$. By (3), $k \equiv -TA(UsB)^{-1} \pmod r$; whence $A_k \equiv 0 \pmod r$. Similarly, $B_k \equiv 0 \pmod s$.

Now suppose that a prime p divides g.c.d. (rA_k, sB_k). Then

(6) $ArT_k + BrsU_k = pc$ for some integer c,

(7) $BsT_k + ArsU_k = pd$ for some integer d.

Multiplying (6) by T_k, (7) by rU_k and subtracting yields: $p[cT_k - drU_k] = Ar[T_k^2 - rsU_k^2] = \pm Ar$. Secondly, if we multiply (7) by T_k, (6) by sU_k and subtract then we get: $p[dT_k - csU_k] = Bs[T_k^2 - rsU_k^2] = \pm Bs$. We have shown that p divides g.c.d. (Ar, Bs) contradicting (1). Hence, g.c.d. $(rA_k, sB_k) = 1$ thereby securing (4). Now we turn to a proof of (5):

$(A_k/r)^2r^3 - (B_k/s)^2s^3 = rA_k^2 - sB_k^2 =$

$(AT_k + sBU_k)^2r - (BT_k + ArU_k)^2s =$

$(A^2r - B^2s)(T_k^2 - rsU_k^2) = (n)(\pm 1) = \pm n.$

Q.E.D.

By Theorem 1, it suffices to find, for each n, an element $A\sqrt{r} + B\sqrt{s}$ with g.c.d. $(Ar, Bs) = 1$ where r and s are positive non-square integers with $A^2r - B^2s = \pm n$; and a solution $T + U\sqrt{rs}$ to $x^2 - rsy^2 = \pm 1$ with g.c.d. $(U, rs) = 1$. The following table gives such elements for all non-zero $n > 0$, (hence for <u>all</u> non-zero n). In the table we write n as a function of $t > 0$. The values $n \in \{1,2,4\}$ are not listed since they represent the special cases $(A,B,r,s,T,U) \in \{(4,5,11,7,351,40), (1,1,5,3,4,1), (1,1,11,7,351,40)\}$ respectively. Note that in the following table, for each of the cases $n = 4t + 2$, $4t$ several choices are given. These choices ensure that r and s are both non-square relatively prime since it is not possible for r and s to be non-square and <u>not</u> relatively prime in all cases simultaneously. Note that the first two lines of the table are the solution to the odd case given by Mollin and Walsh in [7], and the next three lines are the solution to the $n \equiv 2 \pmod 4$ case given by McDaniel [4].

Table 1.

n	A	B	r	s	T	U
$2t+1; t \not\equiv 2 \pmod 5$	1	1	t^2+2t+2	t^2+1	t^2+t+1	1
$2t+1; t \equiv 2 \pmod 5$	$t+1$	1	2	$2t^2+2t+1$	$2t+1$	1
$4t+2$	1	1	$2t^2+4t+1$	$2t^2-1$	$(2t^2+2t-1)^2-1$	$2t^2+2t-1$
$4t+2; t \not\equiv 1 \pmod 3$	1	1	$2t^2+4t+3$	$2t^2+1$	$(2t^2+2t+1)^2+1$	$2t^2+2t+1$
$4t+2; t \equiv 1 \pmod 3$	1	1	$6t^2+8t+3$	$6t^2+4t+1$	$(18t^2+18t+5)^2+1$	$3(18t^2+18t+5)$
$4t; t$ odd	1	1	t^2+2t+2	t^2-2t+2	$(t^6+3t^2)/2$	$(t^4+1)/2$
$4t; t$ even	1	1	$2t^2+2t+1$	$2t^2-2t+1$	$2t^2$	1
$4t; t$ even	1	1	$2t^2+3t+1$	$2t^2-t+1$	$4t^3+2t^2+1$	$2t$
$4t; t$ even	1	1	$2t^2+t+1$	$2t^2-3t+1$	$4t^3-2t^2-1$	$2t$

In all cases the conditions (1) - (3) of Theorem 1 are satisfied, and so we have proved:

Theorem 2. Every non-zero integer is the proper difference of two non-square powerful numbers in infinitely many ways.

Observe that via Table 1 and Theorem 1 we have an effective algorithm for finding these differences, as the following examples illustrate.

Example 1. $n = 3$. We use Table 1, line 1 with $r = 5$, $s = 2$, $T = 3$, and $U = A = B = 1$ to get $(\sqrt{5} + \sqrt{2})(3 + \sqrt{10})^k$ with $k \equiv 1 \pmod{10}$. For $k = 1$ we get $A_k\sqrt{r} + B_k\sqrt{s} = 5\sqrt{5} + 8\sqrt{2}$ and so $3 = 2^7 - 5^3$.

Example 2. $n = 8$. We use Table 1, line 7 with $t = 2$. In this case we form the product $(\sqrt{13} + \sqrt{5})(8 + \sqrt{65})^k$ with $k \equiv 14 \pmod{65}$. For $k = 14$ we get:

$$A_k\sqrt{r} + B_k\sqrt{s} = (4741115028961333\cdot 13)\sqrt{13} + (19876527516465469\cdot 5)\sqrt{5}$$

so that:

$$8 = (4741115028961333)^2\cdot 13^3 - (19876527516465469)^2\cdot 5^3.$$

Remark 1. The choices for r and s in the even cases yield $B = rs = m(m - n)$ where $r = m$ and $s = m - n$. With reference to the discussion given in the introduction this closes the gap in [6, Theorem 2.1, p. 805].

Remark 2. The choices of r and s were made so that rs is of Richaud-Degert type; i.e., of the form $rs = \ell^2 + t$ where t divides 4ℓ and $-\ell < t \leq \ell$. This allows us to write down explicitly the well known fundamental unit of $Q(\sqrt{rs})$. Thus we can guarantee the required G.C.D. conditions.

References

[1] P. Erdős and G. Szerkeres, "Uber die Anzahl der Abelschen Gruppen gegebener Ordnung und Uber ein verwandtes zahlentheoretisches problem" Acta. Litt. Sci. Szeged. (1934), 95-102.

[2] S.W. Golomb, "Powerful Numbers", Amer. Math. Monthly 77 (1970), 848-857.

[3] W.L. McDaniel, "Representations of Every Integer as the Difference of Powerful Numbers", The Fibonacci Quarterly 20 (1982), 85-87.

[4] W.L. McDaniel, "Representations comme la difference des nombres puissants non-carres", C.R. Math. Rep. Sci. Canada 8 (1986), 53-57.

[5] W.L. McDaniel, "Representations of Every Integer as The Difference of Nonsquare Powerful Numbers", Portugaliae Math., 44 (1987), 1-7.

[6] R.A. Mollin and P.G. Walsh, "On Powerful Numbers", Internat. J. Math. and math. Sci. 9 (1986), 801-806.

[7] R.A. Mollin and P.G. Walsh, "On Non-square Powerful Numbers", Fibonacci Quarterly 25 (1987), 34-37.

[8] R.A. Mollin, "The Power of Powerful Numbers", Int. J. Math. and Math. Sci. 10 (1987), 125-130.

[9] I. Slavatsky, "On Mordell's Theorem" Acta. Arith. 11 (1965), 57-66.

[10] C. Vanden Eynden, "Differences between Squares and Powerful Numbers", The Fibonacci Quarterly 24 (1986), 347-348.

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

Received October 7, 1987

Straight Edge Constructions on Planar Cubic Curves

N. S. Mendelsohn, R. Padmanabhan and Barry Wolk
F.R.S.C.

1. Introduction.

In elementary Euclidean geometry constructions using straight edge and compasses play a prominent role. For other second degree curves (conics) there are a few straight edge constructions based on the Pascal-Brianchon theorem which exist in the literature. For higher plane curves the literature appears to be non-existent. Nevertheless, there does exist an interesting class of straight edge constructions to which this paper addresses itself.

2. The Algebra of Cubic Straight Edge Incidence.

We start with some known results. If P and Q are two distinct points on a cubic curve, the line joining P, Q will, in general, meet the curve in a third point R. If the line joining PQ is tangent to the cubic at P then the point R is taken to be P. We introduce a binary operator $\circ$ and put $P \circ Q = R$. It is clear that the following identities hold.

(1) $$P \circ Q = Q \circ P$$

(2) $$P \circ (P \circ Q) = Q$$

A system satisfying identities (1) and (2) has been named in the literature as an extended triple system and sometimes as a non-idempotent Steiner triple system. An important special case of an extended triple system is one which satisfies the medial identity

(3) $$(P \circ Q) \circ (R \circ S) = (P \circ R) \circ (Q \circ S)$$

Systems satisfying the identities (1), (2), (3) also satisfy

(4) $$((P \circ Q) \circ R) \circ S = ((P \circ S) \circ R) \circ Q$$

It is also true that systems satisfying (1), (2), (4) also satisfy (3). A trivial consequence of (1) and (2) is $P \circ Q = R$ iff $P \circ R = Q$. This implies that if $\circ$ is defined on every ordered pair of a set S, then the pair $(S, \circ)$ is a quasigroup. We denote this quasigroup by $Q(S, \circ)$.

If C is a non-degenerate cubic curve defined over a field, and has no singular points (C is an elliptic curve), then it is obvious that $\circ$ is defined on all ordered pairs of points of C and,therefore, the points of C form a quasigroup. In the case of a cubic curve with a singular point, then excluding this point the remaining points also form a quasigroup. A generalization to cubic curves of the Pappus-Pascal-Brianchon theorem

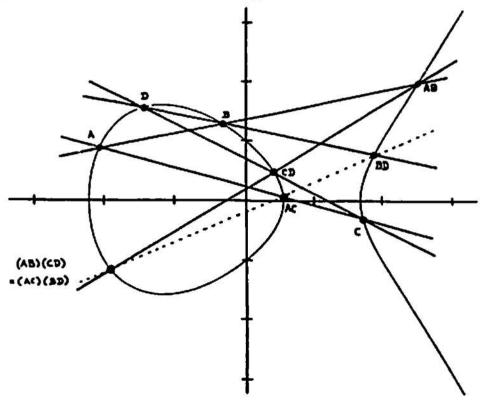


FIGURE 1

implies that the quasigroups in these cases satisfy the medial law (figure 1). A proof of this is found in [2]. If the cubic curve is co-ordinated by a subfield of the reals, we have the notion of a straight edge construction. If P and Q are distinct points on a cubic curve and $R = P \circ Q$ we say that R is obtained by a straight edge construction. A consequence of the medial law is the implication $A \circ B = C \circ D$ implies $A \circ (U \circ C) = (B \circ U) \circ D$ for all U. A derivation of this implication from the Pappus-Pascal-Brianchon theorem for conics is given in [3]. However, the implication can be verified directly and this verification is valid for medial extended triple systems which cannot be associated with a cubic curve. If we put $U = B$ and transfer D to the other side of the equation we obtain $A \circ B = C \circ D$ implies $B \circ B = D \circ (A \circ (B \circ C))$.If now we are given a cubic curve and a point B on it, it is easy to find A, C, D in many ways so that $A \circ B = C \circ D$. In fact, let P be a point on the cubic such that $P \neq B$. Let $A = P \circ B$. (if $A = P$ or $A = B$ choose another point for P). Let C be any other point on the cubic and let $D = P \circ C$ (again if $D = C$ or $D = P$ choose another point for C). Then $P = A \circ B = C \circ D$. In the equation $B \circ B = D \circ (A \circ (B \circ C))$ by avoiding a finite number of choices of P and C we have $B \neq C, A \neq B \circ C$ and $D \neq A \circ (B \circ C)$. Hence the right side of the equation leads to a point obtainable by a straight edge construction. Hence the tangent at a point B is obtainable by a straight edge construction. From this it follows that if $A_1, A_2, \ldots, A_r$ are points on a cubic curve and $P = W(A_1, A_2, \ldots A_r)$ where the right side is a word in the extended triple system algebra, then P is obtainable by a straight edge construction from $A_1, A_2, \ldots, A_r$.

We next look at the connection between medial extended systems and Abelian groups. Let $Q(S, \circ)$ be a medial extended triple system and let e be an arbitrary fixed element of S. Define a system $G(S, +)$ by $a + b = (a \circ b) \circ e$ for $a, b \in S$. Obviously $e + e = e$, and $a + b = b + a$. Now $a+(b+c) = (a\circ((b\circ c)\circ e))\circ e = (((b\circ c)\circ e)\circ a)\circ e$ and $(a+b)+c = (((a\circ b)\circ e)\circ c)\circ e = (((c\circ b)\circ e)\circ a)\circ e$. Hence, $(a+b)+c = a+(b+c)$. Also put $a\circ(e\circ e) = -a$. Then $a+(-a) = (a\circ(a\circ(e\circ e)))\circ e = (e\circ e)\circ e = e$. Hence $G(S, +)$ is an abelian group with identity element e.

Conversely if $G(S, +)$ is an abelian group, define the system $Q(S, \circ)$ by $a \circ b = -a - b$ for all $a, b \in S$. Then identities (1), (2), and (3) are immediately verified and hence $Q(S, \circ)$ is a medial extended triple system. Note that in our definition of $a \circ b$ if e is the identity element of the group then in $Q(S, \circ)$, $e \circ e = e$. If we wish to map $G(S, +)$ into a system $Q(S, \circ)$ in which the identity element e of the group is not idempotent in the corresponding quasigroup, we let e be a free element of the quasigroup and define $a \circ b = -a - b + (e \circ e)$.

Note that if we look at the situation where the quasigroup is defined on a cubic curve C, it is convenient if possible to take a point of inflection as the point e which is used to define addition in an associated group. If we take a set of points on the cubic and and consider the sub-quasigroup generated by straight edge constructions, it does not follow that the point e is generated in the algebra. Hence in the quasigroup $Q(C, \circ)$ a subset of C may generate a subalgebra which does not correspond to a subgroup of $G(C, +)$. Of course if the point e is generated by straight edge constructions from a subset S of C, then the subalgebra generated by S corresponds to a subgroup of $G(C, +)$. The situation is the same even in the case of medial extended system quasigroups which do not arise from cubic curves. The following examples illustrate some of the possibilities.

Example 1. Let C_{3n} be the cyclic group of order $3n$. (This group exists on every non-singular cubic curve over the reals). If we represent the elements of this group by the integers mod $3n$ and put

H = the subgroup of C_{3n} consisting of the integers $\equiv 0 \bmod 3$.

H_1 = the coset consisting of the integers $\equiv 1 \bmod 3$.

H_2 = the coset consisting of the integers $\equiv 2 \bmod 3$.

Then each of H, H_1, H_2 is closed under the operation $x \circ y = -x - y$.

Example 2. Let G be a free abelian group on a set of generators S. Let T be a subset of independent elements of S. Let $a \circ b = -a - b$. Then the elements of the quasigroup generated by T under the operation $\circ$ do not form a subgroup of $G(S, +)$. In fact an easy induction shows that the set of generated elements consists of all finite sums $\sum a_i t_i$ where t_i is in T and the a_i are integers such that $\sum a_i \equiv 1 \bmod 3$.

3. Symmetric Words.

Let $Q(S,\circ)$ be an extended triple system quasigroup. A word $W(a_1,a_2,\dots,a_n)$ is symmetric if it unchanged in value by any permutation of $a_1,a_2,\dots,a_n$. The motivation for studying symmetric words comes from geometric considerations. For instance, if a_1,a_2,a_3,a_4,a_5 are five points on a cubic there is a conic passing through these points. Obviously, this curve is independent of the order in which the points are taken.

Theorem 1. *Let $a_1,a_2,\dots,a_n$ be n free elements in a free extended triple system quasigroup $Q(S,\circ)$. Then if $n \equiv 1 \bmod 3$ or $n \equiv 2 \bmod 3$ there is exactly one equivalence class of symmetric words in the elements $a_1,a_2,\dots,a_n$ in which each of the $a_1,a_2,\dots,a_n$ appears once in any word of the equivalence class. If $n \equiv 0 \bmod 3$ then there is no such symmetric word.*

Proof: Consider the set of words defined inductively as follows;
$W_1 = a_1$, $W_2 = (a_1 \circ a_2)$, $W_4 = (a_1 \circ a_2) \circ (a_3 \circ a_4)$,
$W_5 = ((a_1 \circ a_2) \circ (a_3 \circ a_4)) \circ a_5, \dots$ where $W_{i+1} = W_i \circ a_{i+1}$ if $i \equiv 1 \bmod 3$ and $W_{i+2} = W_i \circ (a_{i+1} \circ a_{i+2})$ if $i \equiv 2 \bmod 3$. We prove that for $i \not\equiv 0 \bmod 3$ each W_i is symmetric in its elements and any symmetric word in $a_1,a_2,\dots,a_i$ of length i is equivalent to W_i. Also if $i \equiv 0 \bmod 3$ there is no symmetric word.

To the quasigroup $Q(S,\circ)$ adjoin an idempotent element e (i. e. take the free product of the one element quasigroup $Q(e,\circ)$ with $Q(S,\circ)$). In this enlarged quasigroup define $a+b = (a\circ b)\circ e$ and hence $a\circ b = -a-b$. Within this group (as in example 2) any word in generators of $Q(S,\circ)$ has the form $\sum n_i a_i$ where $\sum n_i \equiv 1 \bmod 3$. In terms of independent elements $a_i \in S$ the only symmetric words which are generated in which each element appears exactly once are $a_1+a_2+\dots+a_n$ if $n \equiv 1 \bmod 3$ and $-a_1-a_2-\dots-a_n$ if $n \equiv 2 \bmod 3$. Furthermore no word is generated if $n \equiv 0 \bmod 3$. An easy induction shows that $W_n = a_1+a_2+\dots+a_n$ if $n \equiv 1 \bmod 3$ and $W_n = -a_1-a_2-\dots-a_n$ if $n \equiv 2 \bmod 3$. In fact, these are the precise group expressions one would obtain for W_n if one were dealing with the one dimensional complex torus group which is the underlying group of a complex cubic.

There are alternative bracketings which yield the same valued word as W_n. Some may be obtained simply by the application of the commutative law. But some have a greater interest. For instance, if $n \equiv m \not\equiv 0 \bmod 3$, then it is easily deduced that
$W_n(a_1,a_2,\dots,a_n)\circ W_m(a_{n+1},a_{n+2},\dots,a_{n+m}) = W_{n+m}(a_1,a_2,\dots a_{n+m})$.

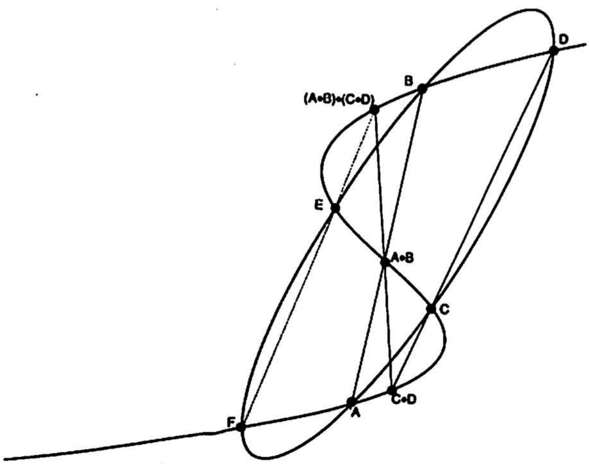


Figure 2

4. Some Geometrical Interpretations.

Consider a real cubic curve C drawn in the plane but in which the inflection points are not marked. We examine three examples of straight edge constructions.

Example 3. Let a_1, a_2, a_3, a_4, a_5 be five distinct points on the cubic C. Through a_1, a_2, a_3, a_4, a_5 there exists a unique conic section which meets the cubic in a sixth point x. In fact $x = W_5(a_1, a_2, a_3, a_4, a_5)$. Note this requires the drawing of only four straight lines as illustrated in figure 2. A proof is based on a consequence of the Pascal-Brianchon theorem and appears in [3]. Note that if three of a_1, a_2, a_3, a_4, a_5 are collinear the conic degenerates into two straight lines and the construction requires the drawing of one line only.

Example 4. Let $a_1, a_2, \ldots, a_8$ be eight distinct points on a cubic curve. Through these points pass an infinite number of cubic curves all of which pass through a fixed point x. In fact, $x = W_8(a_1, a_2, \ldots, a_8)$. This construction requires the drawing of only seven lines (see figure 3).

Example 5. We look at two geometric interpretations of the word $W_{10}(a_1, a_2, \ldots, a_{10})$ where the points a_i are on a cubic curve. Consider the two identities

$$W_{10}(a_1, a_2, \ldots, a_{10}) = W_8(a_1, a_2, \ldots, a_8) \circ W_2(a_9, a_{10}) \tag{5}$$

$$W_{10}(a_1, a_2, \ldots, a_{10}) = W_5(a_1, a_2, \ldots, a_5) \circ W_5(a_6, a_7, \ldots, a_{10}) \tag{6}$$

Equation (5) is interpreted as follows. The ten points are arbitrarily partitioned into disjoint subsets of eight and two points, respectively. The line joining the latter two points meets the cubic in the point x (say). The remaining eight points are the vertices of a pencil of cubics all of which pass through a ninth point y. The point W_{10} is the point where the line through x and y meets the cubic.

The interpretation of equation (6) is geometrically very different. Here the ten points are partitioned into two disjoint sets of five points. Each of these sets define conics which meet the cubic again in points x and y. Again the point W_{10} is the intersection of the line through x and y and the cubic.

The following theorem of Cayley-Bacharach (see [7]) is particularly germane to the concept of straight edge construction. We state this theorem in its most general form.

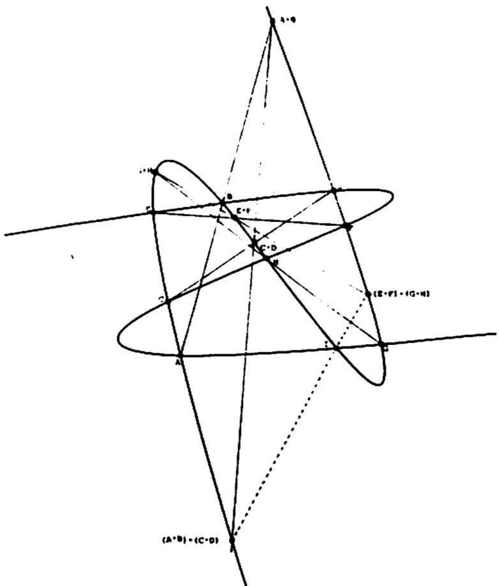


Figure 3

Cayley-Bacharach Theorem. *Let F and G be plane curves of degree m and n, respectively such that they intersect in mn distinct points. Then any curve H of degree $m+n-3$ passing through all but one point of $V(F) \cap V(G)$ also passes through the remaining point.*

This theorem leads to the following interpretation of W_{3n-1} which we state as theorem 2 without proof.

Theorem 2. *Let C be a plane cubic curve and let G be a curve of degree n such that C and G meet in $3n$ points $a_1, a_2, \ldots, a_{3n}$. Then any curve of degree n which passes through $a_1, a_2, \ldots, a_{3n-1}$, also passes through a_{3n} and in fact $a_{3n} = W_{3n-1}(a_1, a_2, \ldots, a_{3n-1})$.*

Examples 3 and 4 are special cases of theorem 2. They were included because they are needed for the interpretation of example 5.

5. An Algebraic Characterisation of the Geometric Processes.

In this section we give two types of results characterizing, respectively, the binary and the quintic geometric processes discussed above by means of formal algebraic conditions. It is easily seen that the (3n-1)-ary case can be handled in the same manner.

Theorem 3. *Let $\star$ be a rational binary operation defined on a non-singular cubic curve in the complex projective plane. Then $x \star y = x \circ y$, the binary law of composition obtained by the process of the chord-tangent construction iff the binary algebra $(\Gamma; \star)$ is an extended triple system and $e \star e = e$ for some inflection point e of the curve Γ.*

Proof: As mentioned before $\circ$ does define an extended triple system on Γ and the tangent at every inflection point e has triple contact with the curve and hence by the very definition of the operation $\circ$, we have $e \circ e = e$ for all inflection points e of the cubic.

Conversely, let $\star$ be a binary rational function defining an extended triple system on Γ and let $e \star e = e$ for some inflection point e of the curve Γ. Form the 4-ary composite rational function
$f(x,y,z,t) = ((x \star y) \star z) \circ (t \circ ((x \circ y) \circ z))$. Now
$f(x,b,b,t) = ((x \star b) \star b) \circ (t \circ ((x \circ b) \circ b)) = x \circ (t \circ x) = t$ and hence f does not depend upon the value of x for the special choice of $y = z = b$ and hence by the "local $\Rightarrow$ global" principle (Cf Lemma 1 of [3] or §2 of [2]), the function f does not depend on x for all values of y, z, t. In other words, we have the global identity $f(x,y,z,t) = f(u,y,z,t)$. Substituting $u = z$ we get that $f(x,y,z,t) = t$ and hence
$((x \star y) \star z) \circ (t \circ ((x \circ y) \circ z)) = t = ((x \circ y) \circ z) \circ (t \circ ((x \circ y) \circ z))$.
Now cancelling the common term $(t \circ ((x \circ y) \circ z))$ we get the basic link between $\star$ and $\circ$, namely,

$$(x \star y) \star z = (x \circ y) \circ z \tag{7}$$

Substituting $x = y = e$ and $z = u \circ v$ we get $e \star (u \circ v) = e \circ (u \circ v)$, and hence, by (7) again, $e \star (u \circ v) = e \star (u \star v)$ for all u, v in Γ.

Cancelling the common element e on both sides of the above equality, we get the desired conclusion that the binary function $u \star v$ is indeed equal to $u \circ v$, the chord-tangent operation. This completes the proof of the theorem.

Using similar reasoning one can prove an analogous result for the 5-ary conic process as given in example 3. We state this result without proof as follows.

Theorem 4. *Let Γ be a non-singular complex cubic curve, and let e be a fixed point of inflection on Γ. A 5-ary rational function Φ defined on Γ is the same as obtained by the 5-ary conic process iff Φ is symmetric in all its five arguments and satisfies the following two identities:*

$$\Phi(\Phi(x,y,e,e,e), x, e, e, e)) = y \tag{1}$$

$$\Phi(e,e,e,e,e) = e \tag{2}$$

References

(1) N. S. Mendelsohn, R. Padmanabhan and B. Wolk, *Planar Projective Configurations*, to appear in Note di Mathematica.

(2) N. S. Mendelsohn, R. Padmanabhan and B. Wolk, *Designs Embeddable in a Planar Cubic Curve*, to appear in Note di Mathematica.

(3) N. S. Mendelsohn, R. Padmanabhan and B. Wolk, *A Ruler Construction on Cubics via Equational Logic*, submitted to Algebra Universalis.

(4) N. S. Mendelsohn, R. Padmanabhan and B. Wolk, *Representation of Desargues and Pappus like Configurations*, submitted to Finite Geometries and Combinatorial Designs.

(5) E. Mendelsohn, N. S. Mendelsohn, R. Padmanabhan and B. Wolk, *Decomposition of Prime Clusters on Complex Cubic Curves*, Congressus Numerantium 57 (1987) 55–61.

(6) N. S. Mendelsohn, R. Padmanabhan and B. Wolk, *Some Remarks on n-Clusters on Cubic Curves*, to appear.

(7) Makato Namba, *Geometry of Projective Algebraic Curves*, Marcel Decker, New York 1986, page 74 Theorem 1.4.19

The research of all three authors was supported by the NSERC of Canada

Department of Mathematics and Astronomy
University of Manitoba
Winnipeg, Canada, R3T 2N2.

Received November 18, 1987

SAMPLE PATH PROPERTIES OF THE SUPPORT PROCESS OF SUPER-BROWNIAN-MOTION

D.A. Dawson F.R.S.C.(1), I. Iscoe(2) and E.A. Perkins(3)

ABSTRACT

Properties of the support process of super-Brownian motion are studied. In particular results on the exact Hausdorff measure of the range, the probability of hitting sets and the non-existence of multiple points in high dimensions are obtained.

1. INTRODUCTION.

Let $M_F(R^d)$ denote the space of finite measures on $(R^d, \mathcal{B}(R^d))$ furnished with the topology of weak convergence. Let $\{S_t : t \geq 0\}$ denote the semigroup of operators on $C(R^d)$ associated with d-dimensional Brownian motion. For $\varphi \in C(R^d)^+$, let $u(t,x)$ denote the unique solution of

$$(1.1)\quad u(t,x) = S_t\varphi(x) - (1/2)\int_0^t S_{t-s}\left[u(s,.)^2\right]ds,\ u(0,x) = \varphi(x).$$

The super-Brownian-motion is a continuous $M_F(R^d)$-valued Markov process X_t which is uniquely determined by the conditional Laplace functional

$$E\left[\exp(-\int\varphi(x)dX_t(x))\,\middle|\,X_s=m\right] = \exp(-\int u(t-s,x)dm(x))$$

for $t > s$ (cf. Watanabe [8]). The law of X on $\Omega = C([0,\infty), M_F)$ with $X(0) = m$ is denoted by Q^m.

For $\omega \in \Omega$, the closed support of $X_t(\omega)$ is denoted by $S(X_t(\omega))$. For $I \subset [0,\infty)$, the range of the support process

$R(I) := \bigcup_{t\in I} S(X_t)$. Let $\bar{R}(I)$ denote the closure of $R(I)$ and

---

(1),(2),(3) Research supported by NSERC.

$\bar{R}^+((r,s]) := \bigcup_{u>r} \bar{R}((u,s])$.

2. HÖLDER RIGHT CONTINUITY

If $A \subset R^d$ and $r > 0$, let $A^r = \{x:d(x,A) \le r\}$ where $d(x,A) := \inf_{y\in A} |x-y|$.

THEOREM 2.1. *Let* $m \in M_F(R^d)$. *Then for* Q^m-a.e. ω *and each* $c > 2$ *there is a* $\delta(\omega,c)$ *such that if* $s,t \ge 0$ *satisfy* $0 < t-s < \delta(\omega,c)$, *then*

$$S(X_t(\omega)) \subseteq S(X_s(\omega))^{c.h(t-s)}$$

where $h(t) := \left[t((\log \frac{1}{t})\vee 1)\right]^{1/2}$.

If K_1 and K_2 are compact subsets of R^d,

$$\rho_1(K_1,K_2) := \sup_{x\in K_1} d(x,K_2)$$

Then

$$\rho(K_1,K_2) := \max\left[\rho_1(K_1,K_2),\rho_1(K_2,K_1)\right]$$

is the Hausdorff metric on $K(R^d)$, the collection of compact subsets of R^d. The continuity of X and compactness of the support of X_t for $t>0$ (the latter follows easily from Theorem 2.1) imply that

$$Q^m\left[\lim_{s\to t} \rho_1(S(X_t),S(X_s)) = 0 \text{ for all } t>0\right] = 1.$$

The above theorem yields the following.

COROLLARY 2.2. *The* $K(R^d)$*-valued process* $S(X_t)$ *is right continuous in the Hausdorff metric*, Q^m-a.s.

REMARK. Theorem 2.1 follows from a sample path Hölder continuity property for a non-standard model of the measure-valued process

X_t which is established in [1]. The latter result is shown to be false for $c<2$.

3. THE RANGE OF THE SUPPORT PROCESS AND THE OCCUPATION-TIME PROCESS.

For $r < s$ the weighted occupation time is defined as

$$Y_{r,s}(A) := \int_r^s X_u(A)du .$$

Note that $\bar{R}((r,s))$ is the closed support for the measure $Y_{r,s}$.

Let $\psi(x) = x^4\log^+\log^+\frac{1}{x}$ where $\log^+(u) = (\log u)\vee 0$, $\psi_0(x) = x^4\log^+\frac{1}{x}$ and $\psi_4(x) = \psi_0(x)\log^+\log^+\frac{1}{x}$. Hausdorff ψ-measure is denoted by ψ-m.

THEOREM 3.1. (a) Let $d > 4$. There are constants $c_{3.1}(d)$ and $c_{3.2}(d)$ such that for all $m \in M_F(R^d)$ and for Q^m-a.e. ω,

$$(3.1)\quad c_{3.1}(d)\psi\text{-m}(\bar{R}((r,s))\cap A) \le Y_{r,s}(A) \le c_{3.2}(d)\psi\text{-m}(\bar{R}((r,s))\cap A)$$

$$(3.2)\quad c_{3.1}(d)\psi\text{-m}(\bar{R}^+((0,s))\cap A) \le Y_{0,s}(A) \le c_{3.2}(d)\psi\text{-m}(\bar{R}((0,s))\cap A)$$

for all $A \in \mathcal{B}(R^d)$ and all $0 < r \le s \le \infty$.

(b) Let $d = 4$. There is a constant $c_{3.2}(4)$ such that for all $m \in M_F(R^d)$ and Q^m-a.e. ω,

$$Y_{r,s}(A) \le c_{3.2}(4)\psi_4\text{-m}(\bar{R}((r,s))\cap A) \quad \text{for all } A \in \mathcal{B}(R^d),\ 0 \le r \le s \le \infty$$

$$\psi_0\text{-m}(\bar{R}((r,\infty))) < \infty \quad \text{for all } r > 0.$$

4. ASYMPTOTICS FOR THE PROBABILITY OF HITTING SMALL BALLS

Let $B(x_0;\epsilon)$ denote the ball of radius ϵ and center x_0. The next result gives the asymptotics as $\epsilon\downarrow 0$ for the probability that the ball has positive mass at a fixed time.

THEOREM 4.1. Let $d \ge 3$, $t_0 > 0$, $x_0 > 0$ be fixed. There is a constant C_d such that as $\epsilon \to 0^+$,

$$Q^m(X_{t_0}(B(x_0;\epsilon)) > 0) \sim C_d.\epsilon^{d-2}\left[\int_{R^d} p(t_0,x-x_0)dm(x)\right].$$

The following estimates for the probability of hitting a ball of radius ϵ are based on Iscoe [4].

THEOREM 4.2.

(a) Assume $d > 4$. There is a constant $c_{4.1}$ and a positive sequence $\{\epsilon_k\}$ converging to zero (and depending only on d) such that if $d(x,\text{supp}(m)) > k\epsilon$ and $k\int|y-x|^{2-d}dm(y) < \epsilon^{4-d}$, then

$$(1-\epsilon_k)c_{4.1}\epsilon^{d-4}\int|y-x|^{2-d}dm(y) \le Q^m(X_t(B(x;\epsilon)) > 0 \text{ for some } t \ge 0)$$

$$\le (1+\epsilon_k)c_{4.1}\epsilon^{d-4}\int|y-x|^{2-d}dm(y) \;.$$

(b) Assume $d = 4$, $d(x,\text{supp}(m)) > (k\epsilon)\vee\epsilon^{1/k}$ and $k\int|y-x|^{-2}dm(y) < \log\frac{1}{\epsilon}$, then

$$(1-\epsilon_k)2\left[\log\frac{1}{\epsilon}\right]^{-1}\left[\int|y-x|^{-2}dm(y) - \epsilon^{2/k}m(R^d)\right]$$

$$\le Q^m(X_t(B(x;\epsilon)) > 0 \text{ for some } t \ge 0)$$

$$\le (1+\epsilon_k)2\left[\log\frac{1}{\epsilon}\right]^{-1}\int|y-x|^{-2}dm(y) \;.$$

Theorem 4.1 yields the following.

COROLLARY 4.1. Let $d \ge 3$. If x^{d-2}-$m(A) = 0$, then $Q^m(A\cap S(X_t) = \phi) = 1$ for all $t > 0$.

The process X is said to hit $A \subseteq R^d$ if $A\cap\bar{R}^+((0,\infty)) \ne \phi$. In dimensions $d \le 3$ it follows from the existence of local times (Iscoe [3], Sugitani [[7]) that X hits points. Moreover

$$Q^m(X \text{ hits } \{x\}) = 1 - \exp\left[-2(4-d)\int |y-x|^{-2} dm(y)\right].$$

In higher dimensions Theorem 4.2 yields the following.

COROLLARY 4.2. _Let_ $d > 4$ _and_ x^{d-4}-$m(A) = 0$. _Then_ X _does not hit_ A Q^m-a.s. _for any_ $m \in M_F(R^d)$.

COROLLARY 4.3. _Let_ $d = 4$ _and_ $\left[\log \frac{1}{x}\right]^{-1}$-$m(A) = 0$. _Then_ X _does not hit_ A Q^m-a.s. _for any_ $m \in M_F(R^d)$.

The set of _k-multiple points_ is defined by

$$R_k := \{x: x \in \bigcap_{i=1}^{k} \bar{R}(I_i), \text{ for some } I_1,\ldots,I_k \text{ disjoint compact intervals in } (0,\infty)\}$$

COROLLARY 4.4. _Let_ $d \geq 5$ _and_ $k \geq \frac{d}{d-4}$. _Then_ $\tilde{R}_k = \phi$ a.s.

REMARKS. (1) In particular this implies that X does not have self-intersections in dimensions $d \geq 8$.
(2) Perkins [6] has shown the existence of intersections of order k if $k < \frac{d}{d-4}$ and determined the Hausdorff dimensions of the sets Γ_k. Also Dynkin [2] has established the existence of self-intersection local times of order k for $k < \frac{d}{d-4}$.
(3) The proofs of Theorems 2.1, 3.1, 4.1 and 4.2 are given in Dawson, Iscoe and Perkins [1].

REFERENCES

[1] D.A. Dawson, I. Iscoe and E.A. Perkins, in preparation.

[2] E.B. Dynkin. Representation for functionals of superprocesses by multiple stochastic integrals with applications to self-intersection local times, preprint.

[3] I. Iscoe. A weighted occupation time for a class of measure-valued branching processes, Probab. Th. Rel. Fields 71(1986), 85-116.

[4] I. Iscoe. On the supports of measure-valued critical branching Brownian motion, Annals of Probability, to appear.

[5] E.A. Perkins. A space-time property of a class of measure-valued branching diffusions, to appear.

[6] E.A. Perkins, in preparation.

[7] S. Sugitani. Some properties for the measure-valued branching diffusion process, preprint.

[8] S. Watanabe. A limit theorem of branching processes and continuous state branching processes, J. Math. Kyoto Univ. 8 (1968), 141-167.

(1) Department of Mathematics and Statistics, Carleton University, Ottawa, Canada K1S 5B6.

(2) Department of Mathematics and Statistics, McGill University, Montreal, Canada H3A 2K6.

(3) Department of Mathematics, The University of British Columbia, Vancouver, Canada V6T 1Y4.

Received December 7, 1987

A MODEL FOR COQUAND'S THEORY OF CONSTRUCTIONS

François Lamarche

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

In [6] we introduced the concept of semigranular category with the goal of extending Girard's model of the second order λ calculus [4] to higher types. In this announcement we use the same raw material to produce a model of Coquand's theory of constructions [1]. Due to space limitations we cannot cover the syntactical aspect of the theory. A detailed account of everything is being written up.

When examining the theory of constructions, one discerns the following features: there are "type-like" constructions of two sizes: small sets (called propositions) and classes (e.g. the type Prop of all sets). There are "term-like" constructions corresponding to mappings between sets or classes. There is the capability of defining dependent types à la Martin-Löf, corresponding to indexed families $(Y_x)_{x \in X}$ where Y_x, X may be either sets or classes, and finally there is the Π operator allowing us to take the product $(\Pi_{x \in X}) Y_x$ of a family; the power of the system comes from the fact that the product of a family of sets is always a set, regardless of whether the indexing type is a set or a class.

Let $\mathbb{C}$ be a category which has multicoproducts [2] and all of whose morphisms are mono. We say a discrete cocone $(x_i : X_i \to Y)_{i \in I}$ in $\mathbb{C}$ is a *sum candidate* if it belongs to a multicoproduct family, i.e.

if $(x_i)_i$ is initial in its component of $\mathrm{Cocone}(X_i)_i$. Similarly a single object W is *empty* if it is initial in its component of $\mathbb{C}$. An object X of $\mathbb{C}$ is *finitely presentable* (f.p.) [8] if the representable functor $\mathrm{Hom}(X,-)$ preserves filtered colimits. X is said to be *prime* if it is not empty, and given any sum candidate $(x_i:X_i\to X)_{i\in I}$ with vertex X there is $i\in I$ such that x_i is an isomorphism. X is *atomic* if it has exactly two subobjects. Atoms are prime.

Definition: A category $\mathbb{C}$ is called an *aggregate* (resp. a *semigranular* category) if

- all morphisms are mono.
- it has multicoproducts and filtered colimits.
- it has a strong generating set made of f.p. prime objects with finite subobject lattices (resp. f.p. atomic objects)
- if $(x_i:X_i\to X)_{i\in I}$ is a sum candidate in $\mathbb{C}$ with $f:A\to X$ where A is prime then there is $i\in I$ and $g:A\to X_i$ with $x_i g = f$.

An aggregate is always a locally $\aleph_0$-multipresentable category [3], and therefore it is multicocomplete and has connected limits. We say a functor $F:\mathbb{C}\to\mathbb{D}$ between aggregates is *entire* if it preserves filtered colimits and pullbacks. Let $A\in\mathbb{D}$. We say an object (X,x) of A/F (i.e. $x:A\to FX$) is a *generic* arrow (cf. [5]) if given any diagram of the form

$$(X,x)\longrightarrow(Y,y)\longleftarrow(Z,z)$$

in A/F there exists a (necessarily unique) $(X,x)\to(Z,z)$ making the triangle commute.

Proposition: <u>If $\mathbb{C},\mathbb{D}$ are aggregates then $F:\mathbb{C}\to\mathbb{D}$ is entire iff</u>

for any prime $A \in \mathbb{D}$, any $y : A \to FY$ there exists a generic $x : A \to FX$ where X is f.p. and a morphism $(X,x) \to (Y,y)$ in A/F.

Given a family $(\mathbb{C}_i)_{i \in I}$ of aggregates (semigranular categories) their product $\Pi_i \mathbb{C}_i$ is an aggregate (semigranular) and is the categorical product for entire functors as morphisms. In particular the one object category $\mathbb{1}$ is semigranular and terminal for entire functors.

In our model (non variable) classes will be interpreted as semigranular categories. A small set will be interpreted as a (possibly empty) semigranular poset whose multicoproduct families are all singletons or empty, that is, as an atomic Scott domain [7], or equivalently as a qualitative domain [4] where the empty semilattice of subsets is allowed. We will use the term qualitative domain to cover those three equivalent entities. Terms between classes will be interpreted as entire functors. We are left to interpret variable terms. It is a standard practice of category theory to consider a "family $(Y_x)_{x \in X}$ of objects of a category indexed by object X" as a morphism $Y \to X$ in the category where Y corresponds to the disjoint sum $\coprod_x Y_x$. Such a morphism will be interpreted in our case as a special kind of fibration $\mathbb{E} \to \mathbb{C}$. For every $S \in \mathbb{C}$ the fiber $\mathbb{E}^S$ will be a semigranular category, and so $\mathbb{E}$ will be a lot like "a disjoint union of semigranular categories". Even if $\mathbb{C}$ is semigranular, $\mathbb{E}$ will not be semigranular, but only an aggregate. Since the syntax of the theory forces us to have towers $\mathbb{E}_n \to \mathbb{E}_{n-1} \to \ldots \to \mathbb{C}$ of fibrations it is natural to develop the theory when the base category $\mathbb{C}$ is an aggregate.

Definition: Let $\mathbb{C}$ be an aggregate. A *semigranular fibration* is a category $E:\mathbb{E}\to\mathbb{C}$ above $\mathbb{C}$ such that

- E is both a fibration and an opfibration (i.e. for every $s:S\to T$ in $\mathbb{C}$, any splitting $s^*:\mathbb{E}^T\to\mathbb{E}^S$ for s has a left adjoint $\exists_s$).
- Every fiber is a semigranular category.
- Every cocartesian arrow is also cartesian ($\exists_s$ is always full and faithful).
- If $A\in\mathbb{E}^S$ is atomic in its fiber and $a:A\to B$ a cocartesian arrow then B is atomic in its fiber ($\exists_s$ sends atoms to atoms).

We will call an object of $\mathbb{E}$ which is atomic in its fiber a *semiatom*. Since E is an opfibration it can be thought of as a covariant functor from $\mathbb{C}$ to the category of all semigranular categories (with morphisms embeddings sending atoms to atoms and that have a coreflector). We need an additional condition making this functor *entire*.

Definitions: an object X of $\mathbb{E}$ is said to be E-*generic* if given any diagram $X\longrightarrow Y\longleftarrow Z$ of cocartesian arrows there exist a (necessarily unique and also, it turns out, cocartesian) morphism $X\to Z$ making the triangle commute. E is an *entire fibration* if for every semiatom A of $\mathbb{E}$ there exists an E-generic X and a cocartesian arrow $X\to A$.

Theorem: If $E:\mathbb{E}\to\mathbb{C}$ is an entire fibration above aggregate $\mathbb{C}$ then $\mathbb{E}$ is an aggregate and E is entire.

We denote by $\mathrm{Fib}(\mathbb{C})$ the category whose objects are entire fibrations above $\mathbb{C}$ and where a morphism from $E:\mathbb{E}\to\mathbb{C}$ to $F:\mathbb{F}\to\mathbb{C}$ is an entire functor $H:\mathbb{E}\to\mathbb{F}$ with $FH=E$. We write $\mathrm{Fib}(\mathbb{C})(E,F)$ for the category whose objects are the functors H as above and where a morphism $\varphi:H\to H'$ is a cartesian natural transformation φ such that $F\varphi=1_E$ (φ is *cartesian* if for any $f:X\to Y$ in $\mathbb{E}$ the commutative square defining naturality for f is a pullback).

Theorem: $\mathrm{Fib}(\mathbb{C})(E,F)$ is a semigranular category.

If $\mathbb{A}$ is a semigranular category the constant fibration $\mathbb{C}\times\mathbb{A}\to\mathbb{C}$ is in $\mathrm{Fib}(\mathbb{C})$. We write $\mathrm{Fib}_s(\mathbb{C})$ for the full subcategory of $\mathrm{Fib}(\mathbb{C})$ whose objects are small-fibered entire fibrations, i.e. where every fiber is a qualitative domain. If $\mathbb{D}$ is another aggregate and $K:\mathbb{D}\to\mathbb{C}$ an entire functor then the (standard on-the-nose) pullback of any entire fibration above $\mathbb{C}$ is an entire fibration above $\mathbb{D}$, and this defines a functor $D^*:\mathrm{Fib}(\mathbb{C})\to\mathrm{Fib}(\mathbb{D})$ which as usual corresponds to substitution in syntax. One shows thus $\mathrm{Fib}(\mathbb{C})$ has finite products.

Theorem: D^* has a right adjoint Π_D which sends small-fibered fibrations to small-fibered ones.

A consequence of this is that $\mathrm{Fib}(\mathbb{C})$ and $\mathrm{Fib}_s(\mathbb{C})$ are always cartesian closed, and in particular $\mathrm{Fib}(\mathbb{1})$, the category of semigranular categories and entire functors. One takes F^E to be $\Pi_F(F^*E)$. Let $G:\mathbb{G}\to\mathbb{D}$ be in $\mathrm{Fib}(\mathbb{D})$. $\Pi_D(G)$ is calculated "pointwise" in the sense that for $S\in\mathbb{C}$ the fiber above S will be the semigranular category $\mathrm{Fib}(\mathbb{D}^S)(1_{\mathbb{D}^S},I^*G)$, where $I:\mathbb{D}^S\to\mathbb{D}$ is the inclusion of the fiber; in other words, it is the class of all splittings $W:\mathbb{D}^S\to\mathbb{G}$, $GW=1_{\mathbb{D}^S}$, just as for sets.

We are left to describe the class $\mathbb{P}$ of all sets and its associated entire fibration $H: \mathbb{H} \to \mathbb{P}$ which classifies all such small fibrations. If qD is Girard's category of qualitative domains and morphisms thereof [4], $\mathbb{P}$ is the disjoint union $qD+\mathbb{1}$, where one isolated object is added to take care of the empty qualitative domain. It is easy to see that a morphism of qualitative domains is the same as an embedding of the posets which sends atoms to atoms and has a right adjoint, and therefore there is a natural small entire fibration $H: \mathbb{H} \to \mathbb{P}$ which is such that for any $E: \mathbb{E} \to \mathbb{C}$ in $Fib_s(\mathbb{C})$ there exists $K: \mathbb{C} \to \mathbb{P}$ with $H \cong K^*H$. This is the semantical counterpart of the fact that a (variable or not) set is a term of type Prop.

References

[1] T. COQUAND Une théorie des constructions, *Thèse de 3 eme cycle*, Paris VII (1985).

[2] Y. DIERS Familles universelles de morphismes, *Ann. Soc. Sci. Bruxelles*, 93-III (1979) 175-195.

[3] Y. DIERS Catégories localement multiprésentables, *Arch. Math.* 34 (1980) 344-356.

[4] J.-Y. GIRARD The system F of variable types fifteen years later, *Theoret. Comp. Sci.* 45 (1986) 159-192.

[5] A. JOYAL Foncteurs analytiques et espèces de structures, *Lect. Notes Math.* 1234, Springer (1987) 126-159.

[6] F. LAMARCHE Extending Girard's model to the higher order lambda calculus, *A.M.S. Abstracts*, Vol 8, N. 8 (Nov 1987)

[7] D. S. SCOTT Domains for denotational semantics, *Lect. Notes Comp. Sci.* 140, Springer (1982).

[8] F. ULMER Locally α-presentable and locally α-generated categories, *Lect. Notes Math.* 195, Springer (1971) 230-247

Department of Mathematics and Statistics
McGill University
Montréal, Québec, Canada H3A 2K6

Received December 8, 1987

Simple zeros of the Dirichlet series formed with Ramanujan's tau-function

J.B. Conrey* and A. Ghosh**

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

Let

$$L(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$$

where τ denotes Ramanujan's tau-function. The series is absolutely convergent for $\sigma > 13/2$ and defines an entire function $L(s)$. It is known that $L(s)$ has real zeros at $s = 0, -1, -2, \ldots$ and that all other zeros are non-real. The non-real zeros are symmetric about the real axis and about the line $\sigma = 6$. It is conjectured that they all lie on the line $\sigma = 6$, i.e., that $L(s)$ satisfies a Riemann Hypothesis. It is known that they all lie in the strip $11/2 < \sigma < 13/2$ and the number of them with ordinates in $(0,T)$ is

$$\frac{T}{\pi} \log \frac{T}{2\pi e} + O(\log T) .$$

---

* Research supported by the Alfred P. Sloan Foundation and the NSF.

** Research supported by the NSF.

Little else is known about the vertical distribution of the zeros. In particular, all that is known about multiplicities of zeros is that the multiplicity of a zero in $0 < t < T$ cannot be larger than a constant times log T.

We remark that there are other Dirichlet series which are known to have infinitely many simple zeros. In fact, a positive proportion of the zeros of the Riemann zeta-function are known to be simple via Levinson's method (see Heath-Brown [4]), and the same result holds for Dirichlet L-functions. Also, the authors and S. Gonek [1] have used a different method to show that the Dedekind zeta function of a quadratic extension of the rationals has at least $T^{6/11}$ simple zeros in the rectangle $0 < \sigma < 1$, $0 < t < T$ if T is sufficiently large.

We are able to show that infinitely many of the non-real zeros of $L(s)$ are simple zeros. In fact, we have a stronger result:

Theorem. For any $\epsilon > 0$ and any $T_0 > 0$ there is a $T \geq T_0$ such that $L(s)$ has at least $T^{1/6-\epsilon}$ simple zeros in the rectangle $11/2 < \sigma < 13/2$, $0 < t < T$.

Our theorem here uses a different method than those mentioned above. The idea of the proof is as follows. Let $\rho = \beta + i\gamma$ denote a zero of $L(s)$. We prove a formula which, roughly speaking, has the shape

$$(*) \qquad \sum_{0<\gamma<T} a(\rho)L'(\rho)\Gamma(\rho)e^{-\pi i\rho/2} \approx \sum_{0<\gamma<\log T} L'(\rho)a(\rho)\Gamma(\rho)T^{\rho} ,$$

where $a(\rho)$ is an innocuous factor. The proof of (*) depends on the functional equation satisfied by $L(s)$, on the fact that $\Gamma(s)$ and $\exp(x)$ are Mellin transforms, and on the periodicity of the exponential function. The proof proceeds somewhat like the proof of an "explicit formula" from classical prime number theory.

If no zeros are simple then both sides of (*) are identically 0 . We prove that $L(s)$ does have at least one simple zero. This requires a special calculation and, to a certain extent, limits the generality of our method. Now let θ be the supremum of the real parts of simple zeros of $L(s)$. We prove that for any $\epsilon > 0$ and any $T_0 > 0$ there are values of $T \geq T_0$ such that the right side of (*) is $\geq T^{\theta-\epsilon/2}$. To do this we use Cauchy's theorem to relate the right hand side to an arithmetic sum involving-the coefficients $\tau(n)$ (again, like an explicit formula). Then we use Landau's theorem on the existence of a singularity on the real axis at the abscissa of convergence of a Dirichlet series (or integral) with non-negative coefficients to show that the arithmetic sum cannot always be small. Next by the use of Good's upper estimate for $L(s)$ (see [3]) and standard bounds for the gamma function, it follows that the individual terms of the left side of (*) are bounded from above by

$$T^{(12+\theta)/3 - 1/6+\epsilon/2}$$

for any $\epsilon > 0$. Thus, the left hand side of (*) must have at least

$$T^{(2\theta-12)/3 + 1/6-\epsilon}$$

non-zero terms for appropriate T . By the symmetry of the zeros, $\theta \geq 6$ from which the result follows.

More generally, suppose that $F(s)$ is represented by a Dirichlet series and an Euler product in some half-plane and that $F(s)$ satisfies a functional equation, say $H(s)F(s)$ is real on some vertical line $\sigma = k$ where

$$H(s) = CA^s \prod_{n=1}^{N} \Gamma(\alpha_n s+\beta_n)$$

for some positive numbers A and α_n and some complex numbers C and β_n . Our method should give the result that if $\sum_{n=1}^{N} \alpha_n \leq 1$ and if $F(s)$ has at least one non-real simple zero in $\sigma \geq k$, then $F(s)$ has infinitely many simple zeros in $\sigma \geq k$.

The details of the proof of the theorem stated above are in [2].

J.B. Conrey and A. Ghosh
Department of Mathematics
Oklahoma State University
Stillwater, OK 74078

Current Address:
J.B. Conrey
School of Mathematics
Institute for Advanced Study
Princeton, NJ 08540

References

1. J.B. Conrey, A. Ghosh, and S.M. Gonek, Simple zeros of the zeta function of a quadratic number field, I, Invent. Math. 86(1986), 563-576..

2. J.B. Conrey and A. Ghosh, Simple zeros of the Ramanujan τ-Dirichlet series, preprint.

3. A. Good, The square mean of Dirichlet series associated with cusp forms, Mathematika 29 (1982), 278-295.

4. D.R. Heath-Brown, Simple zeros of the Riemann zeta function on the critical line, Bull. London Math. Soc. 11(1979), 17-18.

Received January 19, 1988

Linear Systems with Degenerate Quadratic Costs

V. Jurdjevic and I.A.K. Kupka

Presented by G.A. Elliott, F.R.S.C.

(0) Introduction. We assume that our basic setting consists of a given linear autonomous system $(\Sigma)\ \frac{dx}{dt} = Ax + Bu$ with state space X, control space U, both finite dimensional vector spaces, and a cost function $c : X \times U \to \mathbf{R}$, $c(x, u) = \frac{1}{2}\langle Pu, u\rangle + \langle Qx, u\rangle + \frac{1}{2}\langle Rx, x\rangle$. Here $P : Y \to U'$, $Q : X \to U'$, $R : X \to X'$ are linear mappings, U', X' the dual spaces of U and X respectively. P and R are assumed to be symmetric.

We shall study the following optimal control problem: given any two points x^0, x^1 in X and a positive number T find a trajectory $(\overline{x}, \overline{u}) : [0, T] \to X \times U$ of (Σ) such that $\overline{x}(0) = x^0$, $\overline{x}(T) = x^1$ and

$$(\mathrm{Opt})\qquad \int_0^T c(\overline{x}(t), \overline{u}(t))dt = \inf\left\{\int_0^T c(x(t), u(t))dt \;\middle|\; \begin{array}{l}(x, u) : [0, T] \to X \times U \text{ is a} \\ \text{trajectory of } (\Sigma) \text{ and } x(0) = x^0,\ x(T) = x^1\end{array}\right\}$$

We will use $Pb(x^0, x^1, T)$ to denote such a problem and we let $v(x^0, x^1, T)$ stand for the second member of the equality (Opt). In general $v(x^0, x^1, T)$ has its values in $[-\infty, \infty]$.

Our study is based on the following two natural assumptions:

(E) For any x^0, x^1 in X and any $T > 0$, $v(x^0, x^1, T) > -\infty$

(E) implies that $v(0, 0, T) \geq 0$. Hence the zero trajectory is optimal for $Pb(0, 0, T)$. Our second assumption is

(U) For any $T > 0$ the zero trajectory is the only trajectory optimal for $Pb(0, 0, T)$.

In contrast to the free end point problem which has been extensively studied in the control theory literature (for instance, [AC], [BJ], [HS], [K], [O'M]-J], [W], [Y] and more recently [KSW]), the fixed end points problem over a finite time interval has not received much attention (see [KO1], [KO2]).

Our methods are based on linear symplectic geometry, and the results bring into focus several related developments from the theory of singular perturbations [KT1], and the existence of self-adjoint solutions of the associated Ricatti equation. The results also extend very naturally to the infinite time interval ([Y]) and to the study of the algebraic Ricatti equation ([GLR]).

(I) Statement of the Results

Our first result concerns a standard form of the cost function as described by the following proposition.

Proposition 0. *Assume that the assumption (E) is satisfied and the system* (Σ) *is controllable. Then there exist two symmetric mappings* $H : X \to X'$, $W : X \to X'$ *and a feedback mapping* $K : X \to U$ *such that:*

(i) *P and W are positive semi-definite.*

(ii) *for any trajectory* $(x, u) : [a, b] \to X \times U$ of (Σ)

$$\int_a^b c(x(t), u(t))dt = \langle Hx(t), x(t)\rangle \Big|_{t=a}^{t=b} + \frac{1}{2}\int_a^b \Big[\langle Pv(t), v(t)\rangle + \langle Wx(t), x(t)\rangle\Big]dt$$

where $v = u - Kx$.

The problem $Pb(x^0, x^1, T)$ admits a regular synthesis if and only if the quadratic form $u \to c(u, 0)$ is positive definite, or stated equivalently, if the mapping P is positive definite. What we mean by regular synthesis is described by the following theorem:

Theorem 0. *Assume that the assumptions (E), (U) hold and that* (Σ) *is controllable. Then* $Pb(x^0, x^1, T)$ *has a unique optimal trajectory for each* x^0, x^1 *and* $T > 0$ *if and only if* $P \gg 0$. *The optimal trajectory is the projection on* X *of a trajectory* $x : [0, T] \to X \times X'$ *of the Hamiltonian field* $\vec{H}$ *of* H *defined by: by*

$$H(x, p) = -\frac{1}{2}\langle Rx, x\rangle + \langle Ax, p\rangle - \frac{1}{2}\langle B^*p - Qx, p^{-1}(B^*p - Qx)\rangle$$

for each $(x, p) \in X \times X'$. *Moreover,* z *is the unique trajectory of* $\vec{H}$ *which depends continuously on* x^0, x^1 *and* T *such that* $(z(0), z(T))$ *projects onto* (x^0, x^1).

In the case that P has a non zero kernel, there exists a natural extension of the regular synthesis which we term "generalized turnpike phenomenon". It is characterized by the existence of a certain subspace Ω of $X \times X'$ which carries the liftings of the optimal trajectories and the complementary notion of the "constant cost directions". The essential properties of Ω are given by our next proposition.

Proposition 1. *Under assumptions* (E) *and* (U)

(i) *there exist a symplectic vector subspace* Ω *of* $X \times X'$, *a quadratic form* $H : \Omega \to \mathbb{R}$ *and a linear mapping* $F : \Omega \to U$ *with the following property:*

for any $T > 0$ *the mapping* $z \to (\mathrm{proj}_x z, Fz)$ *induces a linear isomorphism between the space of the trajectories of the Hamiltonian field* $\vec{H}$ *of* H *defined on* $[0, T]$ *and the space of all trajectories* $(x, u) : [0, T] \to X \times U$ *of* (Σ) *such that* (x, u) *is optimal for* $Pb(x(0), x(T), T)$,

(ii) *the triple* (Ω, H, F) *is uniquely determined by the pair* (Σ, c) .

In general it can happen that Ω is reduced to zero in which case the only optimal trajectory is the zero trajectory and it can also happen that the projection of Ω onto X is a proper subspace of X.

To compute Ω, H and F we have invented an algorithm which leads to the result in at most m steps, m being the dimension of the control space U. This algorithm bears some resemblance to the methods leading to the Brunovski normal form for linear systems. The space of constant cost directions Y can be defined inductively as follows:

$$Y = \bigcup_{n=1}^{\infty} Y_n, \quad \text{where} \quad Y_0 = B(\ker P) \quad \text{and}$$

$$Y_n = A\big(B(\ker P) \cap Y_{n-1}\big) \quad \text{for} \quad n \geq 1 .$$

Our main result is the following:

Theorem 1. *Let* $\mathrm{Tr}(H)$ *denote the space of all trajectories of the Hamiltonian field* $\vec{H}$ *given by Proposition 1. There exists a unique continuous mapping* $\Gamma : X \times X \times \mathbb{R}^+ \to \mathrm{Tr}(H)$ *such that:*

(i) $\Gamma(x^0, x^1, T)$ *is defined on* $[0, T]$. *Its projection* $\gamma(x^0, x^1, T)$ *with the control* $F(\Gamma(x^0, x^1, T))$ *is the unique optimal trajectory initiating at* $\bar{x}^0 = \gamma(x^0, x^1, T)[0]$ *and terminating at* $\bar{x}^1 = \gamma(x^0, x^1, T)[T]$ *in time* T.

(ii) $x^k - \bar{x}^k \in Y$ *for* $k = 0$ *or* 1.

(iii) *The cost of* $(\gamma(x^0, x^1, T), F(\Gamma(x^0, x^1, T)))$ *is* $v(x^0, x^1, T)$.

(iv) *For any* $x \in X$ *and* $y \in Y$, *the function* $T \in \mathbb{R}_+^* \to v(x, x+y, T)$ *is bounded.*

To explain the significance of the constant cost directions it is instructive to consider the "regularized" problem and apply singular perturbation methods to it. To elaborate, let $P_1 : U \to U'$ be any symmetric positive semi-definite mapping such that its kernel is complementary to the kernel of P. Denote by $Pb(x^0, x^1, T, \varepsilon)$ the problem $Pb(x^0, x^1, T)$ where the cost c has been replaced by $c_\varepsilon : X \times U \to \mathbb{R}$, $c_\varepsilon(x, u) = c(x, u) + \frac{\varepsilon}{2} <P_1u, u>$. By Theorem 0, there is a unique continuous mapping $\lambda : X \times X \times \mathbb{R}_+^* \times \mathbb{R}_+^* \to C^\omega(X)$ (space of all analytic paths $x : [0, T_x] \to X$, T_x depending on x) such that for any x^0, x^1, T, ε, $\lambda(x^0, x^1, T, \varepsilon)$ is the unique optimal trajectory for $Pb(x^0, x^1, T, \varepsilon)$.

As explained in [KT1], [KT2], [KT3], (see also [O'M-J]) when ε goes to 0, the optimal trajectory $\lambda(x^0, x^1, T, \varepsilon)$ consists of an "outer" part (essentially, the "middle" part) and two boundary layers at the extremities 0 and T of $[0, T]$. The "outer" part tends, uniformly in time, to the trajectory $\gamma(x^0, x^1, T)$ of Theorem 1. The boundary layers give rise to the two instant jumps $x^0 \to \bar{x}^0$ and $\bar{x}^1 \to x^1$ along constant cost directions (called fast directions in [KT1], [KT2], [KT3]).

A precise statement is given in the next proposition where we will use the notations of Theorem 1.

Proposition 2. *For any* $\eta > 0$ *and any compact subset* K *in* $X \times X$, *the trajectory* $\lambda(x^0, x^1, T, \varepsilon)$ *of the* ε*-system, restricted to the interval* $[\eta, T-\eta]$, *converges uniformly for* (x^0, x^1) *in* K *to the restriction of the trajectory* $\gamma(x^0, x^1, T)$ *of the singular system to the same interval.*

(ii) *The trajectory* $\lambda(x^0, x^1, T, \varepsilon$ *has asymptotic expansions in* ε *near each of the boundary points* $0, T$ *of the interval* $[0, T]$, *of the form*

$$\sum_{j=1}^{l} \sum_{k=1}^{q(j)} a_{jk}(x^0, x^1, T, \varepsilon)\, e^{\alpha_{jk} t}$$

$a_{jk}(x^0, x^1, T, \varepsilon)$ *is an analytic function in* ε. $\alpha_{jk} = \alpha_{jk}(x^0, x^1, T, \varepsilon)$ *has an expansion of the form*

$$\alpha_{jk} = \frac{\alpha^0_{jk}}{\varepsilon^{1/j}} + \underline{\textit{high order terms}}$$

The jump $x^n - \bar{x}^n$ *is the sum* $\sum_{j=1}^{l} \sum_{k=1}^{q(j)} a_{jk}(x^0, x^1, T, 0)$ *and* $\sum_{k=1}^{q(j)} a_{jk}(x^0, x^1, T, 0)$ *belongs to* $Y_j - Y_{j-1}$.

The methods used in the preceding proposition can also be applied to the free end point problem, to obtain results similar to results obtained by different techniques in [HS] and [HSW].

Conclusion. The generalized optimal synthesis of this paper consists of the following: each generalized optimal trajectory is a concatenation of a "cheap" control trajectory with a regular optimal trajectory, followed by another "cheap" control trajectory. This synthesis is of the "turnpike type" where the cheap control trajectories may be viewed as access routes to the turnpike (given by the regular trajectory).

Such phenomena, even though observed using unbounded controls, may serve as a good model for the bounded case as well. The main difference between the bounded and unbounded case will be that the "cheap control" trajectories will be replaced by the bang-bang trajectories arising from the bounds or the space of controls. The detailed analysis will however be more difficult because of the chattering problems, such as the Fuller type phenomena caused by the matching of the singular extremals with the bang-bang extremals.

References

[AC] B.D.O. Anderson-D.J. Clements, "Singular optimal control: The linear-quadratic problem", Lecture notes in Control and Information Sciences, no. 5, Springer-Verlag 1978.

[BJ] D.J. Bell-D.H. Jacobson, "Singular optimal control problems", Academic Press 1975.

[GLR] I. Gohberg-P. Lancaster-L. Rodman, "On Hermitian solutions of the symmetric algebraic Ricatti equation", *SIAM J. on Contr. and Optim.* 24 (1986) 1323-1334.

[HS] M.L.J. Hautus-L.M. Silverman, "System structure and singular control", *Linear Algebra and Its Applications* 50 (1983) 369-402.

[KE] H. Kelly-T. Edelbaum, "Energy climbs, energy turns and asymptotic expansions", *J. Aircraft* 7 (1970) 93-95.

[KO1] J. Kogan, "Bifurcation of extremals in optimal control", Lecture Notes in Math. no. 1216, Springer-Verlag (1986).

[KO2] J. Kogan, "Structure of minimizers in linear quadratic Bolza problems of optimal control", Preprint, Purdue University 1987.

[KSW] A. Kitapcu-L.M. Silverman-J.C. Willems, "Singular optimal control: a geometric approach", *SIAM J. on Contr. and Optim.* 24 (1986) 369-402.

[KT1] P.V. Kokotovic, "Applications of singular perturbation techniques to control problems", SIAM Review vol. 26 (1984) 501-550.

[KT2] P.V. Kokotovic-H. Khalil-J. O'Reilly, "Singular perturbation methods in control", Academic Press (1986).

[KT3] P.V. Kokotovic, "Singular perturbations techniques in control theory", pp. 1-55 in "Singular perturbations and asymptotic analysis in control systems", P. Kokotovic, A. Bensonssan, G. Blankenship, editors, Lecture notes in Control and Information Sciences, no. 90, Springer-Verlag (1987).

[O'M-J] R.E. O'Malley Jr.-A. Jameson, "Singular perturbations and singular arcs ... part II", IEEE Trans. Aut. Control 22 (1977) 328-337.

[W] M. Wohnam, "Linear multivariable control - A geometric approach", Springer-Verlag (1983).

[Y] V.A. Yakubovich, "Optimization and invariance of linear stationary control systems", Automatika and Telemekhamka no. 8 (1984) 5-44.

V. Jurdjevic
Department of Mathematics
University of Toronto
Toronto, Ontario, Canada M5S 1A1

I.A.K. Kupka
Department of Mathematics
University of Toronto
Toronto, Ontario, Canada M5S 1A1

Received January 22, 1988

On the signature of a graph

Kunio Murasugi, F.R.S.C.

Abstract. It is proved that the signature of a weighted graph is invariant under 2-isomorphism.

Let Γ be a (finite) weighted graph, i.e. Γ is a graph in which $+1$ or -1 is assigned to each edge in Γ. Let $\sigma(\Gamma)$ denote the signature of Γ defined in [1].

In this paper, we will prove the following

Theorem 1. *If two weighted graphs* Γ_1 *and* Γ_2 *are 2-isomorphic, then* $\sigma(\Gamma_1) = \sigma(\Gamma_2)$.

Two graphs Γ_1 and Γ_2 are said to be *2-isomorphic* if one is obtained from the other by applying finitely many times the following two operations Ω_1 and Ω_2. Let Γ be a one-point union of two subgraphs G and H which meet at a vertex v. Then $\Omega_1(\Gamma)$ is another one-point union of G and H which meet at a different vertex v′. To define $\Omega_2(\Gamma)$, suppose that Γ is obtained from two disjoint graphs G and H by identifying vertices u_1 and u_2 of G with v_1 and v_2 of H, respectively. $\Omega_2(\Gamma)$ is a new graph obtained from G and H by modifying the identification so that $u_1 = v_2$ and $u_2 = v_1$.

Now since Proposition 7.4 (2) in [1] shows that $\sigma(\Gamma) = \sigma(\Omega_1(\Gamma))$, it suffices to prove

Proposition 2. *If* $\Gamma_2 = \Omega_2(\Gamma_1)$, *then* $\sigma(\Gamma_1) = \sigma(\Gamma_2)$.

Proof. Let $\{u_1, u_2, w_1, ..., w_n\}$ and $\{v_1, v_2, x_1, ..., x_m\}$ be the set of vertices of G and H. Then the *matrices* B_{Γ_i} of the graphs $\Gamma_i (i = 1, 2)$ are integer $(n + m + 2) \times (n + m + 2)$ matrices of the form [1]:

$$B_{\Gamma_i} = \begin{bmatrix} A_i & B_i & C_i \\ B_i^t & B_0 & 0 \\ C_i^t & 0 & C_0 \end{bmatrix} \quad (i = 1, 2)$$

where

(1) M^t denotes the transpose of M,

(2) B_1 and B_2 are identical $2 \times n$ matrices $\|b_{ij}\|_{1 \le i \le 2,\ 1 \le j \le n}$.

(3) C_i are $2 \times m$ matrices and C_2 is obtained from C_1 by interchanging the rows, i.e. $C_1 = \|c_{ij}\|_{1 \le i \le 2,\ 1 \le j \le m}$ and $C_2 = \begin{bmatrix} c_{21} & \cdots & c_{2m} \\ c_{11} & \cdots & c_{1m} \end{bmatrix}$.

(4) A_i are 2×2 matrices such that $A_1 = \|a_{ij}\|$ and

$$A_2 = A_1 + \begin{bmatrix} \lambda & 0 \\ 0 & -\lambda \end{bmatrix}, \quad \text{where } \lambda = \sum_{i=1}^{m} c_{1i} - \sum_{i=1}^{m} c_{2i}.$$

(5) B_0 is an $n \times n$ matrix obtained from the matrix of the graph G by deleting two rows and columns corresponding to vertices u_1 and u_2. Similarly, C_0 is an $m \times m$ matrix obtained from the matrix of H.

Note that A_i, B_0 and C_0 are all symmetric and the rank of B_{Γ_i} is at most $m + n + 1$.

Now there exist uni-modular matrices P_1 and Q_1 over the rational number field Q which diagonalize B_0 and C_0, respectively, i.e.

$$P_1 B_0 P_1^t = \begin{bmatrix} b_1 & & & & 0 \\ & \ddots & & & \\ & & b_k & & \\ & & & 0 & \\ 0 & & & & \ddots \; 0 \end{bmatrix} = \hat{B}_0 ,$$

where $b_i \neq 0$ for $i = 1, 2, \ldots, k(\leq n)$ and

$$Q_1 C_0 Q_1^t = \begin{bmatrix} c_1 & & & & 0 \\ & \ddots & & & \\ & & c_l & & \\ & & & 0 & \\ 0 & & & & \ddots \; 0 \end{bmatrix} = \hat{C}_0 ,$$

where $c_j \neq 0$ for $j = 1, 2, \ldots, l(\leq m)$. Let

$$R = \begin{bmatrix} I_2 & & 0 \\ & P_1 & \\ 0 & & Q_1 \end{bmatrix},$$

where I_r denotes the identity matrix of rank r. Then for $i = 1, 2,$

$$RB_{\Gamma_i}R^t = \begin{bmatrix} A_i & B'_i & C'_i \\ B'^t_i & \hat{B}_0 & 0 \\ C'^t_i & 0 & \hat{C}_0 \end{bmatrix} = \hat{B}_{\Gamma_i}$$

where $B'_1 = B'_2 = \|d_{ij}\|_{1\leq i\leq 2,\ 1\leq j\leq n}$ and $C'_1 = \|e_{ij}\|$ and $C'_2 = \begin{bmatrix} e_{21} & \cdots & e_{2m} \\ e_{11} & \cdots & e_{1m} \end{bmatrix}$.

For any square matrix M, $M(i)$ denotes the matrix obtained from M by striking out the i^{th} row and i^{th} column.

Case 1. $k = n$ and $l = m$.

Then $\det B_{\Gamma_1}(1) = \det B_{\Gamma_1}(1)$, since each value gives the number of weighted spanning trees of Γ_1 (and Γ_2). Therefore

$$\begin{aligned}\sigma(\Gamma_1) &= \sum_{i=1}^{n} \operatorname{sign}(b_i) + \sum_{j=1}^{m} \operatorname{sign}(c_j) + \operatorname{sign}\Big(\det B_{\Gamma_1} \prod_{i=1}^{n} b_i \prod_{j=1}^{m} c_j\Big) \\ &= \sum_{i=1}^{n} \operatorname{sign}(b_i) + \sum_{j=1}^{m} \operatorname{sign}(c_{ij}) + \operatorname{sign}\Big(\det B_{\Gamma_2} \prod_{i=1}^{n} b_i \prod_{j=1}^{m} c_j\Big) = \sigma(\Gamma_2)\,,\end{aligned}$$

where $\operatorname{sign}(a) = \dfrac{a}{|a|}$ if $a \neq 0$.

Case 2. $k \lneq n$ and $d_{it} \neq 0$ for some $i = 1$ or 2 and some t, $k < t \leq n$ (or $l \lneq m$ and $e_{is} \neq 0$ for some $i = 1$ or 2 and some s, $l < s \leq m$).

Then for $i = 1, 2$, $B_{\Gamma_i}(1)$ (or $B_{\Gamma_i}(2)$) is congruent to

$$\begin{bmatrix} 0 & & 0 & & & d_{it} & & 0 & \\ & b_1 & & & & \cdot & & & \\ 0 & & \ddots & 0 & & \cdot & & 0 & \\ & 0 & & b_k & & \cdot & & & \\ & & & & 0 & & & & \\ d_{it} & \cdot & \cdot & \cdot & & 0 & & & \\ & & & & & & c_1 & & \\ & & & & & & & \ddots\ c_l & \\ 0 & & 0 & & & & & 0 & \\ & & & & & & & & \ddots\ 0 \end{bmatrix}$$

and hence $\sigma(\Gamma_1) = \sigma(\Gamma_2)$. Note that $\operatorname{rank} B_{\Gamma_i}(1) = k + l + 2$.

Case 3. $0 \leq k \lneq n$ and $0 \leq l \lneq m$, and $d_{1t} = d_{2t} = 0$, for $t = k+1, \ldots, n$ and $e_{1s} = e_{2s} = 0$ for $s = l + 1, \ldots m$.

Then we can eliminate all entries of B'_1, C'_1 and $B_1'^{t}\, C_1'^{t}$ by applying elementary row and column operations. To be more precise, there exists a uni-modular matrix S over Q such that

$$S\hat{B}_{\Gamma_i} S^t = \begin{bmatrix} A'_i & & 0 \\ & \hat{B}_0 & \\ 0 & & \hat{C}_0 \end{bmatrix} = \tilde{B}_{\Gamma_i}, \quad i = 1, 2 .$$

To determine A'_i, denote, for $p \le q$, $\alpha_{pq} = \sum_{j=1}^{k} \frac{d_{pj} d_{qj}}{b_j}$ and $\beta_{pq} = \sum_{j=1}^{l} \frac{e_{pj} e_{qj}}{c_j}$.

Then we see that $A'_1 = A_1 - \begin{bmatrix} \alpha_{11} + \beta_{11} & \alpha_{12} + \beta_{12} \\ \alpha_{12} + \beta_{12} & \alpha_{22} + \beta_{22} \end{bmatrix}$ and $A'_2 = A_2 - \begin{bmatrix} \alpha_{11} + \beta_{22} & \alpha_{12} + \beta_{12} \\ \alpha_{12} + \beta_{12} & \alpha_{22} + \beta_{11} \end{bmatrix}$. Since $\sigma(\Gamma_i) = \sigma(B_{\Gamma_i}(1)) = \sigma(B_{\Gamma_i}(2))$, $i = 1, 2$, either the diagonal entries of A'_i are 0 or the sign of these entries must be identical, i.e.

(6) $\quad \text{sign}(a_{11} - \alpha_{11} - \beta_{11}) = \text{sign}(a_{22} - \alpha_{22} - \beta_{22})$ and

$\text{sign}(a_{11} + \lambda - \alpha_{11} - \beta_{22}) = \text{sign}(a_{22} - \lambda - \alpha_{22} - \beta_{11})$.

Note that $\tilde{B}_{\Gamma_i}(1)$ and $\tilde{B}_{\Gamma_i}(2)$ are diagonal. From (6), we see easily that

$$\begin{aligned} \text{sign}\,(a_{11} + \lambda - \alpha_{11} - \beta_{22}) &= \text{sign}\,(a_{11} + \lambda - \alpha_{11} - \beta_{22} + a_{22} - \lambda - \alpha_{22} - \beta_{11}) \\ &= \text{sign}\,(a_{11} - \alpha_{11} - \beta_{11} + a_{22} - \alpha_{22} - \beta_{22}) = \text{sign}\,(a_{11} - \alpha_{11} - \beta_{11}) \end{aligned}$$

and hence $\sigma(\Gamma_1) = \sigma(\Gamma_2)$.

It completes the proof of Proposition 2 and of Theorem 1.

References

[1] K. Murasugi, On invariants of graphs with applications to Knot theory, (to appear).

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

Received January 25, 1988

A LAW OF THE ITERATED LOGARITHM FOR INFINITE DIMENSIONAL ORNSTEIN-UHLENBECK PROCESSES

Miklós Csörgő and Zhengyan Lin

Presented by D.A.Dawson, F.R.S.C.

Abstract: We prove a large deviation theorem and a law of iterated logarithm for infinite dimensional Ornstein-Uhlenbeck processes.

A real valued stationary Gaussian process $\{X(t), -\infty < t < \infty\}$ will be called an Ornstein-Uhlenbeck process with coefficients γ and λ $(\gamma, \lambda > 0)$ if $EX(T) = 0$ and $EX(s)X(t) = (\gamma/\lambda)\exp(-\lambda|t-s|)$. Let $Y(t) = (X_1(t), \ldots, X_i(t), \ldots)$, where $\{X_i(t), -\infty < t < \infty\}$ are independent Ornstein-Uhlenbeck processes with coefficients γ_i and λ_i $(i = 1, 2, \ldots)$. The process $Y(\cdot)$ was first studied by Dawson (1972) as the stationary solution of the infinite array of stochastic differential equations

$$dX_i(t) = -\lambda_i X_i(t)dt + (2\gamma_i)^{1/2}dW_i(t) \quad (i = 1, 2, \ldots), \tag{1}$$

where $\{W_i(t), -\infty < t < \infty\}$ are independent Wiener processes (cf. also Dawson (1975), Walsh (1981) and Antoniadis and Carmona (1987)). If we assume $\sum_{i=1}^{\infty} \gamma_i/\lambda_i < \infty$, then $Y(t)$ is almost surely (a.s.) an ℓ^2-valued Ornstein-Uhlenbeck process $(E\|Y(t)\|_{\ell^2}^2 = \sum_{i=1}^{\infty} \gamma_i/\lambda_i)$, and Dawson (1972) shows that under this condition $Y(\cdot)$ is weakly continuous. If for large i we have also $di^{1+\delta} \geq \lambda_i \geq ci^{1+\delta}$ for some $c > 0, d > 0$ and $\delta > 0$, then Dawson (1972) shows that $Y(\cdot)$ in ℓ^2 is a.s. continuous. Iscoe and McDonald (1986, 1987) establish the a.s. continuity of $Y(\cdot)$ in ℓ^2 under the weaker additional condition $\sum_{i=1}^{\infty} \gamma_i^2/\lambda_i < \infty$, by studying and solving the equivalent problem of a.s. continuity of the process $\sum_{i=1}^{\infty} X_i^2(t)$ via proving powerful large deviation theorems for the latter stochastic process. Iscoe, Marcus, McDonald and Zinn (1987) deal with the strong continuity of $Y(\cdot)$ in ℓ^2 by using Fernique-type techniques concerning a.s. continuity of stationary Gaussian processes. Schmuland (1986, 1987) uses Dirichlet forms to study a class of infinite dimensional processes which are modelled on the process $Y(\cdot)$. His general results can be also used to recover state space and continuity results of the so far mentioned papers. Csörgő and Lin (1987) study $Y(\cdot)$ in terms of the path behaviour of the two-time parameter stochastic process $\{X(t,n),\ -\infty < t < \infty, n = 1,2,\ldots\}$, where $X(t,n) = \sum_{k=1}^{n} X_k(t)$, $X(t,0) = 0$ for all $t \in \mathrm{R}$ and establish P. Lévy type moduli of continuity and large increments rates results for the latter process along the lines of Sections 1.12-1.15 and the Supplementary remarks of Chapter 1 in Csörgő and Révész (1981), where almost sure behaviour of some path increments of the Wiener sheet and the Kiefer process is established. These hinted at increments results do not imply any law of the iterated logarithm for $X(t,n)$. However, Schmuland (1987), using Dirichlet form– techniques, proved that if the X_i of (1) are of variance $\gamma_i/\lambda_i = 1$ and $\sum_{i=1}^{n} \gamma_i/(2n \log\log n) \to 0$ $(n \to \infty)$ then

(2) $$P\left\{\limsup_{n\to\infty} X(t,n)/(2n\log\log n)^{1/2} = 1 \quad \text{for all} \quad t \in \mathrm{R}\right\} = 1.$$

The aim of this exposition is to prove a large deviation result for $X(t,n)$ which can be used to prove also laws of iterated logarithm for the latter Gaussian process whose covariance function is

(3) $$EX(s,m)X(t,n) = \sum_{k=1}^{m\wedge n} (\gamma_k/\lambda_k)\exp(-\lambda_k|t-s|), \quad m \wedge n = 1,2,\ldots.$$

First we state our version of a law of the iterated logarithm. We will use the notation $\lambda_N' = \max_{1\le j\le N} \lambda_j$.

THEOREM. *Assume that*

(4) $$\log \lambda_N' / \log\log N \to 0 \qquad (N \to \infty)$$

and that the non-decreasing sequence $\{T_N\}$ *satisfies*

(5) $$\log T_N / \log\log N \to 0 \qquad (N \to \infty).$$

Suppose also that for any $\epsilon > 0$ *there exist* $1 < \theta_1 < \theta_2$ *such that*

(6) $$\limsup_{k\to\infty}\left(\sum_{j=1}^{\theta_1^{k+1}}\gamma_j/\lambda_j\right)\Big/\left(\sum_{j=1}^{\theta_1^k}\gamma_j/\lambda_j\right)\le 1+\epsilon$$

and

(7) $$\limsup_{k\to\infty}\left(\sum_{j=1}^{\theta_2^{k}}\gamma_j/\lambda_j\right)\Big/\left(\sum_{j=1}^{\theta_2^{k+1}}\gamma_j/\lambda_j\right)\le \epsilon.$$

Then, with $\beta_N = \left(2\sum_{j=1}^N(\gamma_j/\lambda_j)\log\log N\right)^{1/2}$, *we have*

$$\limsup_{N\to\infty}|X(T_N,N)|/\beta_N = \limsup_{N\to\infty}\max_{1\le n\le N}\sup_{|t|\le T_N}|X(t,n)|/\beta_N = 1 \quad \text{a.s.}$$

We note that if $\gamma_i/\lambda_i = 1$ as in (2), then conditions (6) and (7) disappear, and our $\beta_N = (2N\log\log N)^{1/2}$ is like the normalizing sequence of (2).

The proof of Theorem is based on a large deviation result, which we now state.

LEMMA. *For any small enough* $\epsilon > 0$ *there exists* $C = C(\epsilon)$ *such that we have*

(8) $$P\left\{\max_{1\le n\le N}\sup_{|t|\le T}|X(t,n)|\Big/\left(\sum_{j=1}^N\gamma_j/\lambda_j\right)^{1/2}\ge v\right\}\le C\lambda_N'^2 T\frac{1}{v}e^{-\frac{v^2}{2+\epsilon}}$$

for any $v \ge 2(\log(\lambda_N'\epsilon^{-6}))^{1/2}$.

PROOF OF LEMMA. For each fixed t, s and N we have $X(t,N) \stackrel{\mathcal{D}}{=} \mathcal{N}(0,\Gamma^2)$ as well as $X(t+s,N) - X(t,N) \stackrel{\mathcal{D}}{=} \mathcal{N}(0,\Lambda^2(s))$, where $\Gamma^2 = \sum_{j=1}^N\gamma_j/\lambda_j$ and $\Lambda^2(s) = 2\sum_{j=1}^N(\gamma_j/\lambda_j)\times(1-\exp(-\lambda_j s))$. Let $p = [\lambda_N'\epsilon^{-6}]$. Then $p \le \exp(v^2/4)$. For integer k we put $p_k = \exp(2^k\log p)$, $x_k = 2^{k/2}$, $u_k = vx_k$ and define $X_k(t,n) = X(i/p_k,n)$, $i/p_k \le t < (i+1)/p_k$. Since $X(t,n)$ is a sum with independent increments in n, we have

$$\begin{aligned}P\left\{\max_{1\le n\le N}\sup_{0\le t\le 1}|X_1(t,n)|\ge u_0\Gamma\right\} &= P\left\{\max_{1\le n\le N}\max_{1\le i\le p_1}|X(i/p_1,n)|\ge u_0\Gamma\right\}\\ &\le p_1 P\left\{\max_{1\le n\le N}|X(0,n)|\ge u_0\Gamma\right\}\\ &\le cp_1e^{-u_0^2/2}/u_0,\end{aligned}$$

where $c > 0$ is an absolute constant. Similarly,

$$P\left\{\max_{1\le n\le N}\sup_{0\le t\le 1}|X_k(t,n)-X_{k+1}(t,n)|\ge u_k\Lambda\left(\frac{1}{2p_k}\right)\right\}\le cp_{k+1}e^{-u_k^2/2}/u_k.$$

Consequently, we have

$$(9)\quad P\left\{\max_{1\le n\le N}\sup_{0\le t\le 1}\left\{|X_1(t,n)|+\sum_{k=1}^{\infty}|X_k(t,n)-X_{k+1}(t,n)|\right\}\ge u_0\Gamma+\sum_{k=1}^{\infty}u_k\Lambda\left(\frac{1}{2p_k}\right)\right\}$$
$$\le c\sum_{k=0}^{\infty}p_{k+1}e^{-u_k^2/2}/u_k.$$

Also, we have

$$\begin{aligned}\sum_{k=1}^{\infty}u_k\Lambda\left(\frac{1}{2p_k}\right)&\le v\sum_{k=1}^{\infty}\left(2+\sqrt{2}\right)(x_k-x_{k-1})\Lambda\left(p^{-x_k^2}/2\right)\\&\le 4v\int_1^{\infty}\Lambda\left(p^{-y^2}/2\right)dy\\&\le 6v\int_1^{\infty}\left(\sum_{j=1}^{N}(\gamma_j/\lambda_j)\left(1-\exp\left(-\lambda_j p^{-y^2}/2\right)\right)\right)^{1/2}dy\\&\le 4v\left(\sum_{j=1}^{N}\gamma_j/\lambda_j\right)^{1/2}\int_1^{\infty}\epsilon^{3y^2}dy\\&\le v\epsilon^2\left(\sum_{j=1}^{N}\gamma_j/\lambda_j\right)^{1/2},\end{aligned}$$

and, on recalling that $p\le\exp(v^2/4)$, as well as

$$\begin{aligned}\sum_{k=0}^{\infty}p_{k+1}e^{-u_k^2/2}/u_k&=\sum_{k=0}^{\infty}2^{-k/2}p^{2^{k+1}}e^{-v^2 2^k/2}/v\\&\le\left(p^2e^{-v^2/2}/v\right)\sum_{k=0}^{\infty}e^{-k(\log 2)/2+v^2(2^{k+1}-2)/4-v^2(2^{k+1}-1/2)}\\&\le\left(p^2e^{-v^2/2}/v\right)\sum_{k=0}^{\infty}e^{-(k\log 2)/2}\\&\le cp^2e^{-v^2/2}/v.\end{aligned}$$

Inserting now the latter two estimates into (9), we obtain

$$\begin{aligned}&P\left\{\max_{1\le n\le N}\sup_{|t|\le T}|X(t,n)|\ge v\left(1+\epsilon^2\right)\left(\sum_{j=1}^{N}\gamma_j/\lambda_j\right)^{1/2}\right\}\\&\le 2(T+1)P\left\{\max_{1\le n\le N}\sup_{0\le t\le 1}\left\{|X_1(t,n)|+\sum_{k=1}^{\infty}|X_k(t,n)-X_{k+1}(t,n)|\right\}\ge u_0\Gamma+\sum_{k=1}^{\infty}u_k\Lambda\left(\frac{1}{2p_k}\right)\right\}\\&\le C\lambda'^2_N Te^{-v^2/2}/v.\end{aligned}$$

If we now replace $v(1+\epsilon^2)$ by v, then (8) follows at once if $\epsilon > 0$ is small enough.

PROOF OF THEOREM. Using Lemma and conditions (4) and (5), we obtain

$$P\left\{\max_{1\le n\le N}\sup_{|t|\le T_N}|X(t,n)|\ge(1+\epsilon)\left(2\sum_{j=1}^{N}(\gamma_j/\lambda_j)\log\log N\right)^{1/2}\right\}$$
$$\le C\lambda'^2_N T_N\exp\left\{-\frac{2(1+\epsilon)^2}{2+\epsilon}\log\log N\right\}\le\frac{C\lambda'^2_N T_N}{(\log N)^{1+\epsilon}}\le\frac{C}{(\log N)^{1+\epsilon/2}}$$

for all large N. Hence for any $\theta > 1$ we have

(10) $$\limsup_{k\to\infty}\max_{1\le n\le\theta^k}\sup_{|t|\le T_{\theta^k}}|X(t,n)|/\left(2\sum_{j=1}^{\theta^k}(\gamma_j/\lambda_j)\log\log\theta^k\right)^{1/2}\le 1+\epsilon\quad\text{a.s.}.$$

and combining the latter with condition (6) results in

(11) $$\limsup_{N\to\infty}\max_{1\le n\le N}\sup_{|t|\le T_N}|X(t,n)|/\left(2\sum_{j=1}^{N}(\gamma_j\lambda_j)\log\log N\right)^{1/2}\le 1+\epsilon\quad\text{a.s.}.$$

Next we prove

(12) $$\limsup_{N\to\infty}|X(T_N,N)|/\left(2\sum_{j=1}^{N}(\gamma_j/\lambda_j)\log\log N\right)^{1/2}\ge 1-\epsilon\quad\text{a.s.}.$$

Let $n_k=\theta^k$, $\theta>1$. It is easily seen that $X(T_{n_{k+1}},n_{k+1})-X(T_{n_{k+1}},n_k)$, $k=1,2,\ldots$, are independent normal random variables with mean 0 and variance $E(X(T_{n_{k+1}},n_{k+1})-X(T_{n_{k+1}},n_k))^2=\sum_{j=n_k+1}^{n_{k+1}}\gamma_j/\lambda_j$. By condition (7) we can choose θ large enough so that

$$\left(\sum_{j=n_k+1}^{n_{k+1}}\gamma_j/\lambda_j\right)/\left(\sum_{j=1}^{n_{k+1}}\gamma_j/\lambda_j\right)\ge 1-\epsilon$$

for all large k. Hence we have

$$P\left\{|X(T_{n_{k+1}},n_{k+1})-X(T_{n_{k+1}},n_k)|\ge(1-2\epsilon)\left(2\sum_{j=1}^{n_{k+1}}(\gamma_j/\lambda_j)\log\log n_{k+1}\right)\right\}$$
$$\ge C\exp\{-(1-\epsilon)\log\log n_{k+1}\}=\mathcal{O}\left(k^{-(1-\epsilon)}\right).$$

The latter in turn implies

(13) $$\limsup_{k\to\infty}|X(T_{n_{k+1}},n_{k+1})-X(T_{n_{k+1}},n_k)|/\left(2\sum_{j=1}^{n_{k+1}}(\gamma_j/\lambda_j)\log\log n_{k+1}\right)^{1/2}\ge 1-2\epsilon\quad\text{a.s.}$$

It follows from the proof of (10) that we can replace T_{θ^k} in it by $T_{\theta^{k+1}}$, since condition (5) implies that we have $T_{\theta^{k+1}}/(\log\theta^k)^\epsilon \to 0$ ($k\to\infty$) for any $\epsilon > 0$ and $\theta > 1$. Hence, noting condition (7),

$$\limsup_{k\to\infty} |X(T_{n_{k+1}}, n_k)| \Big/ \left(2\sum_{j=1}^{n_{k+1}} (\gamma_j/\lambda_j)\log\log n_{k+1}\right)^{1/2} = 0 \quad \text{a.s.} \tag{14}$$

Now (12) follows from combining (14) with (13), and (12) and (11) together imply the conclusion of Theorem.

ACKNOWLEDGEMENTS. This research of M.Csörgö was supported by an NSERC Canada Grant, and that of Z.Y. Lin by an NSERC Canada Scientific Exchange Award, both held at Carleton University, Ottawa.

The authors wish to thank Don Dawson for valuable advice and discussions.

REFERENCES

[1] ANTONIADIS, A. and CARMONA, R. (1987). Eigenfunction expansions for infinite dimensional Ornstein-Uhlenbeck processes. *Probab. Theory Related Fields 74* 31-54.

[2] CSÖRGŐ , M. and LIN, Z.Y. (1987). Path properties of infinite dimensional Ornstein-Uhlenbeck processes. Manuscript.

[3] CSÖRGŐ, M. and RÉVÉSZ, P. (1981). *Strong Approximations in Probability and Statistics.* Academic, New York.

[4] DAWSON, D.A. (1972). Stochastic evolution equations. *Math. Biosciences 15* 287-316.

[5] DAWSON, D.A. (1975). Stochastic evolution equations and related measure processes. *J. Multivariate Anal. 5* 1-52.

[6] ISCOE, I., MARCUS, M., McDONALD, D. and ZINN, J. (1987). Continuity of ℓ^2-valued Orstein-Uhlenbeck processes. Manuscript.

[7] ISCOE, I. and McDONALD, D. (1986). Continuity of ℓ^2-valued Ornstein-Uhlenbeck processes. *Tech. Rep. Ser. Lab. Res. Stat. Probab. No. 68*, Carleton University - University of Ottawa, Ottawa.

[8] ISCOE, I. and McDONALD, D,(1987). Large deviations for ℓ^2-valued Ornstein-Uhlenbeck processes. *Ann. Probab.* To appear.

[9] SCHMULAND, B. (1986). Dirichlet forms and infinite dimensional stochastic processes. *Tech. Rep. Ser. Lab. Res. Stat. Probab. No. 95*, Carleton University - University of Ottawa, Ottawa.

[10] SCHMULAND, B. (1987). *Dirichlet Forms and Infinite Dimensional Ornstein-Uhlenbeck Processes.* Ph.D. Dissertation, Carleton University, Ottawa.

[11] WALSH, J.B. (1981). A stochastic model of neural response. *Adv. Appl. Probab. 13* 231-281.

DEPARTMENT OF MATHEMATICS
AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, CANADA K1S 5B6

DEPARTMENT OF MATHEMATICS
HANGZHOU UNIVERSITY
HANGZHOU, ZHEJIANG
PEOPLE'S REPUBLIC OF CHINA

Received January 27, 1988

REGULARITY OF l^2-VALUED ORNSTEIN-UHLENBECK PROCESSES

B. Schmuland

Presented by D.A. Dawson, F.R.S.C.

ABSTRACT

We consider a stationary, infinite dimensional Ornstein-Uhlenbeck process with independent coordinates which, at fixed times, are almost surely square summable. Using the theory of Dirichlet forms we find conditions for l^2 sample path continuity. As well, we consider the behaviour along sample paths of the sequence of coordinates.

1. INTRODUCTION

We are interested in the sample path regularity of the stationary vector valued process

$$X(\cdot) = (X_1(\cdot), X_2(\cdot), \ldots, X_i(\cdot), \ldots) \tag{1.1}$$

whose coordinates satisfy

$$dX_i(t) = -\alpha_i X_i(t)dt + \sigma_i dW_i(t), \quad i \geq 1, \tag{1.2}$$

where $\alpha_i > 0$, $\sigma_i > 0$ and $\{W_i(\cdot);\ i \geq 1\}$ are independent Wiener processes. The solution $X_i(\cdot)$ of (1.2) is the Ornstein-Uhlenbeck process with drift coefficient α_i and diffusion coefficient σ_i, which has an invariant measure

$m_i = N(0, \sigma_i^2/2\alpha_i)$. We can also identify $X_i(\cdot)$ as the Hunt process associated with the Dirichlet form E_i on $L^2 = L^2(R; m_i)$, given by the formula

$$(1.3)\qquad \begin{aligned} E_i(f,g) &= 1/2 \int \sigma_i^2 f'(x)\, g'(x)\, m_i(dx) \\ D(E_i) &= \{f \in L^2 : f \text{ is absolutely continuous and } f' \in L^2\}. \end{aligned}$$

See [2] for the general theory of Dirichlet forms and [1] for the connection with stochastic differential equations. The form associated with the process (1.1) is given by the closure in $L^2(X;m)$ of

$$(1.4)\qquad \begin{aligned} E(f,g) &= 1/2 \int \sum_i \sigma_i^2 (\partial/\partial x_i f)(x)(\partial/\partial x_i g)(x)\, m(dx) \\ D(E) &= \bigcup_{k\geq 1} C_o^\infty(R^k). \end{aligned}$$

Here $\bigcup_{k\geq 1} C_o^\infty(R^k)$ refers to cylinder functions which are smooth and have compact support in a finite number of variables, $X = \prod_{i=1}^\infty R_i$ and $m = \prod_{i=1}^\infty m_i$.

2. REGULARITY RESULTS

Let us suppose that $\sum_{i=1}^\infty \sigma_i^2/2\alpha_i < \infty$ so that $m(l^2) = 1$, where l^2 is the subset of points $x = (x_1, x_2, \ldots, x_i, \ldots)$ in X with square summable coordinates. For the stationary process, $X(t)$ has distribution m for all $t \geq 0$ and so

$$(1.5) \qquad P\left(\sum_{i=1}^{\infty} X_i^2(t) < \infty\right) = m(l^2) = 1, \ \forall t \geq 0.$$

In order to pass from a fixed time result such as (1.5) to l^2 sample path continuity we require some control on the fluctuations of $X(\cdot)$ around the steady state m. Such information can be provided by the Dirichlet form in (1.4). Intuitively, (1.4) and (1.2) tell us that a process with larger diffusion coefficients σ_i will exhibit more irregular behaviour. So it is not surprising that our condition is on the size of σ_i^2.

THEOREM 1: *If* $\sum_i \sigma_i^2/2\alpha_i < \infty$ *and* $\sum_i \sigma_i^2(\sigma_i^2/2\alpha_i) < \infty$, *then*

$$P(t \to X(t) \text{ is } l^2\text{-continuous } \forall t \geq 0) = 1.$$

The strategy used to get this result is as follows. Define the function $\|\cdot\|^2 : X \to \overline{R}(= R \cup \{\infty\})$ by $\|\cdot\|^2 = \sum_i x_i^2 \leq \infty$. If $E(\|\cdot\|^2, \|\cdot\|^2)$ is finite then one uses Theorem 4.3.2. of [2] to conclude that

$$P(t \to \|X(t)\|^2 \text{ is } \overline{R}\text{-continuous}) = 1.$$

One can the show that the value ∞ is not attained along sample paths, and by simple Hilbert space theory and the fact that the coordinate processes are continuous we arrive at the conclusion of the theorem. To determine when $E(\|\cdot\|^2, \|\cdot\|^2)$ is finite, observe that the i^{th} partial of $\|\cdot\|^2$ is $2x_i$ and so $E(\|\cdot\|^2, \|\cdot\|^2)$ is equal to

$$1/2 \int 4 \sum_i \sigma_i^2 x_i^2 \, m(dx) = 2 \sum_i \sigma_i^2(\sigma_i^2/2\alpha_i).$$

This is the source of the second summation condition in the theorem.

Finally we turn to a different regularity property of $X(\cdot)$, that of convergence to zero of the coordinates. Note that by Borel-Cantelli and the asymptotic result $\int_x^\infty \exp(-y^2/2)dy \sim 1/x \exp(-x^2/2)$ as $x\to\infty$, we find

$m(x_i\to 0) = 1$ if and only if

$$(1.6) \qquad \sum_{i=1}^{\infty} \exp(-x^2 \alpha_i/\sigma_i^2)<\infty, \ \forall x>0.$$

Here we drop the assumption that $\sum_i \sigma_i^2/2\alpha_i<\infty$, and assume only that (1.6) holds, so that

$$P(X_i(t)\to 0 \text{ as } i\to\infty) = m(x_i\to 0) = 1, \ \forall t\geq 0.$$

Using the relationship which exists between the capacity (Cap_i) associated with E_i (1.3), and the hitting times of $X_i(\cdot)$ we can establish the second theorem. Define the number x_o by

$$x_o = \inf\{x>0:\sigma_i^2 \exp(-x^2 \alpha_i/\sigma_i^2)\to 0 \text{ as } i\to\infty\}$$

which turns out to be the same as letting

$$x_o = \inf\{x>0 : Cap_i(\{x\})\to 0 \text{ as } i\to\infty\}.$$

A little algebra will convince you that, since $\sigma_i^2/\alpha_i \to 0$,

$$x_0 = \overline{\lim_i} \log^+(\sigma_i^2)\ \sigma_i^2/\alpha_i,$$

where $\log^+(x) = \log(x \vee 1)$.

<u>Theorem 2</u>: <u>Under (1.6) we have the following</u>

(i) $P\left(\sup_{0\le t\le T} X_i(t) \ge x_0 + \varepsilon \text{ i.o.}\right) = 0$

<u>and</u>

$P\left(\inf_{0\le t\le T} X_i(t) \le -(x_0 + \varepsilon) \text{ i.o.}\right) = 0$

<u>for all $T>0$ and $\varepsilon>0$.</u>

(ii) $P(\exists\, t \in [0,T]: \{X_i(t)\}_{i=1}^{\infty}$ <u>clusters at each point in</u> $[-x_0,x_0]) = 1$ <u>for all $T>0$.</u>

<u>Comment</u>: We find that if (1.6) holds, then

$$P(X_i(t)\to 0 \text{ as } i\to\infty\ \forall t) = 1$$

if and only if $\log^+(\sigma_i^2)\ \sigma_i^2/2\alpha_i \to 0$. By way of comparison, it is known [3] that if $(\log \sigma_i^2)^r\ \sigma_i^2/2\alpha_i$ is bounded for some $r>1$, and if $\sum_i \sigma_i^2/2\alpha_i < \infty$, then $X(\cdot)$ is l^2-continuous. This is stronger than our Theorem 1.

ACKNOWLEDGEMENT

This work is done while the author was a Ph.D. student working under Professor D.A. Dawson. The author wishes to thank Professor Dawson for his valuable suggestions and encouragement. We also thank I. Iscoe and D. McDonald for sharing their expertise and for posing the problem considered in Theorem 2.

REFERENCES

1. S. Albeverio, R. Hoegh-Krohn and L. Streit. Energy forms, Hamiltonians, and distorted Brownian paths. J. Math. Phys. Vol. 18, No. 5 (1977), 907-917.

2. M. Fukushima. Dirichlet forms and Markov Processes. North-Holland/ Kodansha, 1980.

3. I. Iscoe, M. Marcus, D. McDonald and J. Zinn. Continuity of l^2-valued Ornstein-Uhlenbeck processes. To appear.

Department of Statistics & Applied Probability
University of Alberta
Edmonton, Alberta
Canada
T6G 2G1

Received January 27, 1988

NOTES ON CERTAIN SUBCLASS OF CLOSE-TO-CONVEX FUNCTIONS

SHIGEYOSHI OWA, SEIICHI FUKUI AND OSMAN ALTINTAS

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

ABSTRACT.

The object of the present paper is to derive some properties of certain subclass of close-to-convex functions in the unit disk.

I. INTRODUCTION.

Let $\mathcal{A}$ be the class of functions of the form

$$f(z) = z + \sum_{n=2}^{\infty} a_n z^n \tag{1.1}$$

which are analytic in the unit disk $\mathcal{U} = \{z: |z| < 1\}$.

A function $f(z)$ in $\mathcal{A}$ is said to be a member of the class $\mathcal{R}(\alpha)$ if and only if it satisfies

$$\mathrm{Re}\{f'(z)\} > \alpha \tag{1.2}$$

for some α $(0 \leq \alpha < 1)$ and for all $z \in \mathcal{U}$. It is well-known that $\mathcal{R}(\alpha)$ is the subclass of close-to-convex functions in the unit disk $\mathcal{U}$. Further, recently, Fukui, Owa, Ogawa and Nunokawa [1] have given a starlike boundary of functions belonging to the class $\mathcal{R}(\alpha)$.

2. PROPERTIES OF THE CLASS $P(\alpha)$.

We begin with the statement of the following lemma due to Miller [2] (or Miller and Mocanu [3]).

LEMMA 1. *Let* $\phi(u,v)$ *be a complex function,*

$$\phi: \mathbb{D} \longrightarrow \mathbb{C}, \quad \mathbb{D} \subset \mathbb{C}\times\mathbb{C} \quad (\mathbb{C} \text{ is the complex plane})$$

and let $u = u_1 + iu_2$, $v = v_1 + iv_2$. *Suppose that* $\phi(u,v)$ *satisfies the conditions:*

(i) $\phi(u,v)$ *is continuous in* $\mathbb{D}$,

(ii) $(1,0) \in \mathbb{D}$ *and* $\mathrm{Re}\{\phi(1,0)\} > 0$,

(iii) $\mathrm{Re}\{\phi(iu_2,v_1)\} \leq 0$ *for all* $(iu_2,v_1) \in \mathbb{D}$ *and such that* $v_1 \leq -(1+u_2^2)/2$.

Let $p(z) = 1 + p_1 z + p_2 z^2 + \cdots$ *be regular in* $\mathbb{U}$, *such that* $(p(z),zp'(z)) \in \mathbb{D}$ *for all* $z \in \mathbb{U}$. *If* $\mathrm{Re}\{\phi(p(z),zp'(z))\} > 0$ $(z \in \mathbb{U})$, *then* $\mathrm{Re}\{p(z)\} > 0$ $(z \in \mathbb{U})$.

Now, we derive

THEOREM 1. *If the function* $f(z)$ *defined by (1.1) is in the class* $\mathcal{R}(\alpha)$, *then*

$$\mathrm{Re}\sqrt{\frac{f(z)}{z}} > \frac{1+\sqrt{1+8\alpha}}{4} \quad (z \in \mathbb{U}). \tag{2.1}$$

PROOF. For $f(z) \in \mathcal{R}(\alpha)$, we define the function $p(z)$ by

(2.2) $$\sqrt{\frac{f(z)}{z}} = \beta + (1 - \beta)p(z),$$

where

(2.3) $$\beta = \frac{1 + \sqrt{1 + 8\alpha}}{4}.$$

Then $p(z) = 1 + p_1 z + p_2 z^2 + \cdots$ is regular in $\mathbb{U}$. Taking the differentiations of both sides in (2.2), we see that

(2.4) $$f'(z) = (\beta + (1 - \beta)p(z))^2 + 2(1 - \beta)(\beta + (1 - \beta)p(z))zp'(z)$$

or

(2.5) $$\begin{aligned} &\text{Re}\{f'(z) - \alpha\} \\ &= \text{Re}\{(\beta + (1 - \beta)p(z))^2 + 2(1 - \beta)(\beta + (1 - \beta)p(z))zp'(z) - \alpha\} \\ &> 0. \end{aligned}$$

Letting $p(z) = u = u_1 + iu_2$ and $zp'(z) = v = v_1 + iv_2$, we define the function $\phi(u,v)$ by

(2.6) $$\phi(u,v) = (\beta + (1 - \beta)u)^2 + 2(1 - \beta)(\beta + (1 - \beta)u)v - \alpha.$$

Then, $\phi(u,v)$ satisfies

(i) $\phi(u,v)$ is continuous in $\mathbb{D} = \mathbb{C} \times \mathbb{C}$,

(ii) $(1,0) \in \mathbb{D}$ and $\text{Re}\{\phi(1,0)\} = 1 - \alpha > 0$,

(iii) for all $(iu_2, v_1) \in \mathbb{D}$ such that $v_1 \leq -(1 + u_2^2)/2$,

$$\begin{aligned} \text{Re}\{\phi(iu_2, v_1)\} &= \beta^2 - (1 - \beta)^2 u_2^2 + 2\beta(1 - \beta)v_1 - \alpha \\ &\leq (2\beta^2 - \beta - \alpha) - (1 - \beta)u_2^2 \\ &< 0 \end{aligned}$$

for β given by (2.3).

Noting that $\phi(u,v)$ satisfies the conditions in Lemma 1, we have that $\text{Re}\{p(z)\} > 0$ $(z \in \mathcal{U})$, which completes the proof of Theorem 1.

Making $\alpha = 0$ in Theorem 1, we have

COROLLARY 1. *If the function $f(z)$ defined by (1.1) is in the class $\mathcal{R}(0)$, then*

$$\text{Re}\sqrt{\frac{f(z)}{z}} > \frac{1}{2} \qquad (z \in \mathcal{U}). \tag{2.6}$$

Letting $zf'(z)$ instead of $f(z)$ in Theorem 1, we have

COROLLARY 2. *If the function $f(z)$ defined by (1.1) satisfies*

$$\text{Re}\{f'(z) + zf''(z)\} > \alpha \qquad (0 \leq \alpha < 1;\ z \in \mathcal{U}), \tag{2.7}$$

then

$$\text{Re}\sqrt{f'(z)} > \frac{1 + \sqrt{1 + 8\alpha}}{4} \qquad (z \in \mathcal{U}). \tag{2.8}$$

In order to give our next result, we have to recall here the following lemma due to Obradović and Owa [4].

LEMMA 2. *Let* $a > -1$ *and* $\alpha \geq (a + 1)/(a + 2)$. *Let the function* $f(z)$ *defined by* (1.1) *satisfy the condition*

$$\text{Re}\sqrt{\frac{f(z)}{z}} > \alpha \qquad (z \in \mathcal{U}). \tag{2.9}$$

Then

$$(2.10)\qquad \mathrm{Re}\left\{\frac{a+1}{z^{a+1}}\int_0^z t^{a-1}f(t)dt\right\} > \frac{2(a+1)\alpha^2+1}{2a+3}\qquad (z \in \mathcal{U}).$$

With the aid of Theorem 1 and Lemma 2, we have

THEOREM 2. Let $a > -1$, $0 \le \alpha < 1$, and

$$\beta = \frac{1+\sqrt{1+8\alpha}}{4} \ge \frac{a+1}{a+2}.$$

If the function $f(z)$ defined by (1.1) is in the class $\mathcal{R}(\alpha)$, then

$$(2.11)\qquad \mathrm{Re}\left\{\frac{a+1}{z^{a+1}}\int_0^z t^{a-1}f(t)dt\right\} > \frac{2(a+1)\beta^2+1}{2a+3}\qquad (z \in \mathcal{U}).$$

Letting $\alpha = 0$, Theorem 2 gives

COROLLARY 3. Let $-1 < a \le 0$ and $f(z) \in \mathcal{R}(0)$. Then

$$(2.12)\qquad \mathrm{Re}\left\{\frac{a+1}{z^{a+1}}\int_0^z t^{a-1}f(t)dt\right\} > \frac{a+3}{2(2a+3)}\qquad (z \in \mathcal{U}).$$

Further, taking $a = 0$ in Theorem 2, we have

COROLLARY 4. If the function $f(z)$ defined by (1.1) is in the class $\mathcal{R}(\alpha)$, then

$$\text{(2.13)} \qquad \operatorname{Re}\left\{ \frac{1}{z} \int_0^z \frac{f(t)}{t}\, dt \right\} > \frac{2\beta^2 + 1}{3} \qquad (z \in U),$$

<u>where</u>

$$\beta = \frac{1 + \sqrt{1 + 8\alpha}}{4}.$$

REFERENCES

[1] S. Fukui, S. Owa, S. Ogawa and M. Nunokawa, A note on a class of analytic functions satisfying $\operatorname{Re}\{f'(z)\} > \alpha$, Bull. Fac. Edu. Wakayama Univ. Nat. Sci. 36(1987), 13 - 17.

[2] S. S. Miller, Differential inequalities and Carathéodory function, Bull. Amer. Math. Soc. 81(1975), 79 - 81.

[3] S. S. Miller and P. T. Mocanu, Second order differential inequalities in the complex plane, J. Math. Anal. Appl. 65(1978), 289 - 305.

[4] M. Obradović and S. Owa, On one inequality for some regular functions in $|z| < 1$, Math. Japon. 32(1987), 971 - 978.

S. Owa: Department of Mathematics
Kinki University
Higashi-Osaka, Osaka 577
Japan

S. Fukui: Department of Mathematics
Wakayama University
Wakayama 640
Japan

O. Altintas: Department of Mathematics
Hacettepe University
Beytepe, Ankara
Turkey

Received January 27, 1988

Mailing Addresses

1.	O. Altintas	Department of Mathematics Hacettepe University Beytepe, Ankara, Turkey
2.	J.B. Conrey	School of Mathematics Institute for Advanced Study Princeton, NJ 08540 U.S.A.
3.	M. Csörgő	Department of Mathematics and Statistics Carleton University Ottawa, Ontario, Canada K1S 5B6
4.	D.A. Dawson	Department of Mathematics and Statistics Carleton University Ottawa, Ontario, Canada K1S 5B6
5.	S. Fukui	Department of Mathematics Wakayama University Wakayama 640, Japan
6.	A. Ghosh	Department of Mathematics Oklahoma State University Stillwater, OK 74078 U.S.A.
7.	I. Iscoe	Department of Mathematics and Statistics McGill University Montréal, Québec, Canada H3A 2K6
8.	V. Jurdjevic	Department of Mathematics University of Toronto Toronto, Ontario, Canada M5S 1A1
9.	I.A.K. Kupka	Department of Mathematics University of Toronto Toronto, Ontario, Canada M5S 1A1
10.	F. Lamarche	Department of Mathematics McGill University Montréal, Québec, Canada H3A 2K6
11.	Z. Lin	Department of Mathematics Hangzhou University Hangzhou, Zhejiang, People's Republic of China
12.	N.S. Mendelsohn	Department of Mathematics and Astronomy University of Manitoba Winnipeg, Manitoba, Canada R3T 2N2
13.	R.A. Mollin	Department of Mathematics University of Calgary Calgary, Alberta, Canada T2N 1N4

14. K. Murasugi — Department of Mathematics
University of Toronto
Toronto, Ontario, Canada M5S 1A1

15. S. Owa — Department of Mathematics
Kinki University
Higashi-Osaka, Osaka 577, Japan

16. R. Padmanabhan — Department of Mathematics and Astronomy
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

17. E.A. Perkins — Department of Mathematics
University of British Columbia
Vancouver, British Columbia, Canada V6T 1Y4

18. R. Robson — Department of Mathematics
Oregon State University
Corvallis, Oregon 97331-4605 U.S.A.

19. B. Schmuland — Department of Statistics and Applied Probability
University of Alberta
Edmonton, Alberta, Canada T6G 2G1

20. P.G. Walsh — Department of Mathematics
University of Calgary
Calgary, Alberta, Canada T2N 1N4

21. B. Wolk — Department of Mathematics and Astronomy
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2