vol 33(2000)

THE PUNJAB UNIVERSITY JOURNAL OF MATHEMATICS

DEPARTMENT OF MATHEMATICS
UNIVERISTY OF THE PUNJAB
LAHORE-54590
PAKISTAN

Notice to Contributors

1. The Journal is meant for publication of research papers and review articles covering state of the art in a particular area of mathematical science.

2. Manuscripts should be typewritten and in a form suitable for publication. As far as possible, the use of complicated notations should be avoided. Figures, drawn on separate sheets of white paper in Black Ink, should be suitable in size for inclusion in the Journal.

3. **The contributors are required to provide the disk containing the file of the paper composed in Latex or Scientific Workplace.**

4. References should be given at the end of the paper and be referred to by numbers in serial order on square brackets, e.g. [3]. Reference should be typed as follows:

Reference to Paper:

Hoo, C. S. BCI-algebra with conditions, *Math. Japonica* 32, No. 5 (1987) 749-756.

Reference to Book:

Mitchel, B.: Theory of categories, New York: Academic Press, 1965.

5. Contributions and other correspondence should be addressed to Managing Editor, Mathematics Department, Punjab University, Quaid-e-Azam Campus, Lahore-54590, Pakistan.

6. The decision to accept or reject a paper for publication in the Journal rests fully with the Editorial Board.

7. Authors, whose papers will be published in the Journal, will be supplied 10 free reprints of their papers and a copy of the issue containing their contributions.

8. The Journal which is published annualy will be supplied free of cost in exchange with other Journals of Mathematics.

Now $PS - QR = 1$, forces that

$$-P^2 - \left(\frac{2aP - bR}{-c}\right) R = 1$$

$$\frac{2aPR}{c} - \frac{b}{c}R^2 = 1 + P^2$$

$$P\left(\frac{2a}{c}\right) R - \left(\frac{a^2 - p}{c^2}\right) R^2 = 1 + P^2 \qquad \therefore \quad b = \frac{a^2 - p}{c}$$

$$\Rightarrow p\frac{R^2}{c^2} = P^2 - \frac{2a}{c}PR + \frac{a^2R^2}{c^2} + 1$$

$$p = \frac{c^2P^2}{R^2} - P\frac{2ac}{R} + a^2 + \frac{c^2}{R^2}$$

$$p = \left(\alpha - \frac{cP}{R}\right)^2 + \left(\frac{c}{R}\right)^2$$

Hence, by known results 1.1 and 1.2 we have $p \equiv 1 \pmod 4$.

REFERENCES

[1] Ivan Niven, Herbert S. Zuckerman, *The theory of numbers,* John Willey and Sonc Inc (1991).

[2] Willaim Judson Leveque, *Topics in number theory,* Volume 1, Addision Wesley Publishing Company, Inc. (1965).

[3] Q. Mushtaq, *Modular group acting on real quadratic fields,* Bull Austral Math Soc 37 (1988), 303-309.

[4] Q. Mushtaq, *Reduced Indefinite binary quadratic forms and orbits of the modular group,* Radovi Mathematicki Volume 4 (1988) 331-336.

[5] Imrana Kausar, S. M. Husnine, A. Majeed, *Behaviour of Ambiguous and Totally Negative elements of $Q^*(\sqrt{n})$ under the action of the Modular Group,* Punjab University Journal of Mathematics, Vol. XXX (*1997), 11-34.

[6] Imrana Kousar, S. M. Husnine, A. Majeed, *Action of the group* $H =< t, y: \ t^3 = y^3 = 1 >$ *on the Quadratic Fields,* Punjab University Journal of Mathematics, Vol. XXX (1997), 47-66.

[7] Imrana Kousar, S. M. Husnine, A. Majeed, *Classification of the elements of* $Q^*(\sqrt{p})$ *and a partition of* $Q^*(\sqrt{p})$ *under the action of Modular Group PSL (2, Z),* Punjab University Journal of Mathematics, Vol. XXXI(1998).

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 135–144

FIXED POINT AND BEST APPROXIMATION THEOREMS FOR *-NONEXPANSIVE MAPS

A. R. Khan
Department of Mathematical Sciences
King Faud University of Petroleum and Minerals
Dhahran 31261
Saudi Arabia
E-mail: arahim@kfupm.edu.sa
(On leave from Bahauddin Zakariya University, Multan 60800, Pakistan

N. Hussain
Center for Advanced Studies in Pure and Applied Mathematics
Bahauddin Zakariya University
Multan 60800, Pakistan
E-mail: mnawab@yahoo.com
(Received 20 May, 2000)

In this paper we obtain fixed point and best approximation theorems for

*-nonexpansive multivalued maps defined on a closed convex (not necessarily bounded) subset of a Banach space under certain boundary conditions. The results herein contain those of Husain and Tarafdar. Husain and Latif, Park, Singh and Watson, Xu and others.

We gather together some definitions and facts which will be used in this paper. Let C be a nonempty subset of a Banach space X. We denote by 2^X, $CB(X)$ and $K(X)$ the families of all nonempty, nonempty closed bounded and nonempty compact subsets of X respectively. The Hausdorff metric on $CB(X)$ induced by the metrix d on X is defined as

$$H(A,B) = \max\left\{ \sup_{a \in A} d(a,B), \ \sup_{b \in B} d(b,A) \right\}$$

for A, B in $CB(X)$, where $d(a,B) = \inf_{b \in B} d(a,b)$.

A multivalued map $T : C \to CB(X)$ is called nonexpansive if $H(Tx,Ty) \leq d(x,y)$ for all x, y in C. A multivalued map $T : C \to 2^X$ is said to be

(i) Weakly nonexpansive [4, 5] if given $x \in C$ and $u_x \in Tx$ there is a $u_y \in T_y$ for each $y \in C$ such that $d(u_x, u_y) \leq d(x,y)$

(ii) *-nonexpansive [5, 14] if for all x, y in C and $u_x \in Tx$ with $d(x,u_x) = d(x,Tx)$ there exists $u_y \in Ty$ with $d(y,u_y) = d(y,Ty)$ such that $d(u_x,u_y) \leq d(x,y)$.

(iii) Upper semicontinuous (usc) (lower semicontinuous (Isc)) if

$T^{-1}(B) = \{x \in C : \ Tx \cap B \neq \phi\}$ is closed (open) for each closed (open) subset B of X, T is continuous if T is both usc and Isc.

(iv) Weakly inward if $Tx \subset$ cl $(I_c(x))$ for all $x \in C$, where the inward set $I_C(x)$ of C at $x \in X$ is defined by $I_C(x) = \{x + \gamma(y-x) : y \in C \text{ and } \gamma \geq 0\}$ and 'cl' means taking closure.

(v) Satisfy the Leray-Schauder conditions (in case C has nonempty interior) if there is point z in interior of C such that for each $y \in Tx$.

$$y - z \neq \lambda(x-y) \quad \text{for all} \quad x \in BdC \quad \text{and} \quad \lambda > 1$$

For given $T : C \to 2^X$, we say that C is (KR)-bounded with respect to (w.r.t) T (cf. [8] and [10]) if for some bounded set $A \subset C$ the set

$$G(A) = \cap_{a \in A} G(a, Ta)$$

is either empty or bounded where $G(a,Ta) = \bigcup_{y \in Ta} G(a,y)$ and $G(a,y)$ $= \{z \in C : \|z-a\| \geq \|z-y\|\}$. In what follows, we denote by $P_T(x)$ the (possibly empty) set $\{u_x \in Tx : d(x,u_x) = d(x,T(x)\}$ for each $x \in X$ (cf. [14]). A single valued map $f : C \to X$ is said to be a selector of T if $f(x) \in Tx$ for each $x \in C$.

Bd, and Int, denote the boundary and interior respectively.

The concept of *-nonexpansiveness is different from continuity and hence nonexpansiveness for multivalued mappings $T : C \to 2^X$, as is clear from the following example.

Example Let $X = R^2$ be equipped with Euclidean norm and $C = \{(a,0) : 1/\sqrt{2} \leq a \leq 1\} \cup \{(0,0)\}$

Define $T : C \to 2^X$ by

$$T(a,0) = \begin{cases} (0,1), & \text{if } a \neq 0 \\ L = \text{the line Segment } [(0,1),(1,0)], & \text{if } a = 0 \end{cases}$$

The $P_T(a,0) = \{(0,1)\}$ for all $(a,0) \neq (0,0)$ in C and $P_T(0,0) = \{(1/2,1/2)\}$. This clearly implies that T is *-nonexpansive. But T is not continuous multifunction (cf. [12], p.537).

Also note that $u_x = (1,0) \in T(0,0)$. For any $y = (a,0) \in C$ with $a \neq 0$, $u_y = (0,1)$ such that $|u_x - u_y| = |(1,0) - (0,1)| = \sqrt{2} > |x - y|$. Thus T is not weakly nonexpansive.

A particular form of Theorem 4 due to Park [9] stated below will be needed (see also Theorem A[10]).

Theorem A Let X be a uniformly convex Banach space, C a nonempty closed convex subset of X and $f : C \to X$ a nonexpansive map such that C is (KR) -bounded. Suppose that one of the following holds:

(a) f is weakly inward.

(b) $0 \in \text{Int } C$ and $fx \neq \lambda$ for all $x \in BdC$ and $\lambda > 1$ (i.e. f satisfies Leray-Schauder condition).

Then f has a fixed point.

The following is due to Reich [11].

Theorem B Let C be a closed convex subset of a Banach space X such that the metric projection is usc. If $f : C \to X$ is continuous $f(C)$ is relatively compact, then there is a $y \in C$ such that $\|y - fy\| = d(fy, C)$.

Results The proof of following general theorem is based on Theorem A.

Theorem 1 Let C be a nonempty closed convex subset of a uniformly convex Banach space X and $T : C \to 2x$ closed convex valued *-nonexpansive map such that C is (KR) -bounded with respect to T. Then T has a fixed point under each one of the following boundary conditions.

(1) T is weakly inward.

(2) $\lim_{h\to 0+} d[(1-h)x + hy, C]/h = 0$ for all $x \in C$ and $y \in Tx$.

(3) $0 \in \text{Int } C$ and $y \neq \gamma x$ for all $x \in BdC, y \in T_x$ and $\gamma > 1$.

(4) $T(BdC) \subset C$.

Proof Since $T(x)$ is a nonempty closed convex subset of a uniformly convex Banach space X, therefore each u_x in $P_T(x)$ is unique. Thus by the definition of *-nonexpansiveness of T, there is $u_y = P_T(y) \in Ty$ for all y in C such that

$$\|P_T(x) - P_T(y)\| = \|u_x - u_y\| \leq \|x - y\|$$

So $P_T : C \to X$ is nonexpansive. The (KR) boundedness of C w.r.t. T clearly implies that C is (KR)-bounded w.r.t. P_T.

(1) As T is weakly inward so for each $x \in C$, $Tx \subset \text{cl } (I_C(x))$. Since $P_T(x) \in Tx$ for each $x \in C$ therefore $P_T(x) \in \text{cl } (I_C(x))$ for all $x \in C$. Hence $P_T : C \to X$ is weakly inward. Theorem A(a) implies that P_T has a fixed point. That is there is some x_0 in C such that $P_T(x_0) = x_0$. But $P_T(x) \in Tx$ for each $x \in C$ so $x_0 = P_T(x_0) \in T(x_0)$ as required.

(2) It is known (cf.[10]), p.654) that $f : C \to X$ is weakly inward if and only if $\lim_{h\to 0+} d[(1-h)x + hf(x), C]/h = 0$ for all x in a closed convex subset C of a Banach Space. As $P_T(x) \in T_x$ for all $x \in C$ so $\lim_{h\to 0+} d[(1-h)x+hP_T(x), C]/h = 0$ for $x \in C$. This implies that $P_T : C \to X$ is weakly inward. Now the result is obvious from (1).

(3) As $P_T(x) \in Tx, P_T(x) \neq \gamma x$ for all $x \in BdC$ can $\gamma > 1$. Thus P_T satisfies Leray- Schauder condition. So by Theorem $A(b)$, P_T and therefore T has a fixed

point.

(4) Since $C \subset I_C(x)$ for all $x \in C$ and $I_C(x) = X$ if x is an interior point, therefore T is weakly inward. The conclusion now follows from (1).

This completes the proof.

For single valued map T the concepts of nonexpansiveness and *-nonexpansiveness coincide. Thus we have the following;

Corollary 2 Let C be a nonempty closed convex subset of a uniformly convex Banach space X and $T : C \to X$ a nonexpansive map such that C is (KR)-bounded w.r.t. T. Then T has a fixed point provided one of the boundary conditions (1)-(4) of Theorem 1 holds.

Corollary 2 extends Theorem 3 (4), (8) and (LS) due to Park [10] from Hilbert space set up to that of uniformly convex Banach space. Here we also obtain conclusions of Corollary 15[3] and Remarks 3.9(iv) [15] when C is closed convex and (KR)-bounded.

In case $T : C \to 2^C$ in Theorem 1, we have;

Corollary 3 Let C be a nonempty closed convex subset of a uniformly convex Banach space X and $T : C \to 2^C$ a closed convex valued *-nonexpansive map such that C is (KR)-bounded w.r.t. T. Then T has a fixed point.

Remark 4(i) In Theorem 3.2 [5], the same conclusion was proved under assumptions of the boundedness of C and Opial's condition of X. Here we obtained the same conclusion if C is (KR)-bounded w.r.t. T.

(ii) Corollary 3 provides the conclusion of Corollary 1 [14] for uniformly convex Banach space X without the boundedness of C (see also Remark 3 [14]).

(iii) *-nonexpansive multivalued maps need not be continuous so Theorem 1 applies to the fixed point theory of multifunctions which are not necessarily continuous.

Corollary 5[1] Let C be a nonempty weakly compact convex subset of a uniformly convex Banach space and $T : C \to C$ a nonexpansive map. Then T has a fixed point.

Multivalued analogues of Ky Fan's best approximation theorem have been considered by researchers and interesting applications towards fixed point theory of multifunctions are given by them. We establish a version of this important theorm for *-nonexpansive multivalued maps as follows.

Theorem 6 Let C be a nonempty closed convex subset of a uniformly convex Banach space X. If $T : C \to 2^X$ is closed convex valued *-nonexpansive map and $T(C)$ is relatively compact, then T possesses a nonexpansive selector f such that

$$\|y - fy\| = d(fy, C) \quad \text{for some} \quad y \in C$$

If in addition $\|fy - Qfy\| = d(Ty, C)$ then $d(y, Ty) = d(Ty, C)$, where Q is projection map of X onto C.

Proof If C is closed and convex subset of a uniformly convex Banach space X, then the projection map $Q : X \to 2^C$ defined by

$$Q(x) = \{y \in C : \|x - y\| = d(x, C)\}$$

is single valued and continuous (see [12]), p.535). As in Theorem 1, $P_T : C \to X$ is nonexpansive selector of T. Since $T(C)$ is relatively compact and $P_T(C) \subseteq T(C)$, therefore $P_T(C)$ is relatively compact. By Theorem B, there exists $y \in C$ such that

$$\|y - P_T(y)\| = d(P_T(y), C)$$

By definition of P_T we have $d(x, P_T x) = d(x, U_x) = d(x, T_x)$ for each $x \in C$. Thus $d(y, P_T y) = d(y, Ty)$ and hence $d(y, Ty) = d(y, P_T y) = d(P_T y, C) = \|P_T y - Q\ P_T y\| = d(Ty, C)$ as desired.

If $T : C \to X$, then we have the following extension of Theorem 5 due to Singh and Watson [13].

Theorem 7 Let C be a nonempty closed convex subset of a uniformly convex Banach space X. If $T : C \to X$ is nonexpansive map and $T(C)$ is relatively compact, then there exists a point y in C such that

$$\|y - Ty\| = d(Ty, C)$$

As an application of Theorem 7, we get the following fixed point result, which generalized Theorem 6 and 7 [13].

Corollary 8 Let C be a nonempty closed convex subset of a uniformly convex Banach space X. If $T : C \to X$ is nonexpansive map, $T(C)$ is relatively compact and T satisfies any one of the following conditions:

(1) For each x on the boundary of $C, \|Tx - y\| \leq \|x - y\|$ for some y in C.

(2) For any u on the boundary of C with $u = Q_0T(u)$, that u is a fixed point of T.

Then T has a fixed point in C.

In case $T : C \to 2^C$ in Theorem 6, we have the following fixed point result for

*-nonexpansive maps which provides the same conclusion as of Cor. 3 with different conditions that $T(C)$ is relatively compact.

Corollary 9 Let Cbe a nonempty closed convex subset of a uniformly convex Banach space X and $T : C \to 2^C$ a closed convex valued *-nonexpansive map such that $T(C)$ is relatively compact. Then T admits a fixed point.

Note that if T is single valued then the conclusion of Corollary 5 holds for closed and convex set C.

Following generalizes Theorem 3.2[5], corresponding results in [4] and [6] and Theorem 2 by Xu [4].

Theorem 10 Let X be a Banach space satisfying Opial's condition and C be a weakly compact starshaped subset of X. Then each *-nonexpansive compact valued map $T : C \to 2^C$ has a fixed point.

Proof Since for each $x \in C, Tx$ is nonempty and compact so $P_T(x)$ is nonempty and compact. As in Theorem 1, $P_T : C \to 2^C$ is nonexpansive. Thus P_T and hence T has a fixed point by Corollary 3.11 [15].

Remarks 11 (i) If T is single valued, then the conclusion of Corollary 5 holds for weakly compact starshaped subset of a Banach space satisfying Opial's condition.

(ii) All Hilbert spaces and l^p spaces $(1 < p < \infty)$ satisfy Opial's condition but $L^p[0,1] (p \neq 2)$ are uniformly convex Banach spaces which do not satisfy Opial's condition.

Acknowledgement The author A. R.Khan acknowledges gratefully the support provided by King Fahd University of Petroleum and Minerals during this research.

REFERENCES

[1] F. E. Browder, *Nonexpansive nonlinear Operators in a Banach space,* Proc. Nat. Acad. Sci. U.S.A., 54(1965), 1041-1044.

[2] F. E. Browder and W. V. Petryshyn, *Construction of fixed points of nonlinear mappings in Hilbert spaces,* J. Math. Anal., 20 (1967), 197-228.

[3] T. H. Chang and C.L. Yen, *Some fixed point theorems in Banach space,* J. Math. Anal. Apple. 138 (1989) 550-558.

[4] T. Husain and E. Tarafdar, *Fixed point theorems for multivalued mappings of nonexpansive type*, Yokoh. Math. J, 28 (1980) 1-6.

[5] T. Husain and A. Latif, *Fixed points of multivalued nonexpansive maps*, Math. Japonica, 33, No. 3 (1988), 385-391.

[6] T. Husain and A. Latif, *Fixed points of multivalued nonexpansive maps*, Intern. J. Math & Math. Sci, 14 (1991), 421-430.

[7] W. A. Kirk, *A fixed point theorem for mappings which do not increase distances,* Amer. Math. Monthly, 72(1965), 1004-1006.

[8] W. A. Kirk and W. O. Ray, *Fixed point theorems for mappings defined on*

unbounded sets in Banach spaces, Studia Math., 64 (1979), 127-138.

[9] Sehie Park, *On a problem of Gulevich on nonexpansive maps in uniformly convex Banach spaces, comment.* Math. Univ. Carolinae, 37 (1996), 263-268.

[10] —–, *Best approximations and fixed points of nonexpansive maps in Hilbert spaces,* Numer. Funct. Anal. and Optimiz., 18 (5 & 6) (1997), 649-657.

[11] S. Riech, *Approximate selection, best approximations, fixed points and invariant sets,* J.Math. Anal. Appl, 62 (1978), 104-113.

[12] V. M. Sehgal and S. P. Singh, *A generalization to multifunctions of Fan's best approximation theorem,* Proc. Amer. Math. Soc., 102 (1988), 534-537.

[13] S. P. Singh and B. Watson, *Proximity maps and fixed points*, J. Approx. Theory 39 (1983), 72-76.

[14] H. K. Xu, *On weakly nonexpansive and *-nonexpansive multivalued mappings,* Math. Japonica, 36, No.3 (1991), 441-445.

[15] S. Zhang, *Star-shaped sets and fixed points of multivalued mappings,* Math. Japonica, 36, No. 2(1991), 327-334.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 145–152

RSA CIPHERS WITH MAPLE

Farasat Tahir
Mathematics Department
Government Postgraduate College for Women
Satellite Town, Gujranwala (Pakistan)

Muhammad Tahir
Mathematics Department
Government College
Gujranwala (Pakistan)

(Received 27 August, 1999)

ABSTRACT Although other programming languages are equally good and can be used to handle RSA cipher, Maple provides a more friendly environment in computational works. This paper demonstrates how nicely RSA cipher system works with Maple.

1. INTRODUCTION The widespread use of electronic communications in a commercial environment means that a great deal of data which was sent in a fairly secure manner in the past is now sent by communications links to which many people potentially have access. The aim of security measure is to minimize the vulnerability of assets and resources hence there is a need for concealing the contents of a message and for detecting any tempering with a message. Ciphers are more universal methods of transforming messages into a format whose meaning is not apparent. The most important technique is RSA cipher. As far as RSA system is concerned, there is no faster method of attack than factorization. In 1988 Caron and Silverman managed to factorize a 90-digit number into two prime numbers of 41 and 49 digits, with the add of 24 SUN-workstations. The required processing time was about six weeks. In the same year Lenstra and Manasse successfully factorized a prime number of 96 digits. They employed a large number of computers, which were interconnected by a combination of local area networks and electronic mail. The whole operation took 23 days, which effectively worked out to 10 years of CPU time.

Despite the algorithms for reducing the total number of calculations, the RSA system still requires considerable computational power for processing such large numbers. For this reason in practice the RSA system is not especially well suited for real-time encryption of large amounts of data. The RSA system is therefore often used for enciphering limited amounts of data, for instance for the transportation of secret keys. In this paper we use Maple (computational package of mathematics) to program RSA cipher.

2. BASIC TERMINOLOGY We suppose that one person, the sender, wishes to send another person, the recipient, a message which he/she wants to keep secret from an eavesdropper. The message must be transmitted over an inseure channel, to which it must be presumed the eavesdropper has access. The message is called the plaintext. It is enciphered or encrypted by an algorithm or a set of rules called the encryption algorithm. This algorithm is controlled by a string of symbols called the key. The key is kept secret from every one except the sender and recipient and it should be easily changed in case it has somehow been discovered by the eavesdropper. The output from this algorithm is called the cipher, ciphertext or cryptogram. The inverse process called decryption or deciphering applies the same or a different mathematical function to change the ciphertext back to the original plaintext. It is also controlled by a key. The breaking of a cipher system by an eavesdropper is called cryptanalysis. The difference between cryptanalysis and decryption is that the cryptanalyst has to manage without the decryption key. A cipher system has following components:

1. plaintext message space, M.
2. ciphertext message space, C.
3. key space, K.
4. family of enciphering algorithms, $E_k : M \to C$, where $k \in K$.
5. family of deciphering algorithms, $D_k : C \to M$, where $k \in K$.

Cipher systems must satisfy three general requirements:

1. The enciphering and deciphering algorithms must be efficient for all keys.
2. The system must be easy to use.
3. The security of the system should depend only on the secrecy of the keys and not on the secrecy of the enciphering and deciphering algorithms.

Different cipher systems have different levels of security, depending on how hard they are to break. The security is directly related to the difficulty associated with inverting encryption transformation of a system. Now we will take a look at some methods used in encryption.

2.1. Simple-Substitution Cipher This cipher replaces each character of plaintext with a corresponding character called its substitute. A single one-to-one mapping from plaintext to ciphertext character is used to encipher an entire message.

2.2. Block Cipher Let M be aplaintext message. A block cipher breaks M into successive blocks $M_1, M_2, \cdots$, and enciphers each M_1 with the same key k. Each block is typically several characters long.

2.3. Running Key Cipher In a running-key cipher, the key is as long as the plaintext message. Assume that the letters of plaintext are represented by integers in the ciphertext. The letters are then regarded as integers from 1 to 26 with a = 1 and z = 26 and a blank space is given by the value 27.

2.4. Public Key Cipher In a public-key cryptosystem, the public- key algorithm uses an encryption key different from the decryption key. Since the public key is published, a stranger can use it to encrypt a message which can be decrypted only by the the owner of the private key. For this reason public-key systems are also referred to as non symmetric or one-way.

RSA Cipher [1] The RSA cipher named after its discoverers, Rivest, Shamir and Adleman. The RSA cipher is based on the fact that it is relatively easy to calculate the product of two prime numbers, but that determining the original prime numbers, given the product, is far more complicated.

The encryption and decryption procedure is as follows:

1. Find two large primes p and q, each about 100 digits long and define n by $n = pq$.

2. Compute the unique integer e in the range $1 \leq e \leq (p-1)(q-1)$ that is coprime to $(p-1)(q-1)$. This should be easy if e is prime and is not a factor of $(p-1)(q-1)$.

3. Finally the value of e is used to determine another number, d, for which $ed \equiv 1 \pmod{(p-1)(q-1)}$. The numbers n, e and d are referred to as the modulus, encryption and decryption exponents respectively.

4. Release the pair of integers (e, n) as public key while keeping the numbder d safe to decrypt.

5. Represent M, the message to be transmitted, into an integer, break M into blocks if it is too big.

6. Encrypt M into ciphertext C by the rule $C \equiv M^e \pmod{n}$.

7. Decrypt by using the private key d and the formula $D \equiv C^d \pmod{n}$.

Theorem [2] Consider a message M, which is enciphered according to the RSA system, resulting in a ciphertext $C \equiv M^e \pmod{n}$. The receiver deciphers this message into $D \equiv C^d \pmod{n}$, ensuring that $ed \equiv 1 \pmod{(p-1)(q-1)}$. Then for all cases: $D = M$.

The security of this system relies on the fact that it is almost impossible to calculate the value of d if only the public key (e, n) is known. Thus, the person who issues the public key (e, n) is the only person who knows the precise value of d and therefore also the only person able to decipher encrypted texts.

4. MAPLE WORKSHEET (RSA Cipher)

Computation of n and d

Enter any two large integers.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 1–6

SYMMETRY AND ANTISYMMETRY RESTRICTIONS ON THE FORM OF TRANSPORT FOR MAGNETIC CRYSTALS

M. Shafiq Baig
Department of Mathematics
University of Azad Jammu and Kashmir
Muzaffarabad (A.K.) Pakistan.

(Received 30 October, 1998)

ABSTRACT By using the transformation law for field dependent tensors, the restrictions due to magnetic moment inversion and spatial symmetry on the forms of the magneto-conductivity tensor $\sigma_{ij}(\mathbf{B})$ have been found for magnetic crystals.

Key words: magnetic moments, magnetic point group, transport tensor.

INTRODUCTION There are 1651 3-dimensional Shubnikov space groups which exist when the magnetic moment inversion operator R is taken into account. These are catagorized as follows:

(a) 230 Fedorov generating groups which contain magnetic-inversion as an element.

(b) 230 Senior groups which do not involve magnetic-inversion and

(c) 1191 Junior bicolour groups which contain magnetic-inversion only in combination with spatial transformations.

(a) refers to nonmangetic crystals whereas (b) and (c) refer to magnetic crystals.

The number of space groups, point groups and Laue (enantiomorphous) groups in each of the categories (a), (b) and (c) are as follows[1]:

	(a)	(b)	(c)	**Total**
Space groups	230	230	$517 + 252 + 422$	1651
Point groups	32	32	$21 + 37$	122
Laue groups	11	11	10	32

In the 122 generalized point groups, there are 32 which are obtained by augmenting (increase in number) each of the 32 classical crystallographic point groups by R and its products with the elements of the classical point groups [2]. These are known as grey groups. Of the remaining 90 groups, 32 are identical with the classical groups in the sense that they do not contain either the operator R or any antisymmetric operation. They are called single coloured crystallographic point groups. The remaining 58 groups do not contain R but contain classical as well as anti-symmetric operations. They are called bicoloured magnetic point groups $\{M\}$. The above mentioned 32 classical point groups $\{S\}$ representing the geometric symmetry properties of the 32 classical crystal classes [2, 3]. Their elements consist of rotations and reflections only and can be represented by 3×3 orthogonal matrices in 3-dimensional Euclidean space. They obviously form finite subgroups of $O(3)$ and $GL(3)$.

DISCUSSION [4] and [5] have used the transformation law for field dependent tensors in conjunction with the Onsager reciprocity relation

$$\sigma_{ij}(\mathbf{B}) = \sigma_{ij}(-\mathbf{B}) \tag{1}$$

to establish the form of the magneto-conductivity tensor $\sigma_{ij}(\mathbf{B})$ for each of the 32 classical point groups $\{S\}$. We have now extended that work to find the effects of spatial and magnetic moment inversion symmetry on the tensors that represent the transport coefficients of magnetic materials. This problem has been subjected to some debate as successive workers have been given their particular prescriptions for determination of the symmetry restricted forms of the transport coefficients. After an examination of the treatments of [2] (prescription-A) and [1] (prescription-B), [7] provided a prescription-C which, although concurring with

Kleiner's objection that prescription-A ignored the antiunitary elements of the magnetic point groups, did predict in certain instances different forms of $\sigma_{ij}(\mathbf{B})$. We accept Cracknell's objections to the arguments of both Birss and Kleiner and make some further modifications of our own, one of the most important of which is that the transport tensors are not second rank constant tensors T_{ij} which transform according to

$$T_{ij} = R_{ip} R_{jq} T_{pq} \tag{2}$$

but are magnetic field dependent second rank polar tensors whose transformation law is [4]

$$\sigma_{ij}(|R|R_{1q}B_q, |R|R_{2q}B_q, |R|R_{3q}B_q) = R_{im} R_{jn} \sigma_{mn}(B_1, B_2, B_3) \tag{3}$$

It is at this point that we depart from the previous treatments; the transport tensors transform according to (3) not (2); failure to recognize this has lead earlier to incorrect simplification of the tensors.

Studies of biocoloured magnetic point groups and space groups stem from the introduction by [6] of an antisymmetry operator in addition to the spatial symmetry operators. In most magnetic materials, the magnetic moment can be either parallel or antiparallel to a given direction. For such a physical property, which can take only one or other of two characteristic values, the antisymmetry operator has the effect of changing one of these values to the other. When the symmetry operator R (which for bicoloured magnetic point groups will be the magnetic moment inversion operator) is taken into account, the three types of magnetic point groups $\{M\}$ corresponding to the 32 classical crystallographic point groups $\{S\}$ are:

(i) Type I: Magnetic point groups (there are 32), which do not contain R, i.e. $\{M\} = \{S\}$.

(ii) Type II: Magnetic point groups (there are 32), which do contain R as an element on its own and in combined form RG with G, an element of the classical point groups $\{S\}$, i.e. $\{M\} = \{S\} + R\{S\}$.

(iii) Type III: Mangnetic point groups (there are 58), which contain R only in combination (RG) with the classical point group symmetry elements i.e. $\{M\} = H + R(\{S\} - H)$.

where H is a normal subgroup of the classical point group $\{S\}$.

Type II groups refer to "non-magnetic" crystals (really paramagnetic and diamagnetic crystals and some antiferromagnetic crystals). Types I and III groups refer to magnetic crystals. Several previous workers [1, 2, 7] have identified the magnetic moment inversion operator R with the time-inversion operator θ, but this identification is open to doubt. The operator R commutes with all the spatial symmetry operators i.e. $RG = GR$, where G is an element of the coset $(\{S\} - H)$. To find the form of $\sigma_{ij}(\mathbf{B})$ for magnetic point groups, we need to take account of the symmetry operator belonging to the subgroup H and in addition the operators RG. We treat the problem throughout as an exercise in transformation of field dependent tensors, that is an operator must be applied both to the tensor components and their arguments.

To do this, we must first consider the effect of R on a field dependent tensor by ensuring the invariance of the corresponding physical law under that operator. In the present case Ohm's law of direct current in the presence of a magnetic field:

$$J_i(\mathbf{B}) = \sigma_{ij}(\mathbf{B})E_j \tag{4}$$

Under the operation of magnetic moment inversion, this becomes

$$RJ_i(\mathbf{B}) = R\sigma_{ij}(\mathbf{B})RE_j \tag{5}$$

To find the effect of R on $\sigma_{ij}(\mathbf{B})$, it is required to know the effect of R on $J_i(\mathbf{B})$ and E_j. The electric field vector E_j is invariant under R

$$RE_j = E_j \tag{6}$$

The effect of R on $\mathbf{B}$ is defined as

$$R\mathbf{B} = -\mathbf{B} \tag{7}$$

When the operator R acts on a system containing a magnetic moment and a current density $J_i(\mathbf{B})$, the only effect is to alter the direction of $\mathbf{B}$ and so

$$RJ_i(\mathbf{B}) = J_i(R\mathbf{B}) = J_i(-\mathbf{B}) \tag{8}$$

For Ohm's law to hold in the system under the operation of magnetic moment inversion, substitution of (6) and (8) into (5) leads to

$$R\sigma_{ij}(\mathbf{B}) = \sigma_{ij}(-\mathbf{B}) \tag{9}$$

For the symmetry operations RG, Neumann's principle demands that

$$RG\sigma_{ij}(\mathbf{B}) = \sigma_{ij}(RG\mathbf{B})$$

Therefore

$$GR\sigma_{ij}(\mathbf{B}) = \sigma_{ij}(GR\mathbf{B}) \tag{10}$$

since $RG = GR$. Substituting for $R\sigma_{ij}(\mathbf{B})$ from (9), we obtain

$$RG\sigma_{ij}(-\mathbf{B}) = \sigma_{ij}(GR\mathbf{B}) = \sigma_{ij}(-G\mathbf{B})$$

Therefore

$$G\sigma_{ij}(\mathbf{B}) = \sigma_{ij}(G\mathbf{B}) \tag{11}$$

Thus we obtain

$$\sigma_{ij}(|G|G_{1q}B_q, |G|G_{2q}B_q, |G|G_{3q}B_q) = G_{im}G_{jn}\sigma_{mn}(B_1, B_2, B_3) \tag{12}$$

Therefore, the transformation law (3) for $\sigma_{ij}(\mathbf{B})$ (or $\rho_{ij}(\mathbf{B})$) applies to crystals belonging to any of the three types (I, II, III) of magnetic point groups. When $\mathbf{B} \neq 0$, the form of $\sigma_{ij}(\mathbf{B})$ does not depend on whether the specimen consists of a non-magnetic crystal in an applied magnetic field of a magnetically ordered crystal.

CONCLUSION The symmetry restricted forms of $\sigma_{ij}(\mathbf{B})$ for crystals belonging to magnetic point groups $\{M\}$are identical to those of corresponding crystals of groups $\{S\}$ which have been listed for $\mathbf{B}$ directed along the major crystallographic axes by [4] in the even and odd terminology. Our prescription - D for finding the forms of $\sigma_{ij}(\mathbf{B})$ for a crystal belonging to a magnetic point group is as follows:

(i) Find the corresponding classical point group $\{S\}$ of the magnetic point group $\{M\}$ noting that $\{M\}$ depends upon the direction of $\mathbf{B}$,

(ii) Take the Laue group of this classical point group (see table 1 of [4a]) and use its generating elements in the transformation equation (3) for field dependent tensors to distinguish the non-zero components for a chosen magnetic field direction; and

(iii) apply Onsager's relation (1).

The magnetoresistivity tensor $\rho_{ij}(\mathbf{B})$ and the magnetothermal conductivity $k_{ij}(\mathbf{B})$ take the same forms as $\sigma_{ij}(\mathbf{B})$. The forms of the magnetothermoelectric power $\alpha_{ij}(\mathbf{B})$ and the magneto-Peltier effect $\pi_{ij}(\mathbf{B})$ for the magnetic point groups $\{M\}$ are also the same as those of classical point group crystals in a magnetic field; these have been tabulated by [4b].

REFERENCES

[1] Kleiner, W.H. *Space-time Symmetry of Transport coefficients,* Phyical Review, 142(2), 318. 1996.

[2] Birss, R. R. *Symmetry and Magnetism* Rep. Prog. Phys. 26, 307 Amsterdam: North Holland 1964.

[3] Jaswon, M.A. & Rose, M.A. *Crystal Symmetry: Theory of colour crystallography* John Wiley and Sons, 1983.

[4] Akgoz, Y.C. and Saunders, G.A. *Space-time Symmetry Restrictions on the form of transport tensors:I. Galvanomagnetic effects and II. Thermomagnetic effects* J. Phys. C, Solid State Phys. Vol. 8, 1975.

[5] Baig M.S. *Magnetic Symmetry Restrictions on the Transport Equations,* Ph.D. Thesis, Gazi University ANKARA, 1991.

[6] Muhsin Mert & Baig M.S. *Magnetic Symmetry Restrictions on Linear Transport Tensors* J. of Science of the Faculty of Arts and Science, Gazi University, ANKARA Vol. 5, pp.151-164, 1995.

[7] Cracknell, A.P., Phys. Rev., B7-2145. 1973.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 7–16

PROPERTIES OF THE T-FUZZY SUBHYPERGROUPS

B.Davvaz
Department of Mathematics,
University of Yazd,
P.O. Box: 89195-741,
Yazd, İran
&
Institute for studies in Theoretical Physics and Mathematics,
Tehran, Iran
E-mail: davvaz@vax.ipm.ac.ir

(Received 3 March, 1999)

ABSTRACT The concept of a fuzzy subset of a non-empty set first was introduced by Zadeh in 1965. Recently, the present author applaid the concept of fuzzy sets theory in the theory of algebraic hyperstructures.

In this paper we study the concept of T-fuzzy subhypergroup and anti T^*-fuzzy subhypergroup of a hypergroup H where T and T^* are t-norm and t-conorm respectively. We also obtain some interesting related results.

AMS Mathematics Subject Classification: 20N20, 04A72.

Keyword and phrases Hypergroup; Fuzzy set; t-norm, t-conorm; Fundamental relation; Fundamental group.

1. INTRODUCTION The concept of fuzzy subsets was introduced by Zadeh [20] in 1965. In 1971, Rosenfeld [15] applied this concept to the theory of groups and introduced the concept of a fuzzy subgroup of a group. Since then, a host of mathematicians are engaged in fuzzifying various notions and results of abstract algebra. In 1975, Negoita and Ralescu [14] considered a generalization of Rosenfeld's definition in which the unit interval [0, 1] was replaced by an appropriate lattice structure. In 1979, Anthony and Sherwood [2] redefined a fuzzy subgroup of a group using the concept of triangular norm. This notion was introduced by Schweizer and Sklar [16], in order to generalize the ordinary triangle inequality in a metric space to the more general probabilistic metric space. Several mathematicians have followed the Rosenfeld-Anthony-Sherwood approach in investigating fuzzy group theory (cf. [1, 3, 4, 6, 17]).

The theory of algebraic hyperstructure which is a generalization of the concept of algebraic structures first was introduced by Marty in [13]. In [7, 8, 9, 10, 11] the present author applied the concept of fuzzy sets theory in the theory of algebraic hyperstructures.

In this paper we study the concept of T-fuzzy subhypergroup and anti T^*-fuzzy subhypergroup of a hypergroup H where T and T^* are t-norm and t-conorm respectively. We also study the structure of T-fuzzy subhypergroups under direct product.

2. PRELIMINARIES

We begin by giving some definitions. Although these definitions can be found in [2, 5, 7, 16, 20], they are repeated here to help to the reader.

Definition 2.1 A t-norm is a function $T : [0,1] \times [0,1] \to [0,1]$ satisfying, for every x, y, z in [0, 1]:

(i) $T(x,y) = T(y,x)$,

(ii) $T(x,y) \leq T(x,z)$ if $y \leq z$,

(iii) $T(x,T(y,z)) = T(T(x,y),z)$,

(iv) $T(x,1) = x, T(0,0) = 0$

A $t-$norm is Archimedean iff

(v) $T$is continuous, i.e., it is continuous function with respect to the usual topologies

(vi) $T(x,x) \geq x$.

Obviously, the function min defined on $[0,1] \times [0,1]$ is an Archimedean t-norm.

Definition 2.2 A t-conorm is a function $T^* : [0,1] \times [0,1] \to [0,1]$ satisfying, for every x, y, z in [0, 1]:

$$\begin{array}{ll} (i) & T^*(x,y) = T^*(y,x), \\ (ii) & T^*(x,y) \leq T^*(x,z) \ \text{ if } \ y \leq z, \\ (iii) & T^*(x, T^*(y,z)) = T^*(T^*(x,y),z), \\ (iv) & T^*(x,0) = x, T(1,1) = 1. \end{array}$$

Definition 2.3 Let X be a non-empty set, a mapping $\mu : X \to [0,1]$ is called a fuzzy subset of X. The complement of μ, denoted by μ^c, is the fuzzy set of X given by

$$\mu^c(x) = 1 - \mu(x), \quad \forall x \in X$$

Definition 2.4 Let G be a group. A fuzzy subset μ of G is said to be a T-fuzzy subgroup of G with respect to a t-norm T, if the following axioms hold:

$$\begin{array}{ll} (i) & T(\mu(x), \mu(y)) \leq \mu(xy), \quad \forall x, y \in G, \\ (ii) & \mu(x) \leq \mu(x^{-1}), \quad \forall x \in G \end{array}$$

Definition 2.5 A hyperstructure is a set H together with a function: $H \times H \to \mathcal{P}^*(H)$ called hyperoperation, where $\mathcal{P}^*(H)$ is the set of all non-empty subsets of H.

Definition 2.6 A hyperstructure $(H, \cdot)$ is called a hypergroup if the following axioms hold:

$$\begin{array}{ll} (i) & (x \cdot y) \cdot z = x \cdot (y \cdot z), \quad \forall x, y, z \in H, \\ (ii) & a \cdot H = H \cdot a = H, \quad \forall a \in H \end{array}$$

In the above definition if $x \in H$ and $A, B, \subseteq H$ then

$$A \cdot B = \bigcup_{a \in A b \in B} a \cdot b, \quad x \cdot B = \{x\} \cdot B, \quad A \cdot x = A \cdot \{x\}$$

A subset K of H is called a subhypergroup if $(K, \cdot)$ is a hypergroup.

Let H_1 and H_2 be two hypergroups. Then in $H_1 \times H_2$ we can define a hyperproduct as follows:

$$(x_1, y_1) \circ (x_2, y_2) = \{(a, b) | a \in x_1 \cdot x_2, b \in y_1 \cdot y_2\}$$

and we call this the direct hyperproduct. It is easy to see that $H_1 \times H_2$ equipped with the direct hyperproduct becomes a hypergroup.

Let $(H, \cdot)$ be a hypergroup. We define the relation β^* as the smallest equivalence relation on H such that the quotient H/β^* is a group. In this case β^* called the fundamental equivalence relation on H and H/β^* called the fundamental group. This relation is studied by Corsini [5], see also [18, 19]. Suppose $\beta^*(a)$ is the equivalence class containing $a \in H$, the product $\circ$ on H/β^* is as follows:

$$\beta^*(a) \circ \beta^*(b) = \beta^*(c), \quad \forall c \in \beta^*(a)\beta^*(b)$$

According to [5] if U be the set of all the finite products of H then a relation β can be defined on H such that $\beta = \beta^*$. For all $x, y \in H$, the relation β is as follows:

$$x\beta y \text{ iff } \{x, y\} \subseteq u \quad \text{for some} \quad u \in U$$

Theorem 2.7[19] Let H_1, H_2 be hypergroups. Let β_1^*, β_2^* and β^* be fundamental equivalence relations on H_1, H_2 and $H_1 \times H_2$ respectively, then

$$(H_1 \times H_2)/\beta^* \cong H_1/\beta_1^* \times H_2/\beta_2^*$$

Corollary 2.8 Let β_1^*, β_2^* and β^* be fundamental equivalence relations on H_1, H_2 and $H_1 \times H_2$ respectively, then

$$(x_1, y_1)\beta^*(x_2, y_2) \text{ iff } x_1\beta_1^* x_2, \quad y_1\beta_2^* y_2$$

for all $(x_i, y_i) \in H_1 \times H_2, \quad i = 1, 2$

3. T-FUZZY SUBHYPERGROUPS

Definition 3.1 Let $(H, \cdot)$ be a hypergroup and let μ be a fuzzy subset of H. Then μ is said to be a T-fuzzy subhypergroup of H with respect to a t-norm T, if the following axioms hold:

(i) $T(\mu(x), \mu(y)) \leq \inf_{\alpha \in x \cdot y}\{\mu(\alpha)\}, \quad \forall x, y \in H$

(ii) for all $x, a \in H$ there exists $y \in H$ such taht $x \in a \cdot y$ and

$$T(\mu(a), \mu(x)) \leq \mu(y)$$

(iii) for all $x, a \in H$ there exists $z \in H$ such that $x \in z \cdot a$ and

$$T(\mu(a), \mu(x)) \leq \mu(z)$$

(ii) is called the left fuzzy reproduction axiom and (iii) is called the right fuzzy reproduction axiom.

Definition 3.2 Let $(H, \cdot)$ be a hypergroup and let μ be a fuzzy subset of H. Then μ is said to be an anti T^*-fuzzy subhypergroup of H with respect to a t-conorm T^*, if the following axioms hold:

(i) $\sup_{\alpha \in x \cdot y}\{\mu(\alpha)\} \leq T^*(\mu(x), \mu(y)), \quad \forall x, \ y \in H,$

(ii) for all $x, a \in H$ there exists $y \in H$ such that $x \in a \cdot y$ and

$$\mu(y) \leq T^*(\mu(a), \mu(x))$$

(iii) for all $x, a \in H$ there exists $z \in H$ such that $x \in z \cdot a$ and

$$\mu(z) \leq T^*(\mu(a), \mu(x))$$

Lemma 3.3 Let T be a t-norm. If we define the following:

$$T^*(x,y) = 1 - T(1-x,\ 1-y)$$

then T^* is a t-conorm.

Proof: The proof is straightforward and omitted. □

Theorem 3.4 Let H be a hypergroup and μ be a fuzzy subset of H. Then μ is a T-fuzzy subhypergroup of H with respect to a t-norm T if and only if it's complement μ^c is an anti T^*-fuzzy subhypergroup of H with respect to t-conorm T^*, where T^* is defined in Lemma 3.3.

Proof Let μ be is a T-fuzzy subhypergroup of H with respect to t-norm T. For every x, y in H, we have $T(\mu(x),\ \mu(y)) \leq \inf_{\alpha \in x \cdot y}\{\mu(\alpha)\}$, or $T(1-\mu^c(x), 1-\mu^c(y)) \leq \inf_{\alpha\in x\cdot y}\{1-\mu^c(\alpha)\}$, or $T(1-\mu^c(x), 1-\mu^c(y)) \leq 1 - \sup_{\alpha\in x\cdot y}\{\mu^c(\alpha)\}$, or $\sup_{\alpha\in x\cdot y}\{\mu^c(\alpha)\} \leq 1 - T(1-\mu^c(x),\ 1-\mu^c(y))$, or $\sup_{\alpha\in x\cdot y}\{\mu^c(\alpha)\} \leq T^*(\mu^c(x),\ \mu^c(y))$, and in this way the condition (i) of the Definition 3.2 is verified for μ^c.

Since μ is a T-fuzzy subhypergroup of H with respect to t-norm T, so for every a, x in H, there exists $y \in H$ such that $x \in a \cdot y$ and $T(\mu(a),\ \mu(x)) \leq \mu(y)$, or $T(1-\mu^c(a),\ 1-\mu^c(x)) \leq 1-\mu^c(y)$, or $\mu^c(y) \leq 1 - T(1-\mu^c(a),\ 1-\mu^c(x))$, or $\mu^c(y) \leq T^*(\mu^c(a),\ \mu^c(x))$ and the second condition of Definition 3.2 is satisfied. Thus μ^c is an anti T^*-fuzzy subhypergroup. The converse also can be proved similarly. □

Suppose T_1 and T_2 be two t-norms. T_2 is said to dominate T_1 and write $T_1 << T_2$ if for all $a, b, c, d \in [0,1]$,

$$T_1(T_2(a,c),\ T_2(b,d)) \leq T_2(T_1(a,b),\ T_1(c,d))$$

and T_1 is said weaker than T_2 or T_2 is stronger than T_1 and write $T_1 \leq T_2$ if for all $x, y \in [0,1]$,

$$T_1(x,y) \leq T_2(x,y)$$

Definition 3.5 Let H_1, H_2 be hypergroups and μ, λ be T-fuzzy subhypergroups of H_1, H_2 under t-norm T respectively. The T-product of μ, λ is defined to be the fuzzy subset $\mu \times \lambda$ of $H_1 \times H_2$ with

$$(\mu \times \lambda)(x, y) = T(\mu(x), \lambda(y)), \quad \text{for all } (x, y) \in H_1 \times H_2$$

Proposition 3.6 Let H_1, H_2 be hypergroups and μ, λ be T-fuzzy subhypergroups of H_i under t-norms T_i, $i = 1, 2$ respectively and T' be a t-norm such that $T' \leq T_1, T_2$ and let T be a t-norm such that $T' << T$. Then T-product $\mu \times \lambda$ is a T-fuzzy subhypergroup of $H_1 \times H_2$ under t-norm T'.

Proof Let $x, y \in H_1 \times H_2$ such that $x = (x_1, x_2)$, $y = (y_1, y_2)$. For every $\alpha = (\alpha_1, \alpha_2) \in x \circ y = (x_1, x_2) \circ (y_1, y_2)$ we have

$$\begin{aligned}
(\mu \times \lambda)(\alpha) &= (\mu \times \lambda)(\alpha_1, \alpha_2) = T(\mu(\alpha_1), \lambda(\alpha_2)) \\
&\geq T(T_1(\mu(x_1), \mu(y_1)),\ T_2(\lambda(x_2), \lambda(y_2))) \\
&\geq T(T'(\mu(x_1), \mu(y_1)),\ T'(\lambda(x_2), \lambda(y_2))) \\
&\geq T'(T(\mu(x_1), \lambda(x_2)),\ T(\mu(y_1), \lambda(y_2))) \text{ Since } T >> T' \\
&\geq T'((\mu \times \lambda)(x_1, x_2),\ (\mu \times \lambda)(y_1, y_2))
\end{aligned}$$

Therefore the first condition of Definition 3.1 is satisfied. Now we prove second condition of Definition 3.1 as follows: For every (x_1, x_2) and (a_1, a_2) in $H_1 \times H_2$ there exist (y_1, y_2) in $H_1 \times H_2$ such that

$$T_1(\mu(x_1), \mu(a_1)) \leq \mu(y_1), \quad T_2(\lambda(x_2),\ \lambda(a_2)) \leq \lambda(y_2)$$

Therefore we have $(x_1, x_2) \in (a_1, a_2) \circ (y_1, y_2)$ and

$$\begin{aligned}
(\mu \times \lambda)(y_1, y_2) &= T(\mu(y_1), \lambda(y_2)) \\
&\geq T(T_1(\mu(x_1), \mu(a_1)),\ T_2(\lambda(x_2), \lambda(a_2))) \\
&\geq T(T'(\mu(x_1), \mu(a_1)),\ T'(\lambda(x_2), \lambda(a_2))) \\
&\geq T'(T(\mu(x_1), \lambda(x_2)),\ T(\mu(a_1), \lambda(a_2))) \\
&\geq T'((\mu \times \lambda)(x_1, x_2),\ (\mu \times \lambda)(a_1, a_2))
\end{aligned}$$

The proof of third condition of Definition 3.1 is similar to the proof of second condition. $\square$

Corollary 3.7 Let H_1, H_2 be hypergroups and let μ, λ be T-fuzzy subhypergroups of H_1, H_2 under t-norm T respectively. Then $\mu \times \lambda$ is a T-fuzzy H_v-subgroup of $H_1 \times H_2$ under t-norm T.

Now, let μ be a *min*-fuzzy subhypergroup of H under t-norm min. Then by Theorem 1 of [6] the set $\mu_1 = \{x \in H | \mu(x) \geq t\}$ is a subhypergroup of H. In the following result the T-product is considered for min only.

Corollary 3.8 Let μ and λ are *min*-fuzzy subhypergroups of H_1 and H_2 then

$$(\mu \times \lambda)_t = \mu_1 \times \lambda_t.$$

Definition 3.9 Let H be a hypergroup and μ be a fuzzy subset of H. The fuzzy subset μ_{β^*} on H/β^* is defined as follows:

$$\mu_{\beta^*} : H/\beta^* \longrightarrow [0,1]$$
$$\mu_{\beta^*}(\beta^*(x)) = \sup_{a \in \beta^*(x)} \{\mu(a)\}.$$

Theorem 3.10 Let T be an Archimedian t-norm and H be a hypergroup and μ be a T-fuzzy subhypergroup of H under t-norm T. Then μ_{β^*} is a T-fuzzy subgroup of H/β^* under t-norm T.

Proof The proof is similar to Theorem 5 of [7]. □

Theorem 3.11 Suppose that

(1) H_1, H_2 are hypergroups,

(2) β_1^*, β_2^* and β^* are fundamental equivalence relations on H_1, H_2 and $H_1 \times H_2$ respectively.

(3) T is an Archimedean t-norm,

(4) μ is a T-fuzzy subhypergroup of H_1 under t-norm T,

(5) λ is a T-fuzzy subhypergroup of H_2 under t-norm T.

Then we have

$$(\mu \times \lambda)_{\beta^*} = \mu_{\beta_1^*} \times \lambda_{\beta_2^*}$$

Proof By Corollary 3.7 and conditions (4), (5) we get $\mu \times \lambda$ is a T-fuzzy subhypergroup of $H_1 \times H_2$ under t-norm T, then by Theorem 3.10 we have $(\mu \times \lambda)_{\beta^*}$ is a fuzzy subgroup of the group $(H_1 \times H_2)/\beta^*$ under t-norm T.

Now, assume that $x \in H_1$ and $y \in H_2$ then

$$\begin{aligned}
(\mu \times \lambda)_{\beta^*}(\beta^*(x,y)) &= \sup_{(a,b)\in\beta^*(x,y)} \{(\mu \times \lambda)(a,b)\} \\
&= \sup_{(a,b)\in\beta^*(x,y)} \{T(\mu(a), \lambda(b)\} \\
&= \sup_{a\in\beta_1^*(x)_{b\in\beta_2^*}(y)} \{T(\mu(a),\ \lambda(b))\} \\
&= T(\sup_{a\in\beta_1^*(x)} \{\mu(a)\},\ \ \sup_{b\in\beta_2^*(y)} \{\lambda(b)\}) \\
&= T(\mu_{\beta_1^*}(\beta_1^*(x)),\ \ \lambda_{\beta_2^*}(\beta_2^*(y))) \\
&= (\mu_{\beta_1^*} \times \lambda_{\beta_2^*})(\beta_1^*(x),\ \beta_2^*(y)).\square
\end{aligned}$$

REFERENCES

[1] Akgül, M. Some properties of fuzzy groups, *J. Math. Anal. Appl.* 133 (1988) 93-100.

[2] Anthony, J. M. and Sherwood, H. Fuzzy groups redefined, *J. Math. Anal. Appl.* 69 (1979) 124-130.

[3] Anthony, J. M. and Sherwood, H. A. characterization of fuzzy subgroups, *Fuzzy Sets and Systems* 7 (1982) 297-305.

[4] Biswas, R. Fuzzy subgroups and anti fuzzy subgroups, *Fuzzy Sets and Systems* 35 (1990) 121-124.

[5] Corsini, P.: Prolegomena of hypergroup theory, Second edition, Aviani editor 1993.

[6] Das, P.S. Fuzzy groups and level subgroups, *J. Math. Anal. Appl.* 84 (1981) 264-269.

[7] Davvaz, B. Fuzzy H_v- groups, *Fuzzy Sets and Systems* 101 (1999) 191-195.

[8] Davvaz, B. On H_v - rings and fuzzy H_v-ideals, *Fuzzy Math.* 6 (1998) 33-42.

[9] Davvaz, B. On H_v - subgroups and anti fuzzy H_v-subgroups, *Korean J. Comput. & Appl. Math.* 5 (1998) 181-190.

[10] Davvaz, B. Interval valued fuzzy subhypergroups, *Korean J. Comput. & Appl. Math.* 6 (1999) 197-202.

[11] Davvaz, B. Fuzzy and anti fuzzy subhypergroups, *Proc. of International Conference on Intelligent and Congnitive Systems* FSS, 96, Sponsored by IEE and IRSF, Tehran, Iran, (1996) 140-144.

[12] Freni, D. Una nota sul coure di un ipergruppo e sulla chiu transitiva β^* di β, *Rivista Math. Pura Appl.* 8 (1991) 153-156.

[13] Marty, F. Sur une generalization de la notion de group, 8^{th} *congres Math. Scandinaves, Stockholm* (1934) 45-49.

[14] Negoita, C.V. and Ralescu, D.A.: Applications of Fuzzy sets to System, Analysis, New York-Toronto, John Wiley and Sons, 1975.

[15] Rosenfeld, A. Fuzzy groups, *J. Math. Anal.* 35, (1971) 512-517.

[16] Schweizer, B. and Sklar, A. Statistical metric space, *Pacific J. Math.* 10 (1960) 313-334.

[17] Sherwood, H. Product of fuzzy subgroups, *Fuzzy Sets and Systems* 11 (1983) 79-81.

[18] Vougiouklis, T. The fundamental relation in hyperrings. The general hyperfield, *Proceedings of the Forth International congress on Algebraic Hyperstructures and Applications* (AHA 1990), World Scientific, (1991) 203-211.

[19] Vougiouklis, T.: Hyperstructures and their representations, Florida, Hadronic Press, Inc., 1994.

[20] Zadeh, L.A. *Fuzzy sets, Inform. Control* 8 (1965) 338-353.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii (2000) pp. 17–26

ON SOME PRODUCTS OF PERMUTABILITY AND SUBNORMALITY OF SUBGROUPS

Akbar Hussani
Department of Mathematics
Iran University of Science & Technology
Narmak, Tehran 16844, Iran

Shaban Sedghi
Department of Mathematics
Ghaemshahr Islamic Azad
University Ghaemshahr
Mazandaran, Iran

(Received 5 June, 1998)

ABSTRACT A subgroup H of a group G is called a quasi-normal subgruop of G, if $HK = KH$ for all subgroups K of G. We will show that if H is a quasi-normal subgroup of a group G such that $[G : H]$ is a prime, or $[G : H] = 2^a m$, where $a = 1, 2, m$ is an odd and square free number, then H is a normal subgroup of G. However for an odd prime p and $n \geq 3$ or for $p = 2$ and $n \geq 4$ let G be the group of order p^n with generators a and b and $a^{p^{n-1}} = 1$, $b^p = 1$, and $ba = a^{1+p^{n-2}}b$. Let $H =< b >$. Then $[G : H] = p^{n-1}$ and H is a quasi-normal in G but not normal in G.

AMS subject classification Number: 20D35

1. INTRODUCTION If G is a group and if A, B are subgroup of G, the subgroup $< A, B >$ of G generated by $A \cup B$ is of interest. To be able to control the properties of the group $< A, B >$ by those of A and B, the generation of $< A, B >$ must happen in a special way. The most transparent case we have is when $< A, B >$ coincides with the product set $AB = \{ab | a \in A, b \in B\}$. It is well known that this holds if and only if $AB = BA$. Two subgroups A and B of a group G which have this property, are called permutable. A sufficient condition for the permutability of A and B is that A normalizes B (that is, $a^{-1}ba \in B$ for all $a \in A, b \in B$) or vice versa. Particularly, if A is a normal subgroup of G, we have $AB = BA = < A, B >$ for every subgroup B of G.

In 1939, [4, 13.2.1] Ore introduced the concept of a quasi-normal subgroup of a group, a generalization of a normal subgroup.

Definition 1.1 A subgroup H of a group G is called a quasi-normal subgroup of G, if $HK = KH$ for all subgroups K of G.

Remark 1.2 If H is a subgroup of G, then the following conditions are equivalent.

(i) H is quasi-normal in G.

(ii) For every $g \in G$ and $h \in H$, there exist $r \in \mathbb{Z}$ and $h' \in H$ such that $hg = g^r h'$.

We note that $G = < x, y | x^8 = y^2 = 1, \quad y^{-1}xy = x^5 >$ is an example of a group having a quasi-normal subgroup which is not normal. Q_8 is an example of group having a quasi-normal subgroup which is normal but D_8 is an example of a group which has a subgroup of index 4 which is not quasi-normal.

Next lemma shows the relation between quasi-normal subgroups and factor groups of normal subgroup contained in such subgroups.

Lemma 1.3 If G is a group and $N \subset H \subset G$ are subgroups with N normal in G, then H is quasi-normal in G if and only if $\frac{H}{N}$ is quasi-normal in $\frac{G}{N}$.

Proof It follows from definition immediately. □

Of course every normal subgroup is quasi-normal, which might lead one to hope that subnormal subgroups also have this property. However the converse it is not necessarily true.

One may adopt the opposite point of view, asking whether quasi-normal subgroups are subnormal.

Ore in [4, 13 · 2 · 2] shows that if H is a quasi-normal subgroup of a finite group G, then H is subnormal. While in general a quasi-normal subgroup of an infinite group need not be subnormal.

Finally, Stonehewer in [3] shows that, a quasi-normal subgroup of a finitely generated group G is subnormal.

In 1962, Ito and Szep [6] obtained an interesting result which showed that the difference between normality and quasi-normality in general is small.

Also if H is a quasi-normal subgroup of G, then the quotient group $\frac{H}{H_G}$ is nilpotent, that is, $\frac{H}{H_G}$ is contained in the Fitting subgroup $F\left(\frac{G}{H_G}\right)$ of $\frac{G}{H_G}$. Here H_G denotes the intersection of all conjugates $H^g = g^{-1}H_g$ of H with $g \in G$.

2. NORMALITY OF QUASI-NORMAL SUBGROUPS

Next theorems shows the condition when quasi-normality implies normality.

Theorem 2.1 Let H be a quasi-normal subgroup of a group G such that $[G : H]$ is a prime then H is a normal subgroup of G.

Proof Suppose that this is false, then there is a conjugate $H' = g^{-1}Hg$ of H such that $H' \neq H$. Let $K = HH' = H'H$. Since $[G : H]$ is prime and $H \subset K \subset G$, $K = G$. In particular $g = hh'$ for some $h \in H$, $h' \in H'$. Hence $g = hg^{-1}h_1g$ for some $h, h_1 \in H$. However this implies that $g \in H$ so $H' = H$ contradicting the assumption. This complete the proof. □

We know that if index H in G is equal to 2, then H is normal in G. We show in next theorem that a quasi-normal subgroup H of G such that $[G : H] = 4$ is a normal subgroup of G

Theorem 2.2 A quasi-normal subgroup H of group G such that $[G : H] = 4$ is a normal subgroup of G.

Proof Suppose that this is false, then there is a conjugate $H' = g^{-1}Hg$ of H

such that $H' \neq H$. Let $K = HH' = H'H$. Since $H \subset K \subset G$ and $[G : H] = 4$ it follows that K is H or G or else $[K : H] = 2$. If $K = H$ then $H' \subseteq K = H$ so $H' = H$ a contradiction. If $K = G$ then as in the proof of theorem 2.1, H is normal in G. Thus $[K : H] = 2$, and H is normal in K, also $[G : K] = 2$, and K is normal in G.

We conclude that there are exactly two conjugate of H, namely H and H'. Let $N = H \cap H'$. By definition N is core of H in G and therefore is a normal subgroup of G. Moreover

$$[K : H] = [HH' : H] = [H' : N] = [H : N] = 2$$

Since $N \subset H \subset G$, $[G : H] = 4$, $[H : N] = 2$ and N is normal in G the group $\frac{G}{N}$ has order 8, $\frac{H}{N}$ is quasi-normal in $\frac{G}{N}$ and has index 4. We know that every quasi-normal subgroup of a group G of order 8, is normal in G. Thus $\frac{H}{N}$ is normal in $\frac{G}{N}$ so H is normal in G, contradicting the initial assumption. From this it follows that H is normal in G. □

In general we show that;

Theorem 2.3 If H is a quasi-normal subgroup of a group G and $[G : H] = 2^a m$, where $a = 1, 2$, m is an odd and square free number, then H is a normal subgroup of G.

Proof We will argue by induction on $n = 2^a m$. If $n = 1$, the result is obvious. For $n = 2^a$, where $a = 1, 2$ it follows from Theorems 2.1 and 2.2. Consider any element $g \in G$. Since H is quasi-normal in $G, H < g >$ is a subgroup of G and H is quasi-normal in $H < g >$. If $H < g > \neq G$, then by the induction hypothesis, H is normal in $H < g >$, so $Hg = gH$.

If $H(g) = G$, then $[H < g >: H] = n$. This implies that n is the least positive integer k such that $g^k \in H$. Let $x = g^p$ and $y = g^{m_1}$, where p is a prime $(p \neq 2)$ and does not divide m_1 $\left(m_1 = \frac{n}{p}\right)$. Then the least positive integer k such that $x^k \in H$ is $\frac{n}{p} = m_1$, so $[H < x >: H] = m_1$ similarly $[H(y) : H] = p$.

Since H is quasi-normal in both $H < x >$ and $H < y >$, the inductive hypothesis shows that $Hx = xH$ and $Hy = yH$. The fact that $(p, m_1) = 1$ implies that $g \in < x, y >$, hence $Hg = gH$. □

Lemma 2.4 Let H be a quasi-normal subgroup of a finite group G. If $(n, |G|) = 1$, then H is quasi-normal in the group $G \times \mathbb{Z}_n$ where $\mathbb{Z}_n$ denotes the cyclic group of order n.

Proof Let $k \in G \times \mathbb{Z}_n$ and $h \in H$. We will show that $hk = k^{r'}h'$ for some integer r' and $h' \in H$. We have $k = (g, a^s)$ for some $g \in G$ and integer s, where $< a >= \mathbb{Z}_n$. Since H is quasi-normal in G, $hg = g^r h'$ for some integer r and $h' \in H$: Because $(n, |G|) = 1$, there is an integer r' such that $r' \equiv r \pmod{|G|}$ and $r' \equiv 1 \pmod{n}$. Hence

$$\begin{aligned} hk &= (h,1)(g,a^s) = (hg,a^s) = (g^r h', a^s) = (g^{r'}h', a^s) \\ &= (g^{r'}, a^s)(h',1) = (g^{r'}, a^{r's})(h',1) = (g,a^s)^{r'}(h',1) = k^{r'}h' \end{aligned}$$

and H is quasi-normal in $G \times \mathbb{Z}_n$. $\square$

3. SOME QUASI-NORMAL SUBGROUPS WHICH ARE NOT NORMAL For any positive integer m that is divisible by 8 or the square of an odd prime, we will exhibit a finite group G and a quasi-normal subgroup H such that $[G : H] = m$ and H is not normal in G.

Given a group G and $a, b \in G$, let $[a, b]$ denote $a^{-1}b^{-1}ab$, the commutator of a and b. Then we have [5, Lemma 2.2]

(i) If $[a, b]$ commutes with a, then $[a^n, b] = [a, b]^n$ for any $n \in \mathbb{Z}$.

(ii) If $[a, b]$ commutes with a and b, then for any integer $n \geq 0$

$$(ab)^n = a^n b^n [b, a]^{\binom{n}{2}}$$

Lemma 3.1 For an odd prime p and $n \geq 3$ or for $p = 2$ and $n \geq 4$ let G be the group of order p^n with generators a and b and $a^{p^{n-1}} = 1$, $b^p = 1$ and $ba = a^{1+p^{n-2}}b$. Let $H =< b >$. Then $[G : H] = p^{n-1}$ and H is quasi-normal in G but not normal in G.

Proof Every element in G has a unique representation in the form $a^i b^j$ with

$0 \leq i < p^{n-1}$, $0 \leq j < p$. Since $a^{-1}ba = a^{p^{n-2}}b \notin H$, H is not normal in G. To prove that H is quasi-normal in G, we first note the following.

Since
$$ba^pb^{-1} = (bab^{-1})^p = (a^{1+p^{n-2}})^p = a^{p+p^{n-1}} = a^p$$

we have $a^p \in Z(G)$ and $a^{p^{n-2}} \in Z(G)$. Since
$$[b,a] = b^{-1}(a^{-1}ba) = b^{-1}a^{p^{n-2}}b = a^{p^{n-2}}$$

We have $[b,a]$, $[a,b] \in Z(G)$. So for any $i,j \in Z, [b^j, a^i] = [b,a]^{ij} \in Z(G)$ by (i) and similarly $[a^i, b^j] \in Z(G)$. Also
$$[b,a] = (a^{p^{n-2}})^p = a^{p^{n-1}} = 1$$

Let $g \in G$ and $h \in H$. Then $g = a^ib^j$ and $h = b^k$ for some $i,j,k \geq 0$. Let $r = 1 + p^{n-2}k$. By Remark 1.2, it suffices to show that $hg = g^rh$. By (ii)
$$g^r = (a^ib^j)^r = a^{ir}b^{jr}[b^j, a^i]^{\binom{r}{2}}$$

Note that
$$a^{ir} = a^i(a^{p^{n-2}})^{ik} = a^i[b,a]^{ik} = a^i[b^k, a^i]$$
and that
$$b^{jr} = b^{j+p^{n-2}jk} = b^j$$

Also the restrictions on p and n imply that p divides $\binom{r}{2}$ and $[b^j, a^i]^{\binom{r}{2}} = [b,a]^{ij\binom{r}{2}} = 1$, since $[b,a]^p = 1$. Thus, $g^r = a^i[b^k, a^i]b^j$. Consequently,

$$\begin{aligned} g^rh &= g^rb^k = a^i[b^k, a^i]b^{j+k} = a^ib^k[b^k, a^i]b^j \\ &= a^ib^k(b^{-k}a^{-i}b^ka^i)b^j = b^ka^ib^j = hg \end{aligned}$$

4. ON SOME PRODUCTS OF CONJUGATE-PERMUTABLE SUBGROUP: In the proof that a quasi-normal subgroup is subnormal [4]. One only needs to show that it is permutable with all of its conjugates. This leads to a new concept concerning subgroups.

Definition 4.1 A subgroup H of a group G is called a conjugate- permutable subgroup of $G(H <_{c-p} G)$, if $HH^g = H^gH$ for all $g \in G$.

In this section we prove that conjugate-permutable subgroups are subnormal, and we prove some elementary properties of conjugate-permutable subgroups. We also give example of subnormal subgroups that are not conjugate-permutable subgroups, and of conjugate- permutable subgroups that are not quasi-normal.

Of course every quasi-normal subgroup is a conjuage-permutable subgroup, however the converse it is not necessarily true.

Example 4.1 We note that $H =< yx >$ is a conjugate-permutable subgroup of $D_8 =< x, y | x^4 = y^2 = 1,\ y^{-1}xy = x^{-1} >$, but H is not a quasi-normal subgroup of D_8.

As in the proof of theorem 2.1, it is easy to see that if H is a conjugate-permutable subgroup of a group G such that $[G : H]$ is a prime then H is a normal subgroup of G. Also if H is a maximal conjugate-permutable subgroup of G, then H is a normal subgroup of G.

Corollary 4.1 If $H <_{c-p} G$ and G is finite group, then H is subnormal.

Example 4.2 Let $D_{16} =< x, y | x^8 = y^2 = 1,\ y^{-1}xy = x^{-1} >$, $H =< y >$, and $K =< yx^6 >$. Then H is subnormal in D_{16} (since D_{16} is nilpotent), but

$$HK = \{1, yx^6,\ y, x^6\} \neq \{1, yx^6, y, x^2\} = KH$$

So H is not a conjugate-permutable group.

Corollary 4.2 If G is a finite group with all maximal subgroups conjugate-permutable, then G is nilpotent.

Foguel in [1] proved the following theorem: If G is a finite group and there exist $H <_{c-p} G$ such that H is a maximum subgroup of a $P \in Syl_2(G)$, then G is solvable.

Huppert [5, Satz 10.3,p.724] proved the following theorem: If a finite group is the product of pairwise permutable cyclic subgroups then it is supersolvable. Of course the converse of this statement is not even true in the class of nilpotent groups.

Assume G be a finite group. $\pi(G)$ denotes the set of prime divisors of the order of the group G.

Lemma 4.3 Let P be a normal p-subgroup of G, Q a Sylow q-subgroup of $G, p \neq q, H$ a subgroup of P such that $HQ = QH$. Then H is normalized by Q.

Proof It is obvious.

Theorem 4.4 Let H be an abelian normal subgroup of a group G such that $G' \leq H$ and the Sylow subgroups of H are elementary abelian. Assume that for every $q \in \pi(H)$ the Sylow q-subgroup Q of H can be written as $Q = Q_1 \cdots Q_s$ where Q_1 is a cyclic and permutable with Sylow p-subgroup of G for all $p \in \pi(G)$ and $1 \leq i \leq S$. Then G is supersolvable.

Proof We prove the claim by induction on the order of H. We show that Q contains a normal subgroup of order q of G. Let Q^* be a Sylow q-subgroup of G, then $Q \leq Q^*$. Let $1 = B_0 \triangleleft B_1 \triangleleft \cdots \triangleleft B_r = Q$ such that $B_i \triangleleft Q^*$ and $\frac{B_i}{B_{i-1}}$ is of order q for all i. Let $1 \leq t \leq r$ minimal such that B_t contains a subgroup A of G such that A is permutable with Sylow p-subgroup of G for all $p \in \pi(G)$. If A is normal in Q^*, then by Lemma 4.3 it is normal in G, too. Assume A is not normal in Q^*, then there is an element b of $Q*$ such that $A^b \neq A$. Clearly b fixes every element of $\frac{B_t}{B_{t-1}}$ by conjugation. Let $A =< a >$, $A^b =< a_1 >$ with $aa_1^{-1} \in B_{t-1}$. Let P be a Sylow p-subgroup $(p \neq q)$ such that $PA = AP$, Then by Lemma 4.3 P normalizes A. Let $x \in P$ then $a^x = a^t$ for some integer t. Then $(a^b)^{x^b} = (a^b)^t$ follows. As $G' \leq H$ and $a, a^b \in H$ we obtain that $(a_1^b)^t = (a_1^b)^{x^b} = (a_1^b)^{x[x,b]} = (a_1^b)^x$, hence every element of P acts as raising to some power t on $< a, a_1^b >$. Now it follows that $< aa_1^{-1} >$ is permutable with Sylow p-subgroup of G for all $p \in \pi(G)$ and $< aa_1^{-1} >$ contained in B_{t-1}, a contradiction. Thus A is normal in H. It is easy to see that $\frac{G}{A}$ satisfies the conditions of our Theorem, consequently $\frac{G}{A}$ is supersolvable, which implies the supersolvability of G. $\square$

REFERENCES

[1] Foguel, T., *Conjugate-Permutable*, J. Algebra 191 (1997), 235-239.

[2] Huppert, B., *Endlichen Gruppen I* Springer-Verlag, New York, 1967.

[3] Stonehewer, S.E., *Permutable subgroups of infinite groups*, Math. Z. 125 (1972), 1-16.

[4] Robinson, D.J.S., *A Course in the Theory of Groups*, 2nd ed. Springer-Verlag, New York 1996.

[5] Daniel Gorenstein. Finite Groups, *Harper's Series in Modern Mathematics*, Harper & Row, New York 1968.

[6] Ito, N & Szep J, *Uber die Quasinormalteiler von endlicher Gruppen*, Acta Sci. Math 23 (1962), 168-170.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii (2000) pp. 27–36

FIXED POINT THEOREMS IN COMPLETE AND COMPACT METRIC SPACES

Guo-Jing Jiang
Dalian Management Cadre's College,
Dalian,Liaoning 116033
People's Republic of China
(Received 14 June, 1999)

ABSTRACT Two fixed point theorems in complete and compact metric spaces are established. A result of Hardy and Rogers is obtained as a particular case of our result under relaxed conditions.

Key words and phrases: Fixed point, complete metric space, compact metric space, Zorn's lemma.

1991 **AMS subject classification.** 54H25

INTRODUCTION Goebel, Kirk and Shimi [1] proved the following theorem.

Theorem. Let X be a uniformly convex Banach space, C a nonempty bounded, closed and convex subset of X and $f : C \to C$ a continuous map such that

$$\|fx - fy\| \leq a\|x - y\| + b[\|x - fx\| + \|y - fy\|] + c[\|x - fy\| + \|y - fx\|]$$

for all $x, y \in C$ where $a, b, c \geq 0$ and $a + 2b + 2c \leq 1$. Then f has a fixed point in C.

The purpose of this paper is to establish the existence of fixed points for the above maps in metric spaces. If the continuity of f in the above theorem is replaced by $b > 0$ and $c > 0$, then we may establish a fixed point theorem in complete metric spaces which extends Theorem 1 of Hardy and Rogers [2]. Imitating Kannan and Kirk's methods, we obtain also a fixed point theorem in compact metric spaces.

Let f be a self map of a metric space (X, d). For $E \subset X, \bar{E}$ and $\delta(E)$ denote the closure and diameter of E respectively. Define

$$\begin{aligned} \mathcal{F} &=. \{E|E \text{ in nonempty closed and } f\text{ --invariant subset of } X\} \\ \mathcal{F} &= \{E|E \in \mathcal{F} \text{ and } \delta(\mathcal{E}) > \prime\} \end{aligned}$$

N and ω denote the sets of positive integers and nonnegative integers respectively.

2. FIXED POINT THEOREMS

Our main result is as follows.

Theorem 1 Let f be a self map of a complete metric space (X, d) satisfying

$$\begin{aligned} &(1) \quad d(fx, fy) \leq ad(x, y) + b[d(x, fx) + d(y, fy)] \\ &\qquad + c[d(x, fy) + d(y, fx)] \quad \text{for} \quad x, y \in X; \\ &(2) \quad a, b \text{ and } c \text{ are nonnegative and } a + 2b + 2c = 1. \end{aligned}$$

If $b > 0$ and $c > 0$, then f has a unique fixed point w in X and $\lim_{n\to\infty} f^n x = w$ for each $x \in X$.

The following lemmas will be helpful in proving Theorem 1.

Lemma 1 Let f be a self map of a metric space (X, d) satisfying (1) and (2). Then

(i) $d(f_x^n x,\ f^{n+1}x) \leq d(f^{n-1}x,\ f^n x)$

for $x \in X$ and $n \in N$;

(ii) $d(f^n x, f^{n+1}x) \leq d(x, fx) + c^k[d(f^{n-k}x, f^{n+1}x) - (1+k)d(x, fx)]$

for $x \in X$ and $n, k \in \omega$ with $0 \leq k \leq n$.

Proof By (1), (2) and the triangle inequality we have

$$\begin{aligned} d(f^n x, f^{n+1}x) &\leq (a+b)d(f^{n-1}x, f^n x) + bd(f^n x, f^{n+1}x) \\ &\quad + cd(f^{n-1}x, f^{n+1}x) \\ &\leq (a+b+c)d(f^{n-1}x, f^n x) + (b+c)d(f^n x, f^{n+1}x) \\ &= (1-b-c)d(f^{n-1}x, f^n x) + (b+c)d(f^n x, f^{n+1}x) \end{aligned}$$

which implies (i) holds.

For $r, s \in \omega$ and $r > s$ we have by the triangle inequality and (i)

(3) $d(f^r x, f^s x) \leq \sum_{i=s}^{r-1} d(f^i x, f^{i+1}x) \leq (r-s)d(x, fx)$

Take $n \in \omega$. Clearly (ii) holds for $k = 0$. Suppose that (ii) holds for $k = m < n$; i.e.

(4) $d(f^n x, f_x^{n+1}) \leq d(x, fx) + c^m[d(f^{n-m}x, f^{n+1}x) - (1+m)d(x, fx)]$

Using (1), (2) and (3) we obtain

$$\begin{aligned} d(f_x^{n-m}, f_x^{n+1}) &\leq ad(f^{n-m-1}x, f^n x) + b[d(f^{n-m-1}x, f^{n-m}x) \\ &\quad + d(f^n x, f^{n+1}x)] + c[d(f^{n-m-1}x, f^{n+1}x) \\ &\quad + d(f^n x, f^{n-m}x)] \\ &\leq a(1+m)d(x, fx) + 2bd(x, fx) \\ &\quad + c[d(f^{n-m-1}x, f^{n+1}x) + md(x, fx)] \\ &\leq (a+2b+2c)(1+m)d(x, fx) + c[d(f^{n-m-1}x, \\ &\quad f^{n+1}x) - (2+m)d(x, fx)] \\ &= (1+m)d(x, fx) + c[d(f^{n-m-1}x, f_x^{n+1} \\ &\quad -(2+m)d(x, fx)] \end{aligned}$$

From (4) and the above inequalities we get

$$d(f^n x, f_x^{n+1}) \leq d(x, fx) + c^{m+1}[d(f^{n-m-1}x, f^{n+1}x) - (2+m)d(x, fx)]$$

Hence (ii) holds for $k = m+1$. By induction (ii) is true for $0 \leq k \leq n$. This completes the proof.

Lemma 2 Let f be a self map of a complete metric space (X, d) satisfying (1), (2) and $b > 0$. Assume $\{x_n\}_{n\in N} \subset X$, $D \subset X$ and $h(x) = d(x, fx)$ for $x \in X$. Then

(iii) f has at most a fixed point;

(iv) $\{x_n\}_{n\in N}$ is convergent provided that $\lim_{n\to\infty} d(x_n, fx_n) = 0$;

(v) D is bounded if $h(D)$ is bounded.

Proof We first show that (iii) holds. Suppose x and y are fixed points of f and $x \neq y$. By (1), (2) and $b > 0$ we have

$$d(x,y) = d(fx, fy) \leq (a+2c)d(x,y) = (1-2b)d(x,y) < d(x,y)$$

which is a contradiction. Hence (iii) holds.

We now show that (iv) holds. It suffices to prove $\{x_n\}_{n\in N}$ is a Cauchy sequence. Let $n, m \in N$. By (1), (2) and $b > 0$ and the triangle inequality we get

$$\begin{aligned} d(fx_n, fx_m) \leq ad(x_n, x_m) &+ b[d(x_n, fx_n) + d(x_m, fx_m)] \\ &+ c[d(x_n, fx_n) + d(fx_n, fx_m) \\ &\quad + d(x_m, fx_m) + d(fx_m, fx_n)] \end{aligned}$$

which implies

$$d(fx_n, fx_m) \leq \frac{a}{1-2c} d(x_n, x_m) + \frac{b+c}{1-2c}[d(x_n, fx_n) + d(x_m, fx_m)]$$

Consequently

$$\begin{aligned} d(x_n, x_m) &\leq d(x_n, fx_n) + d(fx_n, fx_m) + d(fx_m, x_m) \\ &\leq \frac{a}{1-2c} d(x_n, x_m) + \frac{1+b-c}{1-2c}[d(x_n, fx_n) + d(x_m, fx_m)] \end{aligned}$$

which implies

$$d(x_n, x_m) \leq \frac{1+b-c}{1-a-2c}[d(x_n, fx_n) + d(x_m, fx_m)]$$

Since $\lim_{n\to\infty}(x_n, fx_n) = 0$, $\{x_n\}_{n\in N}$ is a Cauchy sequence by the above inequality. Hence (iv) holds.

We next show that (v) holds. Suppose that $h(D)$ is bounded. Then there exists $M > 0$ such that $h(x) \leq M$ for all $x \in D$. Take $u \in D$. For each $x \in D$, we obtain by the triangle inequality and (1), (2)

$$\begin{aligned} d(x,u) &\leq h(x) + h(u) + d(fx, fu) \\ &\leq 2M + ad(x,u) + b[h(x) + h(u)] + c[d(x,u) + \\ &\quad h(u) + d(u,x) + h(x)] \end{aligned}$$

which implies

$$d(x,u) \leq \frac{2M(1+b+c)}{1-a-2c} = \frac{1}{b}M(1+b+c)$$

Hence

$$\delta(D) = \sup\{d(x,y) | x, y \in D\} \leq \frac{2}{b}M(1+b+c)$$

i.e., D is bounded. Hence (v) holds. This completes the proof.

Proof of Theorem 1 Let $x \in X$ and $r_n = d(f^{n-1}x, f^n x)$ for $n \in N$. It follows from (i) of Lemma 1 that the sequence $\{r_n\}_{n\in N}$ is monotonically decreasing and bounded and so convergent. Put $\lim_{n\to\infty} r_n = r$. By (v) of Lemma 2, $\{f^n x\}_{n\in\omega}$ is bounded. Consequently there exists $M > 0$ such that $d(f^p x, f^q x) \leq M$ for all $p, q \in \omega$. We claim that $r = 0$. If not, then there is $m \in N$ such that $(m+1)r > M$. Note that $0 < c < 1$. Take $\epsilon = \frac{1}{2}c^m[(m+1)r - M] > 0$. Since $\lim_{n\to\infty} r_n = r$, there exists $k \in N$ such that $0 \leq r_n - r < \epsilon$ for $n \geq k$. By (ii) of Lemma 1, we obtain

$$\begin{aligned} d(f^{m+k-1}x, f^{m+k}x) &= d(f^m f^{k-1}x, f^{m+1}f^{k-1}x) \\ &\leq d(f^{k-1}x, f^k x) + c^m[d(f^{k-1}x, f^{m+k}x) \\ &\quad - (1+m)d(f^{k-1}x, f^k x)] \\ &\leq r_k + c^m[M - (1+m)r_k] < r + \epsilon \\ &\quad + c^m[M - (1+m)r] < r \end{aligned}$$

which implies $r \le r_{m+k} < r$, which is impossible and hence $r = 0$. It follows from (iv) of Lemma 2 that $\{f^n x\}_{n\in N}$ converges to some point w in X.

We next prove that w is a fixed point of f. Using (1) we have

$$\begin{aligned} d(w, fw) &\le d(w, f^n x) + d(f^n x, fw) \\ &\le d(w, f^n x) + a d(f^{n-1}x, w) \\ &\quad + b[d(f^{n-1}x, f^n x) + d(w, fw)] \\ &\quad + c[d(w, f^n x) + d(f^{n-1}x, fw)] \end{aligned}$$

As $n \to \infty$, we obtain

$$d(w, fw) \le (b + c) d(w, fw) \le \frac{1}{2} d(w, fw)$$

which implies $w = fw$ i.e., w is a fixed point of f. It follows from (iii) of Lemma 2 that w is the only fixed point of f. This completes the proof.

Remark 1 Our Theorem 1 extends Theorem 1 of Hardy and Rogers [2].

The following results are inspired by Theorem A of Kannan [3] and Theorem of Kirk [1].

Theorem 2 Let f be a self map of a compact metric space (X, d) satisfying (1), (2) and $b = 0$. Assume for each $E \in \mathcal{F}$, there exist $x, y \in E$ such that

(5) $\lim_{n\to\infty} \sup d(y, f^n x) < \delta(E)$

Then f has a fixed point.

Proof Order $\mathcal{F}$ by set inclusion. Clearly $X \in \mathcal{F} \ne \phi$. By the compactness of X, we can apply Zorn's lemma to show the existence of a minimal element E in $\mathcal{F}$. Obviously $\overline{fE} \subset E$. This implies $f\overline{fE} \subset fE \subset \overline{fE}$. Hence $\overline{fE} \in \mathcal{F}$. By minimality of E, we obtain $\overline{fE} = E$. We assert that E is a singleton. Otherwise $\delta(E) > 0$. Then $E \in \mathcal{F}$. It follows from (5) that there exist $x_0, y_0 \in E$ such that $r = \lim_{n\to\infty} \sup d(y_0, f^n x_0) < \delta(E)$. Set

$$F = \{y | y \in E \quad \text{and} \quad \lim_{n\to\infty} \sup d(y, f^n x_0) \le r\}$$

We now prove that $F = E$.Clearly $y_0 \in F \neq \phi$. Let $\{y_k\}_{k\in N} \subset F$ and $\lim_{n\to\infty} y_k = y$. For $k \in N$ we have

$$d(y, f^n x_0) \leq d(y, y_k) + d(y_k, f^n x_0)$$

we implies

$$\lim_{n\to\infty} \sup d(y, f^n x_0) \leq d(y, y_k) + \lim_{n\to\infty} \sup d(y_k, f^n x_0) \leq d(y, y_k) + r$$

Let k tend to infinity. Then $\lim_{n\to\infty} \sup d(y, f^n x_0) \leq r$. Consequently $y \in F$; i.e. F is closed. For $y \in F$, by (1) we have

$$d(fy, f^n x_0) \leq ad(y, f^{n-1} x_0) + c[d(y, f^n x_0) + d(fy, f^{n-1} x_0)]$$

which implies

$$\begin{aligned}
\lim_{n\to\infty} \sup d(fy, f^n x_0) &\leq a \lim_{n\to\infty} \sup d(y, f^{n-1} x_0) \\
&+ c[\lim_{n\to\infty} \sup d(y, f^n x_0) + \\
&\lim_{n\to\infty} \sup d(fy, f^{n-1} x_0)] \\
&= (a + c) \lim_{n\to\infty} \sup d(y, f^n x_0) + \\
&c \lim_{n\to\infty} \sup d(fy, f^n x_0) \\
&= (1 - c)r + c \lim_{n\to\infty} \sup d(fy, f^n x_0)
\end{aligned}$$

i.e. $\lim_{n\to\infty} \sup d(fy, f^n x_0) \leq r$. Hence $fy \in F$ and $f \in \mathcal{F}$. Thus the minimality of E yields $F = E$. Set

$$G = \{u | u \in E \text{ and } \sup\{d(u, y) | y \in E\} \leq r\}$$

We next prove that $G = E$. Since X is a compact metric space, $\{f^n x_0\}_{n\in N}$ has a convergent subsequence $\{f^{n_k}, x_0\}_{k\in N}$. Let $\lim_{k\to\infty} f^{n_k},\ x_0 = v$. Then $v \in E$. For any $y \in E$, we have

$$d(y, v) = \lim_{k\to\infty} d(y, f^{n_k} x_0) \leq \lim_{n\to\infty} \sup d(y, f^n x_0) \leq r$$

which implies $v \in G \neq \phi$. Let $\{u_n\}_{n\in N} \subset G$ and $\lim_{n\to\infty} u_n = u$. Then for any $y \in E$ we get

$$d(u, y) \leq d(u, u_n) + d(u_n, y) \leq d(u, u_n) + r$$

As $n \to \infty$, we have $d(u, y) \leq r$ and hence $u \in G$; i.e. G is closed. For $y \in E = \overline{fE}$, there exists a sequence $\{y_n\}_{n \in N} \subset E$ such that $\lim_{n\to\infty} d(y, fy_n) = 0$. Let $u \in G$. Using (1) we get

$$\begin{aligned} d(y, fu) &\leq d(y, fy_n) + d(fy_n, fu) \\ &\leq d(y, fy_n) + ad(y_n, u) + c[d(y_n, fu) + d(u, fy_n)] \\ &\leq d(y, fy_n) + (a + c)r + c \sup\{d(y, fu) | y \in E\} \end{aligned}$$

It is easy to show that

$$\sup\{d(y, fu) | y \in E\} \leq \frac{a + c}{1 - c} r = r$$

Hence $fu \in G$ and $fG \subset G$. Consequently $G \in \mathcal{F}$. By the minimality of E, we have $G = E$. It follows that

$$\delta(G) \leq r = \lim_{n\to\infty} \sup d(y_0, f^n x_0) < \delta(E) = \delta(G)$$

which is impossible. Hence E contains only a point, which is a fixed point of f. This completes the proof.

Corollary Let f be a self map of a compact metric space (X, d) satisfying (1), (2) and $b = 0$. Assume for each $E \in \mathcal{F}$, there exists $y \in E$ such that

(6) $\sup\{d(y, x) | x \in E\} < \delta(E)$

Then f has a fixed point.

Proof Note that (6) implies (5). Corollary follows from Theorem 2.

REFERENCES

[1] K. Goebel, W. A. Kirk and T. N. SHimi, *A fixed point theorem in uniformly convex spaces*, Boll. Un. Mat. Ital. 7(1973), 65-75.

[2] G.E. Hardy and T.D. Rogers, *A generalization of a fixed point theorem of Reich*, Canad. Math, Bull. 16(1973), 201-206.

[3] R. Kannan, *Construction of fixed points of a class of nonlinear mappings*, J. Math. Anal. Appl. 41(1973), 430-438.

[4] W.A. Kirk, *A fixed point theorem for mappings which do not increase distances*, Amer. Math. Monthly 72(1965), 1004-1006.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii (2000) pp. 37–50

THE ORBITS OF $Q^*(\sqrt{P})$, $p=2$ or $p \equiv 1 \pmod 4$ UNDER THE ACTION OF THE MODULAR GROUP

M. Aslam Malik
Government College
Sahiwal

S.M. Husnine
Department of Mathematics
University of the Punjab
Lahore

Abdul Majeed
Department of Mathematics
University of the Punjab
Lahore

(Received 20 May, 1999)

ABSTRACT: In this paper we determine the number of orbits of $Q^*(\sqrt{P}), p$ a rational prime, under the action of the modular group $G = < x, y : x^2 = y^3 = 1 >$ in the cases $p = 2$ and $p \equiv 1 \pmod 4$

1. INTRODUCTION: For any two rational integers a and b, (a, b) denotes the greatest common divisor of a and b.

For any non square positive rational integer n, let $Q^*(\sqrt{n}) = \left\{ \frac{a+\sqrt{n}}{c}\ a, \right.$

$c \in Z, \frac{(a^2-n)}{c}$ a rational integer and $\left(a, \frac{a^2-n}{c}, c\right) = 1\}$.

For $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$; its conjugate $\bar{\alpha} == \frac{a-\sqrt{n}}{c}$ may or may not have the same sign. If α and $\bar{\alpha}$ have different signs, then α is called an ambiguous number [4].

If $\alpha = \frac{a+\sqrt{n}}{c}$, then $N(\alpha) = \alpha\bar{\alpha} = \frac{a^2-n}{c^2}$ is called the norm of α. An $\alpha \in Q^*(\sqrt{n})$ is an ambiguous number if $N(\alpha) = -1$

In such a case $n = a^2 + c^2$

A coset diagram is just a graphical representation of a permutation action of a finitely generated group.

In this paper we study the coset diagrams of the modular group $G =< x, y : x^2 = y^3 = 1 >$ under its action on $Q^*(\sqrt{n})$. Thus in our case the diagram consists of a set of small triangles representing the action of $C_3 =< y : y^3 = 1 >$ and a set of edges representing the action of $C_2 =< x x^2 = 1 >$.

They are called coset diagrams because the vertices of the triangles can be identified with cosets of some subgroup of the group.

In our diagram where there are only two generators, namely x and y. In the case of y, which has order 3, there is a need to distinguish y from y^{-1}. The 3-cycles of y are therefore represented by small triangles, with the convention that y permutes their vertices counter-clockwise, while the fixed points of y are denoted by heavy dots.

Also to make the diagram slightly less complicated, we omit the loops corresponding to fixed points x, because then the geometry of the figure makes the distinction between x-edges and y -edges obvious.

Let $C' = CU(\infty)$ be the extended complex field. Mushtaq [4] has proved that $Q^*(\sqrt{n})$ is invariant under the action of $G =< x, y : x^2 = y^3 = 1 >$ where $x : C' \to C'$ and $y : C' \to C'$ are the Mobius transformations defined by:

$$x(z) = \frac{-1}{z}, \ y(z) = \frac{z-1}{z}$$

He has also shown that $Q^*(\sqrt{n})$ contains only a finite number of ambiguous numbers and those occurring in a particular orbit of $Q^*(\sqrt{n})$ form a unique closed path in the coset diagram under the action of G on $Q^*(\sqrt{n})$.

The actual number of ambiguous numbers in $Q^*(\sqrt{n})$ has been determined in [2] as a function of n.

In [3], the integers, units and primes of $Q^*(\sqrt{n})$ have been investigated. The exact number of ambiguous integers, ambiguous units and ambiguous primes in $Q^*(\sqrt{n})$ have also been determined there.

In particular it has been mentioned that an ambiguous unit (respectively prime) is a unit (respectively prime) which is an ambiguous number in $Q^*(\sqrt{n})$.

G will always denote the modular group, unless mentioned otherwise.

In this paper we determine the number of distinct closed paths formed by ambiguous numbers of $Q^*(\sqrt{n})$ under the modular group action.

2. PERLIMINARIES

Lemma 2.1 [1] Let p be a rational prime. Suppose that $p = 2$ or $p \equiv 1 \pmod 4$. Then p can be written as a sum of two squares.

Note: A rational prime p where $p \equiv 1 \pmod 4$ can be expressed as $a^2 + b^2$. Apart from these eight variations $(\pm a)^2 + (\pm b)^2 = (\pm b)^2 + (\pm a)^2 = p$, the expression of p as a sum of two squares is unique.

Theorem 2.2 [4] Ambiguous numbers in the orbit $\alpha^G = \{\alpha^g : g \in G\}$ of $\alpha \in Q^*(\sqrt{n})$ form a single closed path and it is the only closed path contained in the coset diagram for the orbit α^G.

The following simple remark is useful to determine the number of orbits of $Q^*(\sqrt{n})$ under the action of G.

Remark 2.3 The number of disjoint orbits α^G, $\alpha \in Q^*(\sqrt{n})$, is equal to the number of closed paths in the coset diagram under the action of G on $Q^*(\sqrt{n})$.

The results that follow will be used later in this paper.

Lemma 2.4 Let $\alpha \in Q^*(\sqrt{n})$.

Then

$$g(\bar{\alpha}) = \overline{g(\alpha)}, \quad \forall g \in G$$

Proof: Let $\alpha \in Q^*(\sqrt{n})$

Then

$$\begin{aligned}
\overline{x(\alpha)} &= \overline{\left(\frac{-1}{\alpha}\right)} = \frac{-1}{\overline{\alpha}} = x(\overline{\alpha}) \\
y(\alpha) &= 1 + x(\alpha) \\
y(\overline{\alpha}) &= 1 + x(\overline{\alpha}) = 1 + \overline{x(\alpha)} \\
&= \overline{1 + x(\alpha)} = \overline{y(\alpha)}
\end{aligned}$$

Also $y^2(\alpha) = y(y(\alpha))$ so that

$$\overline{y^2(\alpha)} = \overline{y(y(\alpha))} = y(\overline{\alpha'}), \quad \alpha' = y(\alpha)$$

$$= y(\overline{y(\alpha)}) = y(y(\overline{\alpha})) = y^2(\bar{\alpha})$$

As each $g \in G$ is a word in x, y or $y^2 = y^{-1}$ and $\overline{\alpha_1 \alpha_2} = \overline{\alpha_1}\ \overline{\alpha_2}$, so $g(\overline{\alpha}) = \overline{g(\alpha)}, \quad \forall g \in G$.

Definition 2.5 Let $\alpha \in Q^*(\sqrt{n}$. Then the number of ambiguous numbers in the orbit α^G is called the ambiguous length of α with respect to G. We simply call it the ambiguous length of α.

Lemma 2.6 For a real quadratic irrational number β in $\alpha^G, \alpha \in Q^*(\sqrt{n})$.

$$\begin{array}{ll}
(i) & x(-\beta) = -x(\beta) \\
(ii) & y(-\beta) = 2 - y(\beta) \\
(iii) & xy^2(-\beta) = -[yx(\beta)] \\
(iv) & yx(-\beta) = -[xy^2(\beta)] \\
(v) & y^2x(-\beta) = -[xy(\beta)], \qquad \text{and} \\
(vi) & xy(-\beta) = -[y^2x(\beta)]
\end{array}$$

Proof:

(i) Here for $\beta \in \alpha^G$, $\alpha \in Q^*(\sqrt{n})$

$$x(\beta) = \frac{-1}{\beta} = \frac{1}{-\beta} = -x(-\beta)$$

(ii) $y(-\beta) = 1 + x(-\beta) = 1 + \frac{1}{\beta} = 2 - \left(1 - \frac{1}{\beta}\right) = 2 - y(\beta)$

(iii) $xy^2(\beta) = \beta - 1$, so $xy^2(-\beta) = -\beta - 1$
Also $yx(\beta) = \beta + 1$, so that $yx(\beta) = 1 + \beta = -xy^2(-\beta)$

(iv) Here $yx(\beta) = \beta + 1 \Rightarrow yx(-\beta) = -\beta + 1$

and $xy^2(\beta) = \beta - 1 \Rightarrow xy^2(\beta) = \beta - 1$

so we have (iv). Similarly for (v) and (vi)

Remark 2.8:

- Using lemma 2.4, it is easy to see that for $\alpha \in Q^*(\sqrt{n})$, if $\bar{\alpha} \in \alpha^G$ then, for all $\beta \in \alpha^G$, $\bar{\beta} \in \alpha^G$.
- Using lemma 2.6, it is easy to see that for $\alpha \in Q^*(\sqrt{n})$, if $-\alpha \in \alpha^G$ then, for all $\beta \in \alpha^G$, $-\beta \in \alpha^G$.
- Hence, by corollary 2.7, it is easy to see that for $\alpha \in Q^*(\sqrt{n})$, if $-\bar{\alpha} \in \alpha^G$ then, for all $\beta \in \alpha^G$, $-\bar{\beta} \in \alpha^G$.

Remark 2.9: For $\alpha \in Q^*(\sqrt{n})$, since $g(\overline{\alpha}) = \overline{g(\alpha)}$, for all $g \in G$, $\bar{\alpha}^G$ consists of just conjugates of elements of α^G and vice versa. So for each $\alpha \in Q^*(\sqrt{n})$, the ambiguous lengths of α and $\bar{\alpha}$ are the same.

A necessary condition for the orbits α^G and $\bar{\alpha}^G$ to be identical or disjoint is given in the lemma that follows.

Lemma 2.10: For $\alpha \in Q^*(\sqrt{n})$ let $N(\alpha) = -1$, then $\alpha^G = \bar{\alpha}^G$.

Proof: Here $N(\alpha) = \alpha\bar{\alpha} = -1 \Rightarrow \bar{\alpha} = \frac{-1}{\alpha} = x(\alpha)$ and $x(\bar{\alpha}) = \alpha$. So $\alpha \in \bar{\alpha}^G$ and $\bar{\alpha} \in \alpha^G$. As $\alpha \in \alpha^G$ α^G and $\bar{\alpha}^G$ are not disjoint so $\alpha^G = \bar{\alpha}^G$.

3. THE ORBITS OF $Q^*(\sqrt{2})$ UNDER THE MODULAR GROUP ACTION: In this section we prove that G acts transitively on $Q^*(\sqrt{2})$.

Throughout this paper we assume that p is a rational prime. Since either $p = 2$ or $p \equiv 1, 3 \pmod 4$ so we discuss these cases separately.

Theorem 3.1: The only orbit under the action of G on $Q^*(\sqrt{2})$ is $Q^*(\sqrt{2})$ itself. That is G acts transitively on $Q^*(\sqrt{2})$.

Proof: Let

$$\alpha = \frac{a+\sqrt{2}}{c} \in Q^*(\sqrt{2})$$

such that

$$N(\alpha) = \alpha\bar{\alpha} = -1$$

Then

$$a^2 + c^2 = 2 \tag{1}$$

Theonly integral values of a and c satisfying (1) are ± 1, ± 1. Therefore there are exactly four distinct ambiguous numbers, namely

$\frac{1+\sqrt{2}}{\pm 1}$, $\frac{-1+\sqrt{2}}{\pm}$ of $Q^*(\sqrt{2})$ such that $x(\pm 1 + \sqrt{2}) = \pm 1 - \sqrt{2}$ and no other element of $Q^*(\sqrt{2})$ is mapped onto its conjugate under x.

Moreover

$$x(\pm\sqrt{2} = \frac{\mp\sqrt{2}}{2}, \quad yx(\pm\sqrt{2} = 1 \pm \sqrt{2}$$

and $xy^2(\pm\sqrt{2}) = -1 \pm \sqrt{2}$. This shows that the eight numbers

$$\pm\sqrt{2}, \frac{\pm\sqrt{2}}{2}, \frac{1+\sqrt{2}}{\pm 1}, \frac{1-\sqrt{2}}{\pm 1} \text{ of } Q^*(\sqrt{2})$$

form a single closed path under the action of G.

By [2] $Q^*(\sqrt{2})$ contains eight ambiguous numbers and these numbers are

$$\pm\sqrt{2},\ \frac{\pm\sqrt{2}}{2},\ \frac{1+\sqrt{2}}{\pm 1},\ \frac{1-\sqrt{2}}{\pm 1}$$

So, by theorem 2.2 and remark 2.3, the only orbit under the action of G on $Q^*(\sqrt{2})$ is $Q^*(\sqrt{2})$ itself.

Consequently G acts transitively on $Q^*(\sqrt{2})$

4. THE ORBITS OF $Q^*(\sqrt{p})$, WHERE $p \equiv 1$ (MOD 4) UNDER THE MODULAR GROUP ACTION: The section is concerned with the determination of number of orbits of $Q^*(\sqrt{p})$, $p \equiv 1 \pmod 4$, under the action of G.

In contrast with the action of G on $Q^*(\sqrt{2})$ we prove that G does not act transitively on $Q^*(\sqrt{2})$, $p \equiv 1$ (mod 4). Before a discussion on the number of orbits in $Q^*(\sqrt{p})$ we prove the following lemma.

Lemma 4.1: Let

$$\alpha = \frac{a+\sqrt{p}}{c} \in Q^*(\sqrt{p})$$

where p is any fixed rational prime and c is fixed. Then elements of the from $\frac{a'+\sqrt{p}}{c}$ of $Q^*(\sqrt{p})$, $a' = a + kc$, $k \in Z$, belong to α^G.

Proof: Let

$$\alpha = \frac{a+\sqrt{p}}{c} \in Q^*(\sqrt{p})$$

and $a' = a + kc$, $k \in Z$. Then

$$c|(p-a^2) \Leftrightarrow c|(p-a'^2)$$

and

$$\left(a, \frac{a^2-p}{c}, c\right) = 1 \Leftrightarrow \left(a', \frac{a'^2-p}{c}, c\right) = 1$$

So

$$\alpha \in Q^*(\sqrt{p}) \Leftrightarrow \alpha + k = \frac{(a+kc)+\sqrt{p}}{c} \in Q^*(\sqrt{p})$$

for all $k \in Z$.

Also, as $yx(\alpha) = \alpha + 1$ and $xy^2(\alpha) = \alpha - 1$, $(yx)^k(\alpha) = \alpha + k$ and $(xy^2)^k(\alpha) = \alpha - k$, $\forall k \in Z$ so $\alpha \in Q^*(\sqrt{p}) \Leftrightarrow \alpha + k \in \alpha^G$ for all $k \in Z$.

Note: If $\frac{-2a}{c} = k$ is a rational integer then

$$(yx)^k(\alpha) = \alpha + k = \frac{-a+\sqrt{p}}{c} = -\bar{\alpha} \in \alpha^G$$

Lemma 4.2: Let p be an odd rational prime and $\alpha = \frac{a+\sqrt{p}}{c}$ be an ambiguous number in $Q^*(\sqrt{p})$. Then

$$yx(\alpha) = \overline{-\alpha} \Leftrightarrow = \frac{-1+\sqrt{p}}{2} \quad \text{or} \quad \frac{1+\sqrt{p}}{-2}$$

Proof: Let

$$\alpha = \frac{a+\sqrt{p}}{c} \in Q^*(\sqrt{p})$$

Then α is an ambiguous number $\Leftrightarrow a^2 < p$.

Now

$$yx(\alpha) = \overline{-\alpha} \Leftrightarrow \alpha + 1 = \overline{-\alpha} \Leftrightarrow \alpha + \bar{\alpha} = -1 \Leftrightarrow \frac{a+\sqrt{p}}{c} + \frac{a-\sqrt{p}}{c} = -1 \Leftrightarrow -2a = c$$

As we know that

$$\frac{a+\sqrt{p}}{-2a} \in Q^*(\sqrt{p}) \Leftrightarrow \frac{a^2-p}{-2a}$$

is an integer and

$$\left(a, \frac{a^2-p}{-2a}, -2a\right) = 1$$

Now $\frac{a^2-p}{-2a}$ is an integer $\Leftrightarrow -2a|(a^2-p) \Leftrightarrow a^2 - p$ is even and $a|(a^2-p)$

Which is possible only if α is odd and $a|p$

$$(\because a|(a^2-p),\ a|a^2)$$

That is $a = \pm 1$ ($\because a^2 < p$ and p is rational prime)

So

$$yx(\alpha) = -\bar{\alpha} \Leftrightarrow = \frac{-1+\sqrt{p}}{2} \quad \text{or} \quad \alpha = \frac{1+\sqrt{p}}{-2}$$

Remark 4.3:

- If α is one of the numbers $\pm\sqrt{p}$, $\frac{\pm\sqrt{p}}{p}$, then $-\overline{\alpha} = \alpha$ and no other element of $Q^*(\sqrt{p})$ satisfies this condition.
- Also there is no α in $Q^*(\sqrt{p})$ such that $\alpha = \bar{\alpha}$.
- Moreover $\alpha \neq -\alpha$, for all $\alpha \in Q^*(\sqrt{p})$.

Theorem 4.4: Let $p \equiv 1 \pmod 4$ be a rational prime. Then $Q^*(\sqrt{p})$ splits into exactly two disjoint orbits under the action of G.

Proof: Since $p \equiv 1 \pmod 4$,

$$P = a^2 + c^2 = (\pm a)^2 + (\pm c)^2 = (\pm c)^2 + (\pm a)^2 \rightarrow (A)$$

Apart from these eight variations, the expression (A) is unique for some integers a and c, by lemma 2.1. Now

$$P = a^2 + c^2 \Rightarrow \frac{a^2 - p}{c^2} = -1$$

so that,

if $\gamma = \frac{a+\sqrt{p}}{c}$, then $\gamma\bar{\gamma} = -1$ and γ is an ambiguous number of $Q^*(\sqrt{p})$.

Also $x(\gamma) = -\frac{1}{\gamma} = \bar{\gamma}$

The equation (A) shows that a and c can not be both even or both odd.

Without any loss of generality, we can suppose that a is even and c is odd. Then there are exactly eight distinct ambiguous elements, namely,

$$\frac{a+\sqrt{p}}{\pm c}, \quad \frac{-a+\sqrt{p}}{\pm c}, \quad \frac{c+\sqrt{p}}{\pm a}, \quad \frac{-c+\sqrt{p}}{\pm a} \quad \text{of} \quad Q^*(\sqrt{p})$$

which of mapped to their conjugates under x.

That is if γ is one of these numbers then $x(\gamma) = \frac{-1}{\gamma} = \bar{\gamma}$ while other elements of $Q^*(\sqrt{p})$ are not mapped on to their conjugates under x.

Let

$$\alpha = \frac{a+\sqrt{p}}{c}$$

and

$$\beta = \frac{c+\sqrt{p}}{a}$$

So b is even as $b = \frac{p-c^2}{a} = a$

Consider now the orbit β^G. Clearly $\beta \in \beta^G$. Also let

$$\beta' = \frac{c'+\sqrt{p}}{a'} \in \beta^G$$

We prove that all $\beta' = \frac{c'+\sqrt{p}}{a'} \in Q^*(\sqrt{p})$, with c' odd, and $b' = \frac{p-c'^2}{a'}$, a' both even, belong to β^G.

Now every $g \in G$ is a word in x, y or $y^2 = y^{-1}$. So it is enough to show that $x(\beta')$, $y(\beta')$ are of the form β'.

But $x(\beta') = \frac{c'-\sqrt{p}}{b'} = \frac{-c'+\sqrt{p}}{-b'}$. Here $-c'$ is odd and $-b'$ is even.

Also $\frac{p-c'^2}{-b'} = -a'$ is even.

Similarly $y(\beta') = \frac{-(b'+c')+\sqrt{p}}{-b'}$. Here $-(b'+c')$ is odd, $-b'$ is even and $\frac{p-(b'+c)^2}{-b'} = \frac{p-b'^2-c'^2-2b'c'}{-b'} = -a'+b'+2c'$ is even. In particular $\frac{-1+\sqrt{p}}{\pm 2}$, $\frac{1+\sqrt{p}}{\pm 2}$ belong to β^G. So β^G consists of all elements of $Q^*(\sqrt{p})$ of the form $\frac{c'+\sqrt{p}}{a'}$, with c' odd and $\frac{p-c'^2}{a'}$, a' both even. As, by lemma 4.2, $yx(\alpha) = -\bar{\alpha}$ if and only if $\alpha = \frac{-1+\sqrt{p}}{2}$ or $\frac{1+\sqrt{p}}{-2}$, so by remark 2.8, for all $\delta \in \beta^G, \bar{\delta}, -\delta, -\bar{\delta} \in \beta^G$. Hence all the four ambiguous elements $\beta, \overline{-\beta}, -\beta, -\overline{\beta}$ belong to β^G. Further since, by theorem 2.2[4], ambiguous numbers in the orbit β^G form a unique closed path in the coset diagram, so there exists $g \in G$ such that $g(\beta) = -\beta$. But by lemma 2.4, $g(\bar{\beta}) = \overline{g(\beta)} = \overline{-\beta}$. Thus we have a closed path of $\beta^G = \left(\frac{1+\sqrt{p}}{2}\right)^G$ shown in figure 4.1.

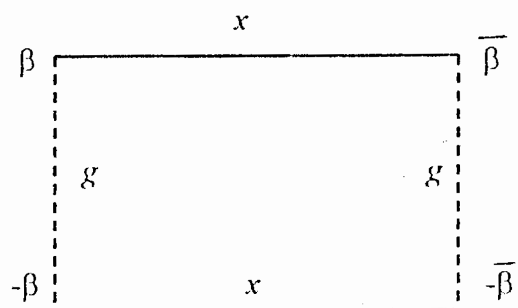

Figure 4.1

Again, by remark 4.3, if γ is one of the numbers $\pm\sqrt{p}$, $\frac{\pm\sqrt{p}}{p}$, then $\overline{-\gamma} = \gamma$ and no other element of $Q^*(\sqrt{p})$ satisfies this condition. Also $\bar{\delta} \neq \delta$ for all $\delta \in Q^*(\sqrt{p})$. As $x(\pm\sqrt{p}) = \frac{\mp\sqrt{p}}{p}$, so by remark 2.8, $\bar{\gamma}, -\gamma, \overline{-\gamma}$ belong to the same orbit $\alpha^G = (\sqrt{p})^G$, for all $\gamma \in \alpha^G$. The closed path of α^G is shown in figure 4.2.

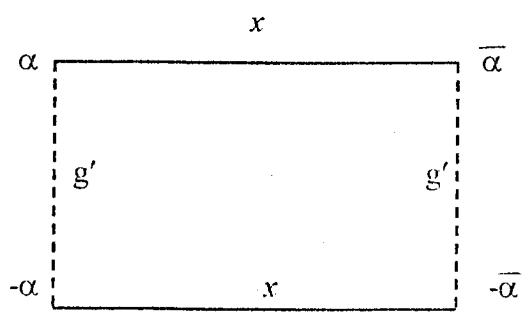

Figure 4.2

Further since $\alpha \notin \beta^G$, so α^G and β^G are disjoint

Moreover since $y(\delta) \neq \pm\bar{\delta}$, $yx(\delta) \neq \bar{\delta}$, $\delta \in Q^*(\sqrt{p})$. For if $y(\delta) = \pm\bar{\delta}$, Then $\frac{\delta-1}{\delta} = \pm\bar{\delta}$, and so $\delta - 1 = \pm\delta\bar{\delta}$, which is impossible because $\pm\delta\bar{\delta}$ is rational and $\delta - 1$is an irrational number.

Similarly if $yx(\delta) = \bar{\delta}$, $\delta = \frac{a_1+\sqrt{p}}{c_1}$, then $\frac{(a_1+c_2)+\sqrt{p}}{c_1} = \frac{a_1-\sqrt{p}}{c_1}$ so $c_1 = -2\sqrt{p}$ which is impossible. Also $y^2(\delta) \neq \pm\bar{\delta}$, for all $\delta \in Q^*(\sqrt{p})$.

Thus, as there are exactly eight distinct ambiguous numbers of $Q^*(\sqrt{p})$ which we mapped on to their conjugates under x, so there are exactly two distinct closed paths in the coset diagram under the action of G on $Q^*(\sqrt{p})$ and hence, by Remark 2.3, $Q^*(\sqrt{p})$ splits into exactly two disjoint orbits under the action of G.

They are precisely $(\sqrt{p})^G$ and $\left(\frac{1+\sqrt{p}}{2}\right)^G$.

Remark 4.5:

(i) $Q^*(\sqrt{p})$ splits into exactly two orbits such that one of these orbits consists of all elements of the form $\alpha = \frac{a+\sqrt{p}}{c}$, where a is odd and c, $\frac{p-a^2}{c}$ are both even, and the second orbit contains all forms of elements other than this form. So both of the disjoint orbits of $Q^*(\sqrt{p})$ under the action of G have different number of ambiguous numbers.

That is the number of ambiguous elements in these orbits is not the same.

Moreover the ambiguous length of $\beta = \frac{c+\sqrt{p}}{a}$ is greater than that of the ambiguous length of α.

(ii) The action of G on $Q^*(\sqrt{2})$ is transitive, whereas it is not so on $Q^*(\sqrt{p})$, $p \equiv 1 \pmod 4$.

REFERENCES

[1] Ivan Niven, Herbert S. Zurckerman and Hugh L. Montgomery, *An introduction to the theory of numbers*, Johnwiley and sons, Inc. 1991.

[2] M. Aslam, S. M. Husnine and A. Majeed, *Modular Group Action on certain Quadratic Fields*, PUJM, Vol. XXVIII (1995), pp 47-68.

[3] M. Aslam, S. M. Husnine and A. Majeed, *On Invariant Subsets of certain Quadratic Fields under Modular Group Action*, PUJM, Vol. 29 (1996), pp 20-26.

[4] Q. Mushtaq, *Modular Group Acting on Real Quadratic Fields*, Bull Austral. Math. Soc, Vol. 37 (1988), pp 303-309.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 51-64

COEFFICIENT ESTIMATES FOR CERTAIN CLASSES OF ANALYTIC FUNCTIONS

M. K. Aouf
H. E. Darwish & A. A. Attiya
Department of Mathematics
Faculty of Science
Mansoura University
Mansoura, Egypt.
E-mail: Sinfac@mum.mans.eun.eg

(Received 1 May, 1999)

ABSTRACT In the present paper we investigate the coefficient estimates for functions belonging to the classes $S_k^b(A, B)$ and $C_k^b(A, B)$ of analytic functions which are introduced here.

Key Words: Univalent, complex order, starlike, convex.
AMS (1991) Subject Classification. 30C45

1. INTRODUCTION Let S denote 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 disc $U = \{z : |z| < 1\}$. We use Ω to denote the class of analytic functions $w(z)$ in U satisfies the conditions $w(0) = 0$ and $|w(z)| < 1$ for $z \in U$.

Let $\mathbf{S}^b(\mathbf{A}, \mathbf{b})$ denote the class of functions $f(z) \in \mathbf{S}$ satisfy the conditions $f(z)/z \neq$

0 in U and

$$1+\frac{1}{b}\left(\frac{zf'(z)}{f(z)}-1\right) \prec \frac{1+Az}{1+Bz}, \ z \in U \tag{1.2}$$

where $\prec$ denotes subordination, $b \neq 0$ is any complex number and A and B are arbitrary fixed numbers, $-1 \leq \mathbf{B} < \mathbf{A} \leq 1$. The class $S^b(A,B)$ was studied by Sohi and Singh [30].

Further let $C^b(A,B)$ denote the class of functions $f(z) \in S$ satisfy the conditions $f'(z) \neq 0$ in U and

$$1+\frac{1}{b}\frac{zf''(z)}{f'(z)} \prec \frac{1+Az}{1+Bz}, \ z \in U \tag{1.3}$$

It follows from (1.2) and (1.3) that

$$f(z) \in C^b(A,B) \ \text{ if and only if } \ zf'(z) \in S^b(A,B) \tag{1.4}$$

By specializing b, A and B, we obtain several subclasses studied by various authors in earlier papers:

(1) $S^1(A,B) = S^*(A,B)$ (Janowski [11]), $C^1(A,B) = C(A,B)$ (Mazur [16], Silverman and Silvia [27]), $S^{1-\alpha}(1,-1), = S^*(\alpha)(0 \leq \alpha < 1)$ the class of starlike functions of order α, $0 \leq \alpha < 1$) was introduced by Roberston [26]) and $C^{1-\alpha}(1,-1) = C(\alpha)$ $(0 \leq \alpha < 1)$ (the class of convex functions of order $\alpha, 0 \leq< 1$, was introduced by Roberston [26] and Pinchuk [25]).

(2) $S^{(1-\alpha)\cos\lambda e^{-i\lambda}}(1,-1) = S^\lambda(\alpha)\left(|\lambda| < \frac{\pi}{2}, 0 \leq \alpha < 1\right)$ (Libera [14]), $C^{(1-\alpha)\cos\lambda e^{-i\lambda}}(1,-1) = C^\lambda(\alpha)\left(|\lambda| < \frac{\pi}{2}, 0 \leq \alpha < 1\right)$ (Chichra [8] and Sizuk [29]), $S^{(1-\alpha)\cos\lambda e^{-i\lambda}}(1, 1-2\beta = S^\lambda(\alpha,\beta)$ $(|\lambda| < \lambda/2,\ 0 \leq \alpha < 1,\ 0 < \beta \leq 1)$ (Mogra and Ahuja [18]) and $C^{(i-\alpha)\cos\lambda e^{-1\lambda}}(1, 1-2\beta) = C^\lambda(\alpha\beta)$ $(|\lambda| < \frac{\pi}{2},\ 0 \leq \alpha < 1,\ 0 < \beta \leq 1))$ (Ahuja [1]).

(3) $S^b(1,-1) = S(1-b)$ (Nasr and Aouf [20]), $C^b(1,-1) = C(b)$ (Waitrowski [32]) and Nasr and Aouf [21]), $S^b(1, 1-2\beta) = S(1-b,\beta)(0 < \beta \leq 1)$ and $C^b(1, 1-2\beta) = C(b,\beta)(0 < \beta \leq 1)$ (Aouf, Owa and Obradovic' [6]).

(4) $S^b\left(1, \frac{1}{M}-1\right) = F(b,M)\left(M > \frac{1}{2}\right)$ (Nasr and Aouf [22]), $C^b\left(1, \frac{1}{M}-1\right) = G(b,M)\left(M > \frac{1}{2}\right)$ (Nasr and Aouf [23]), $C^{\cos\lambda e^{-i\lambda}}\left(1, \frac{1}{M}-1\right) = F_{\lambda,\mathrm{M}}\left(|\lambda| < \frac{\pi}{2},\right.$ $\left.M > \frac{1}{2}\right)$ (Kulshrestha [13]), $C^{\cos\lambda e^{-i\lambda}}\left(1, \frac{1}{M}-1\right) = G_{\lambda,\mathrm{M}}\left(|\lambda| < \frac{\pi}{2},\ M > \frac{1}{2}\right)$ (Kulshrestha [13]), $S^{(1-\alpha)\cos\lambda e^{-i\lambda}}\left(1, \frac{1}{M}-1\right) = F_{\mathrm{M}}(\lambda,\alpha)\left(|\lambda| < \frac{\pi}{2}, 0 \leq \alpha < 1,\ \ M > \frac{1}{2}\right)$

(Aouf [23]), $C^{(1-\alpha)\cos\lambda e^{-i\lambda}}\left(1, \frac{1}{M}-1\right) = G_M(\lambda,\alpha)\left(|\lambda| < \frac{\pi}{2}, 0 \le \alpha < 1,\ M > \frac{1}{2}\right)$ (Aouf [2,3]), $S^1\left(1, \frac{1}{M}-1\right) = F(1,M)\left(M > \frac{1}{2}\right)$ (Singh and Singh [28]) and $S^{(1-\alpha)\cos\lambda e^{-i\lambda}}\left(\frac{M^2-m^2+m}{M}, \frac{1-m}{M}\right) = S^*_{m,M}(\alpha,\lambda)(1-m < M \le m,\ 0 \le \alpha < 1$ and $|\lambda| < \frac{\pi}{2})$ (Jakubowski [10]).

MacGregor[15] obtained upper bounds for the moduli of the coefficients of a starlike functions whose power series representation in U is of the form

$$f(z) = z + \sum_{n=k+1}^{\infty} a_n z^n \tag{1.5}$$

Boyd [7], Srivastava [31], Mogra and Juneja [19], Aouf [4, 5] and Owa and Aouf [24] extended MacGregor's result to different classes of analytic functions.

In the present paper, we determine sharp coefficient estimates for the classes $S_k^b(A,B)$ and $C_k^b(A,B)$ whose power series representation of the form (1.5).

2. COEFFICIENT ESTIMATES

We shall use the following lemma in our investigation:

Lemma 1. If k, q are positive integers and $-1 \le B < A \le 1$, then

$$(A-B)^2|b|^2 + \sum_{m=1}^{q}\left\{\frac{1}{m!}\prod_{j=0}^{m-1}\left|\frac{(A-B)b}{k} - Bj\right|^2\right\}.$$

$$.\left\{|(A-B)b - mkB|^2 - m^2k^2\right\} =$$

$$= \left\{\frac{k}{(q-1)!}\prod_{j=0}^{q-1}\left|\frac{(A-B)b}{k} - Bj\right|^2\right\}.$$

The Lemma can be proved by induction of q for a fixed k in the same way as the lemma in [7].

Theorem 1 Let a function $f(z)$ given by (1.1) be in the class $S_k^b(A,B)$.

(i) If $(A-B)^2|b|^2 > (n-1)\{(n-1)(1-B^2)+2B(A-B)\ \mathrm{Re}\ \{b\}\}$, $n \geq mk+1$, $m \in N$, then

$$|a_n| \leq \frac{k}{(m-1)!(n-1)} \left\{ \prod_{j=0}^{m-1} \left| \frac{(A-B)b}{k} - Bj \right| \right\} \tag{2.1}$$

for $mk+1 \leq n \leq (m+1)k$ and $m = 1, 2, 3, \cdots, N+1$, and

$$|a_n| \leq \frac{k}{(N+1)!(n-1)} \prod_{j=0}^{N+1} \left| \frac{(A-B)b}{k} - Bj \right| \tag{2.2}$$

for $n > (N+2)k$, where $N = [G]$ (Gauss symbol) and

$$G = \frac{(A-B)^2|b|^2}{(n-1)\{(n-1)(1-B^2)+2B(A-B)\ \mathrm{Re}\ \{b\}\}}$$

(ii) If $(A-B)^2|b|^2 \leq (n-1)\{(n-1)(1-B^2)+2B(A-B)\ \mathrm{Re}\ \{b\}\}$ $n \geq k+1$, then

$$|a_n| \leq \frac{(A-B)|b|}{(n-1)} \tag{2.3}$$

for $n \geq k+1$. The estimates in (2.1) are sharp for $n = mk+1$, $m = 1, 2, 3, \cdots, N+1$, while the estimates in (2.3) are sharp for each n.

Proof Since $f(z) \in S_k^b(A, B)$, by definition of subordination, there exists an analytic function $g(z)$ which satisfies

$$g(z) = \frac{zf'(z) - f(z)}{-Bzf'(z) + [b(A-B)+1]f(z)} \tag{2.4}$$

and $|g(z)| < 1 (z \in U)$. Also we note that

$$g(z) = c_k z^k + c_{k+1} z^{k+1} + \cdots$$

It follows from (2.4) that

$$\sum_{n=k+1}^{\infty} (n-1)a_n z^n = (c_k z^k + c_{k+1} z^{k+1} + \cdots)[(A-B)bz$$

$$+\sum_{n=k+1}^{\infty}((A-B)b-B(n-1)a_n z^n].$$

Equating the coefficients of the same powers on both sides (2.5), we see that

$$(n-1)a_n = (A-B)bc_{n-1}(n = k+1,\ k+2,\cdots,2k) \tag{2.6}$$

Since $|g(z)| < 1$ implies that

$$\sum_{n=k}^{2k-1} |c_n|^2 \leq 1 \tag{2.7}$$

we have

$$\sum_{n=k+1}^{\infty} (n-1)^2|a_n|^2 \leq (A-B)^2|b|^2 \tag{2.8}$$

Equation (2.5) can be written as

$$\sum_{n=k+1}^{p} (n-1)a_n z^n + \sum_{n=p+1}^{\infty} d_n z^n = g(z)[(A-B)bz$$

$$+\sum_{n=k+1}^{p-k} [((A-B)b-B(n-1))a_n z^n] \tag{2.9}$$

Since, (2.9) is of the form $F(z) = g(z)h(z)$ and $|g(z) < 1(z \in U)$, we know that

$$\frac{1}{2\pi}\int_0^{2\pi} \left|F(re^{i\theta})\right|^2 d\theta \leq \frac{1}{2\pi}\int_0^{2\pi} \left|h(re^{i\theta}\right|^2 d\theta \tag{2.10}$$

for each $r(0 < r < 1)$. Equation (2.10) in terms of the coefficients (2.9) can be expressed as

$$\sum_{n=k+1}^{p} (n-1)^2|a_n|^2 r^{2n} + \sum_{n=p+1}^{\infty} |d_n| r^{2n} \leq (A-B)^2|b|^2 r^2$$

$$\sum_{n=k+1}^{p-k} |((A-B)b-B(n-1))|^2|a_n|^2 r^{2n} \tag{2.11}$$

In particular (2.11) implies that

$$\sum_{n=k+1}^{p} (n-1)^2|a_n|^2 r^{2n} \leq (A-B)^2|b|^2 r^2$$

$$+ \sum_{n=k+1}^{p-k} |((A-B)b - B(n-1)))|^2 |a_n|^2 r^{2n} \tag{2.12}$$

Letting $r \to 1$ in (2.12), we obtain

$$\sum_{n=p-k+1}^{p} (n-1)^2|a_n|^2 \leq (A-B)^2|b|^2$$

$$+ \sum_{n=k+1}^{p-k} \{|((A-B)b - B(n-1))|^2 - (n-1)^2\}|a_n|^2 \tag{2.13}$$

(i) If $(A-B)^2|b|^2 > (n-1)\{(n-1)(1-B^2) + 2B(A-B)\ rmRe\ \{b\}\}$, $n \geq mk+1$, $m = 1, 2, 3, \cdots$

We now establish, by an inductive argument, the inequalities

$$\sum_{n=mk+1}^{(m+1)k} (n-1)^2|a_n|^2 \leq \left\{ \frac{k}{(m-1)!} \prod_{j=0}^{m-1} \left| \frac{(A-B)b}{k} - Bj \right| \right\}^2 \tag{2.14}$$

and

$$\sum_{n=mk+1}^{(m+1)k} \left\{ |(A-B)b - B(n-1)|^2 - (n-1)^2 \right\} |a_n|^2$$

$$\leq \left\{ \frac{1}{m!} \prod_{j=0}^{m-1} \left| \frac{(A-B)b}{k} - Bj \right| \right\}^2 \{|(A-B)b - mkB|^2 - m^2k^2\} \tag{2.15}$$

for $m = 1, 2, 3, \cdots, N+1$, where $N = [G]$ is given by

$$G = \frac{(A-B)^2|b|^2}{(n-1)\{(n-1)(1-B^2) + 2B(A-B)\ \mathrm{Re}\ \{b\}\}}$$

and [G] is the greatest integer not greater than G.

For $m = 1$, (2.14) gives

$$\sum_{n=k+1}^{2k} (n-1)^2 |a_n|^2 \leq (A-B)^2 |b|^2$$

which is the same as (2.8). Thus (2.14) is valid for $m = 1$. We can prove (2.15) for $m = 1$ by using (2.8) as follows:

$$\sum_{n=k+1}^{2k} \{|(A-B)b - B(n-1)|^2 - (n-1)^2\} |a_n|^2$$

$$\leq \frac{|(A-B)b - Bk|^2}{k^2} \sum_{n=k+1}^{2k} (n-1)^2 |a_n|^2$$
$$\leq \frac{\{|(A-B)b - Bk|^2 - k^2\}(A-B)^2|b|^2}{k^2}$$

which establishes (2.15) for $m = 1$.

Now let $q > 1$ and suppose that (2.14) and (2.15) hold true for $n = 1, 2, 3, \cdots, q-1$. Using (2.13) with $p = (q+1)k$ and the inductive hypothesis concerning (2.14), we have

$$\sum_{n=qk+1}^{(q+1)k} (n-1)^2 |a_n|^2 \leq (A-B)^2 |b|^2$$

$$+ \sum_{n=k+1}^{qk} \{|((A-B)b - B(n-1))|^2 - (n-1)^2\} |a_n|^2$$

$\leq (A-B)^2|b|^2 +$

$$\sum_{m=1}^{q-1} \sum_{n=mk+1}^{(m+1)k} \{((A-B)b - B(n-1))|^2 - (n-1)^2\} |a_n|^2$$

$\leq \ (A-B)^2|b|^2 +$

$$\sum_{m=1}^{q-1} \left\{ \frac{1}{m!} \prod_{j=0}^{m-1} \left| \frac{(A-B)b}{k} - Bj \right| \right\}^2 \{|(A-B)b - mkB|^2 - m^2k^2\}$$

be the induction hypothesis.

Using Lemma 1, we get

$$\sum_{n=qk+1}^{(q+1)k}(n-1)^2|a_n|^2 \leq \left\{\frac{k}{(q-1)!}\prod_{j=0}^{q-1}\left|\frac{(A-B)b}{k}-Bj\right|^2\right\}$$

so that (2.14) holds for $m = q$.

Continuing our argument, we use (2.14) with $m = q$ to deduce (2.14) for $m = q$.

This completes the proof of (2.14), (2.15) and (2.1) follows from (2.14).

In order to prove (2.2), we suppose $n > (N+2)k$. Letting $p = (q+1)k$ in (2.13), we see

$$\sum_{n=qk+1}^{(q+1)k}(n-1)^2|a_n|^2 \leq (A-B)^2|b|^2$$

$$+\sum_{n=k+1}^{qk}\{|((A-B)b-B(n-1)))|^2-(n-1)^2\}|a_n|^2$$

which gives

$$(n-1)^2|a_n|^2 \leq (A-B)^2|b|^2+$$

$$\sum_{n=k+1}^{qk}\{|((A-B)b-B(n-1))|^2-(n-1)^2\}|a_n|^2$$

$$=(A-B)^2|b|^2+\sum_{n=k+1}^{(N+2)k}\{|((A-B)b-B(n-1))|^2-(n-1)^2\}|a_n|^2+$$

$$\sum_{n=(N+2)k+1}^{qk}\left\{|((A-B)b-B(n-1)^2|-(n-1)^2\right\}|a_n|^2$$

$$=(A-B)^2|b|^2+\sum_{m=1}^{N+1}\sum_{n=mk+1}^{(m+1)k}\left\{|((A-B)b-B(n-1)|^2-(n-1)^2\right\}|a_n|^2$$

$$\sum_{m=N+2}^{q-1}\sum_{n=mk+1}^{(m+1)k}\left\{|((A-B)b-B(n-1))|^2-(n-1)^2\right\}|a_n|^2$$

$$\leq (A-B)^2|b|^2+$$

$$\sum_{m=1}^{N+1} \sum_{n=mk+1}^{(m+1)k} \left\{|((A-B)b-B(n-1)|^2-(n-1)^2\right\} |a_n|^2 \tag{2.16}$$

An application of (2.14) and (2.16) leads us to

$$(n-1)^2|a_n|^2 \leq \left\{\frac{k}{(N+1)!} \prod_{j=0}^{N+1} \left|\frac{(A-B)b}{k} - Bj\right|\right\}^2$$

that is,

$$|a_n| \leq \frac{k}{(N+1)!(n-1)} \prod_{j=0}^{N+1} \left|\frac{(A-B)b}{k} - Bj\right| (n > (N+2)k)$$

(ii) If $(A-B)^2|b|^2 \leq (n-1)\{(n-1)(1-B)^2 + 2B(A-B) \text{ Re } \{b\}\}$, $n \geq k+1$ then (2.13) gives

$$\sum_{n=k+1}^{P} (n-1)^2|a_n|^2 \leq (A-B)^2|b|^2$$

or

$$|a_n| \leq \frac{(A-B)|b|}{(n-1)}, \qquad (n \geq k+1)$$

which proves (2.3). The function $f(z)$ given by

$$f(z) = \begin{cases} \frac{z}{(1+BZ^k)^{\frac{-b(A-B)}{Bk}}}, & B \neq 0, \\ (1+Bz^k) & \\ z \exp\left(\frac{bA}{k}z^k\right), & B = 0, \end{cases} \tag{2.17}$$

where $(A-B)^2|b|^2 > (n-1)\{(n-1)(1-B)^2+2B(A-B) \text{ Re } \{b\}\}$, shows that the estimates in (2.1) are sharp for $n = mk+1,\ 1, m = 1, 2, \cdots$, while the estimates in (2.3) are sharp for

$$f_n(z) = z \exp\left[\frac{(A-B)b}{(n-1)} z^{n-1}\right] \tag{2.18}$$

where $(A-B)^2|b|^2 \le (n-1)\{(n-1)(1-B)^2+2B(A-B)\ \mathrm{Re}\ \{b\}\},\ \ n \ge K+1$

Remarks on Theorem 1

1. Putting $A=1,\ B=-1$ and $b=1$ in Theorem 1, we get the result due to MacGregoer [15].

2. Putting $A=1,\ B=-1$ and $b=1-\alpha,\ 0\le\alpha<1$, in Theorem 1, we get the result due to Boyd [7].

3. Putting $A=1,\ B=-1$ and $b=(1-\alpha)\cos\lambda e^{-i\lambda},\ 0\le\alpha<1$ and $|\lambda|<\frac{\pi}{2}$, in theorem 1, we get the result due to Gopalakrishna and Shetiya [9].

4. Putting $b=(1-\alpha)\cos\lambda e^{-i\lambda},\ 0\le\alpha<1$ and $|\lambda|<\frac{\pi}{2}$, in Theorem 1, we get the result due to Aouf [4].

5. Putting $A=1,\ B=1-2\beta,\ 0<\beta\le 1$, in Theorem 1, we get the result due to Owa and Aouf [24].

6. Putting (i) $b=(1-\alpha)\cos\lambda e^{-i\lambda},\ 0\le\alpha<1$ and $|\lambda|<\frac{\pi}{2},\ A=1$ and $B=1-2\beta,\ 0<\beta\le 1$, (ii) $b=(1-\alpha)\cos\lambda e^{-i\lambda},\ 0\le\alpha<1$ and$|\lambda|<\frac{\pi}{2},\ A=1$ and $B=-1$ (iii) $b=\cos\lambda e^{-i\lambda},\ |\lambda|<\frac{\pi}{2},\ A=1$ and $B=\frac{1-\delta}{\delta},\ \delta>\frac{1}{2}$, (iv) $b=\cos\lambda e^{-i\lambda}$ and $B=\frac{\cos\lambda-1}{2},\ |\lambda|<\frac{\pi}{2}$, respectively, in Theorem 1, we get the results obtained by Mogra [17].

7. Putting $b=1-\alpha,\ 0\le\alpha<1,\ A=1$, and $B=1-2\beta,\ 0<\beta\le 1$ in Theorem 1, we ger the result due to Mogra and Juneja [19].

Nothing that $f(z)\in C_k^b(A,B)$ if and only if $zf'(z)\in S_k^b(A,B)$, we have for the functions belonging to the class $C_k^b(A,B)$.

Theorem 2 Let a function $f(z)$ given by (1.5) be in the class $C_k^b(A,B)$.

(i) If $(A-B)^2|b|^2 > (n-1)\{(n-1)(1-B^2)+2B(A-B)\ \mathrm{Re}\ \{b\}\},\ \ n\ge mk+1,\ \ m\in N$, then

$$|a_n| \le \frac{k}{(m-1)!n(n-1)}\left\{\prod_{j=0}^{m-1}\left|\frac{(A-B)b}{k}\right|-B_j\right\} \tag{2.19}$$

for $mk+1 \leq n \leq (m+1)k,\ m = 1,2,3,\cdots,N+1$, and

$$|a_n| \leq \frac{k}{(N-1)!n(n-1)} \prod_{j=0}^{N+1} \left| \frac{(A-B)b}{k} - Bj \right| \tag{2.20}$$

for $n > (N+2)k$, where N is defined in Theorem 1.

(ii) If $(A-B)^2|b|^2 \leq (n-1)\{(n-1)(1-B^2)+2B(A-B)\,\mathrm{Re}\,\{b\}\},\ n \geq k+1$, then

$$|a_n| \leq \frac{(A-B)|b|}{n(n-1)} \tag{2.21}$$

for $n \geq k+1$. The estimates in (2.19) are sharp for function $f(z)$ given by

$$1 + \frac{zf''(z)}{f'(z)} = \frac{1+[B+(A-B)b]z^k}{1+Bz^k} \tag{2.22}$$

for $n = mk+1,\quad m = 1,2,3,\cdots$, while the estimates in (2.21) are sharp for functions $f_n(z)$ given by

$$f_n'(z) = \exp\left(\frac{(A-B)b}{n-1} z^{n-1}\right)$$

REFERENCES

[1] O.P.Ahuja, *Certain generalization of the Robertson functions,* Yokohama Math. J. 31 (1983), 5-11.

[2] M.K. Aouf, *Bounded p-valent Robertson functions of order α,* Indian J.Pure Appl. Math. 16 (1985), no.7, 775-790.

[3] M.K.Aouf, *Bounded spiral-like functions with fixed second coefficient,* Internat. J. Math. Math. Sci. 12 (1989), no. 1, 113-118.

[4] M.K.Aouf, *Coefficient estimates for a certain class of spiral-like mappings,* Soochow J. Math. 2 (1990), 231-239.

[5] M.K.Aouf, *Coefficient estimates for bounded starlike functions of complex order*, Tamkang J. Math. 25(1994), no. 2, 113-123.

[6] M.K.Aouf, *S. Owa and M. Obradovic', Certain classes of analytic functions of complex order and type beta*, Rend. Mat. 11 (1991), 691-714.

[7] A.V.Boyd, *Coefficient estimates for starlike functions of order α*, Proc. Amer. Math. Soc. 17 (1966), 1016-1018.

[8] P.N. Chichra, *Regular functions $f(z)$ for which $zf'(z)$ is α-spiralike*, Proc. Amer. Math. Soc. 49 (1975), 151-160.

[9] H.S. Gopalakrishna and V.S.Shetiya, *Coefficient estimates for spiral-like mappings,* J. Karnatak Univ. Sci. 18 (1973), 297-307.

[10] Z. J. Jakubowski, *On coefficients of starlike functions of some classes*,Bull. De L'Academic Polonaise des Sciences 19(1971), no. 9, 811-815.

[11] W. Janowski, *Some extremal problems for certain families of analytic functions*, Ann. Polon. Math. 28 (1973), 297-326.

[12] O.P.Juneja and M.L. Mogra, *On starlike functionsof order α and type β,* Notices Amer. Math. Soc. 22(1975), A-384, Abstract no. 75T-B80.

[13] P.K. Kulshrestha, *Bounded Robertson functions,* Rend.Mat. (7) 9 (1976), 137-150.

[14] R. J. Libera, *Univalent α-spiral functions*, Cand. J.Math. 19(1967), 449-456.

[15] T.H. MacGregor, *Coefficient estimates of starlike mappings,* Michigan Math. J. 10 (1963), 277-281.

[16] R. Mazur, *On a subclass of convex functions*, Zesz. Nauk. Pol. Mat. 13 (1981), 15-20.

[17] M.L.Mogra, *On coefficient estimates for λ-spirallike and Robertson functions*, Rend. Mat. (7) 3 (1983), no. 1, 95-106.

[18] M.L.Mogra and O.P.Ahuja, *On spiral-like functions of order α and type β*, Yokohama Math. J. 29 (1981), 145-156.

[19] M.L. Mogra and O.P.Juneja, *Coefficient estimates for starlike functions*, Bull. Austral. Math. Soc. 16(1977), 415-425.

[20] M.A.Nasr and M.K.Aouf, *Starlike function of complex order,* J. Natur. Sci. Math. 25(1985), 1-12.

[21] M.A.Nasr and M.K.Aouf, *On convex functions of complex order,* Bull.Fac. Sci.Mansoura Univ. 9 (1982), 565-582.

[22] M.A.Nasr and M.K.Aouf, *Bounded starlike functions of complex order*, Proc. Indian Acad. Sci. (Math. Sci.) 92(1983), 97-102.

[23] M.A.Nasr and M.K.Aouf, *Bounded convex functions of complex order*, Bull. Fac. Sci. Mansoura Univ. 10 (1983), 513-527.

[24] S.Owa and M.K.Aouf, *On coefficient estimates for certain classes of analytic functions of complex order b and type beta*, J. Fac. Sci. Tech. Kinki. Univ. 29 (1993), 5-11.

[25] B. Pinchuk, *On starlike and convex functions of order* α, Dune Math. J. 35 (1968), 621-734.

[26] M.S. Robertson, *On the theory of univalent functions*, Ann. Math. 37 (1936), 374-408.

[27] H. Silverman and E.M.Silvia, *Subclasses of starlike functions subordinate to convex functions,* Cand. J. Math. 37 (1985), 48-61.

[28] R. Singh and V. Singh, *On a class of bounded starlike functions,* Indian J. Pure Appl. Math. 5(1974), 733-754.

[29] P.I.Sizuk, *Regular functions* $f(z)$ *for which* $zf'(z)$ *is* α*-spirallike,* Proc. Amer. Math. Soc. 49 (1975), 151-160.

[30] N.S.Sohi and L.P.Singh, *A class of bounded starlike functions of complex order,* Indian J. Math. 33 (1991), no. 1, 29-35.

[31] R.S.L.Srivastava, *Univalent spiral functions, Topics in analysis,* 327-341 (Lecture Notes in Mathematics, 419.Springer-Verlag, Berlin, Heidelberg, New York, 1974).

[32] P.Wiatrowski, *The coefficients of a certain family of holomorphic functions*, Zeszyty Nauk. Univ. Lodzk. Nauki. Math. Przyrod 39(1971), 75-85.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii (2000) pp. 65-72

A NOTE ON STATISTICAL LIMIT POINTS

Binod Chandra Tripathy
Mathematical Sciences Division
Institute of Advanced Study in Science and Technology
KHANAPARA; GUWAHATI-781 022; INDIA

(Dedicated to my sisters Prabasini, Pramila and Pratima)

(Received 15 October, 1997)

ABSTRACT In this article we prove the statistical analogue of some of the limit theorems on convergent sequences.

Key Words statistical convergence, density, statistical cluster point, thin subsequence, nonthin subsequence.

1. INTRODUCTION

The conceptof statistical convergence was introduced by Fast [4], Buck [1] and Schoenbery [10] independently. Further the concept was studied and linked with summability by Fridy [5], [6], Cannor [2], Maddox [7], Rath and Tripathy [8], Salat [9], Tripathy [11], [12], [13] and many others. The concept of statistical Cauchy sequences and statistical limit points was introduced by Fridy [5], [6]. Most of the concepts depend on the idea of certain density of a subset of the set of N of natural numbers. In this article we give examples where the statistical limit deviates from ordinary limits and establish some results.

For $K \subseteq N$, we have $K_n = \{k \in K : k \leq n\}$ and $|K_n|$ denotes the number of elements in K_n. Then the *natural density* of K is defined by $\delta(K) = \lim_{n\to\infty} \frac{|K|}{n}$ if exists. A real number sequence (x_n) is said to be *statistically convergent* to L, written as stat-lim $x_n = L$ if for every $\epsilon > 0$, $\delta(\{k \in N : |x_k - L| \geq \epsilon\}) = 0$. The number L is necessarily unique.

2. DEFINITIONS AND PROPERTIES If (x_{kj}) is a subsequence of (x_n) and $K = \{k_j : j \in N\}$, then it is called as a *thin subsequence* of (x_n) if $\delta(K) = 0$. It is called as a *nonthin* subsequence of (x_n) if $\delta(K) \neq 0$ or K fails to have natural density. A sequence with is statistically convergent to zero is called a *statistically null sequence.*

Definition 1 The number μ is a *statistical limit point* of the number sequence (x_n) provided that there is a nothin subsequence of (x_n) that converges to μ.

Definition 2 The number μ is a *statistical cluster point* of the number sequence (x_n) provided that for every $\epsilon > 0$ the set $\{n \in N : |x_n - \mu| < \epsilon\}$ does not have density zero.

Definition 3 The sequence (x_n) is said to be *statistically bounded* if there exists a $A > 0$ such that the set $\{n \in N : |x_n| > A\}$ has zero natural density.

Definition 4 A real sequence (x_n) is said to be *statistically monotonic increasing* if there exists such a set $K = \{k_1 < k_2 < --- < k_n < ---\} \subset N$ that $\delta(K) = 1$ and $x_{k_n} \leq x_{k_{n+1}}$ for all $n \in N$.

Similarly we can define *statistically monotonic decreasing* sequences. The above definition is corrected by Tripathy [12], became proposition 3 of Fridy [6] fails to hold by his definition. This is shown by an example.

The following well-known lemmas are required for establishing the results of this article.

Lemma 1 *Let a bounded sequence (x_n) be statistically convergent to L, then $(C, 1) - \lim x_n = L$. (See for example [10], Lemma 4.)*

Lemma 2 *A sequence (x_n) is statistically convergent to L if and only if there* *exists such a set* $K = \{k_1 < k_2 < - - - k_n < - - -\} \subset N$ that $\delta(K) = 1$ and $\lim_{n\to\infty} x_{k_n} = L$ *(see for example [9], Lemma 1.1).*

Lemma 3 *If the sequences* (x_n) *and* (y_n) *tend to zero and if* (y_n) *is positive and decreasing then*

$$\lim_{n\to\infty} \frac{x_n}{y_n} = \lim_{n\to\infty} \frac{x_n - x_{n+1}}{y_n - y_{n+1}}$$

provided the limit on the right exists, whether finite or infinite (see for example [3], Problem 18(i), page 86).

Lemma 4 *If* (x_n) *is a bounded number sequence, then* (x_n) *has a statistical cluster point. (See for example [6], Corollary.)*

For (x_n) a convergent sequence, we have $\lim - \sup x_n = \lim - \inf x_n = \lim x_n$. But for statistically convergent sequences, the equality may or may not hold. For this consider the following example.

Example 1 Define the sequence (x_n) by

$$x_n = \begin{cases} 2, & \text{if } n = k^2 \text{ and } n \text{ is even,} \\ -2, & \text{if } n = k^2 \text{ and } n \text{ is odd, } k \in N, \\ n^{-1}, & \text{otherwise} \end{cases}$$

From the above example it is clear that *a statistically monotonic sequence can have at most one statistical cluster point, but more cluster points.*

If a sequence has one statistical cluser point, then it may or may not be statistically convergent. Consider the following example.

Example 2 Define the sequence (x_n) by

$$x_n = \left[\begin{array}{ll} 1, & n \text{ even} \\ n, & n \text{ odd} \end{array} \right.$$

From the above examples, it is clear that *lim - sup* x_n *and lim-inf* x_n *may or may not be the statistical cluster points of the sequence* (x_n).

3. THE MAIN RESULTS The proof of the following two propositions are obvious.

Proposition 1 *If a sequence (x_n) is statistically convergent to L, then every nonthin subsequence will have L as a statistical limit point.*

Proposition 2 *A statistically monotonic sequence is statistically convergent if and only if it is statistically bounded equivalently it is unbounded over a thin subsequence.*

Theorem 3 *Let (x_n) be a bounded statistically convergent sequence. Then*

$$\lim_{n\to\infty} (x_1 x_2 x_3 \cdots x_n)^{1/n} = stat\ -\lim x_n$$

where $x_n > 0$, for all n.

Proof Let (x_n) be a bounded sequence which is statistically convergent to L. Then $(\log x_n)$ is also a bounded sequence, statistically convergent to $\log L$. Then by Lemma 1 it follows that

$$\frac{\log x_1 + \log x_2 + \cdots + \log x_n}{n} \to \log L, \quad \text{as} \quad n \to \infty$$

$$\Rightarrow (x_1 x_2 x_3 \cdots x_n)^{1/n} \to L = \text{stat} - \lim x_n \quad \text{as} \quad n \to \infty$$

The following Proposition follows from Lemma 4.

Proposition 4 *If a sequence has no statistical cluster point, then it is unbounded.*

Theorem 5 *If the bounded sequences (x_n) and (y_n) are statistically convergent to L and M respectively, then*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} x_k y_{n-k+1} = LM$$

and

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k-1}^{n} x_k y_k = LM$$

Proof Let (x_n) and (y_n) be bounded sequences, statistically convergent to L and M respectively. Then we have $x_n = L + a_n$ and $y_n = M + b_n$ say, where (a_n) and (b_n) are statistically null sequences which are bounded. Then

$$\frac{1}{n}\sum_{k=1}^{n} x_k y_{n-k+1} = LM + \frac{1}{n}\sum_{k=1}^{n} a_k b_{n-k+1} + \frac{M}{n}\sum_{k+1}^{n} a_k + \frac{L}{n}\sum_{k=1}^{n} b_k$$

By Lemma 1, the three sums on the right converge to zero. Similarly the second part follows.

Theorem 6 *Let* (x_n) *be a sequence and* $K = \{k_i : i \in N\} \subset N$ *be such that* $\delta(K) = 1$ *and* $\lim_{i\to\infty} \frac{x_{k_{i+1}}}{x_{k_i}} = L$ *, then* stat-lim $x_n = 0$ if $|L| < 1$.

Proof Let (x_n) be a sequence and $K = \{k_1 : i \in N\} \subset N$ be such that $\delta(K) = 1$ and $\lim_{1\to\infty} \frac{x_{k_{i+1}}}{x_{k_i}} = I$.

$$\Rightarrow \lim_{i\to\infty} \left| \frac{x_{k_{i+1}}}{x_{k_i}} \right| = |L|$$

Then for any $\epsilon > 0$ there exists n_0 such that $\left|\frac{x_{k_{i+1}}}{x_{k_i}}\right| \prec |L| + \epsilon$ for all $k_n > n_0$. Since $|L| < 1$, so we can have $\epsilon > 0$ such that $|L| + \epsilon = \lambda < 1$. Thus we have $\frac{|x_{k_{i+1}}|}{|x_{k_i}|} < \lambda$ for all $k_n > n_0$. Now replacing n by $n, n+1, n+2, \cdots, n+p$ successively and on multiplying we have

$$\frac{|x_{k_{n+P}}|}{x_{k_n}} \prec \lambda^p$$

$$\begin{aligned} &\Rightarrow \ |x_{k_{n+p}}| \to 0, \quad \text{as} \quad p \to \infty \\ &\Rightarrow \ x_{k_n} \to 0, \quad \text{as} \quad n \to \infty \\ &\Rightarrow \ (x_n) \ \text{ is a statistically null sequence} \end{aligned}$$

Similarly the other case follows.

Theorem 7 *Let (x_n) and (y_n) be bounded statistically null sequences such that (y_n) is positive and statistically strictly monotonic decreasing, then there exists a subset $K = \{k_i : i \in N\} \subset N$ such that $\delta(K) = 1$ and*

$$\lim_{i\to\infty} \frac{x_{n_i}}{y_{n_i}} = \lim_{i\to\infty} \frac{x_{n_i} - x_{n_{i+1}}}{y_{n_i} - y_{n_{i+1}}}$$

Proof By Lemma 2, let K_1 be the set on which (x_n) is a null sequence. By definition let K_2 be the set on which (y_n) is statistically strictly monotonic increasing and is a null sequence. Let $K = K_1 \cap K_2$. Then $\delta(K) = 1$ and on $K, (x_n)$ and (y_n) satisfy all the conditions of Lemma 3. Thus the result follows.

Now we state the statisticalanalogue of a result on convergent sequences.

Proposition 8 *If (y_n) is a statistically monotonic sequences divergent to ∞ with $y_n \neq 0$ for all n and (x_n) is any sequence, then there exists a subset $K = \{n_i : i \in N\} \subset N$ such that $\delta(K) = 1$ and*

$$\lim_{i\to\infty} \frac{x_{n_i}}{y_{n_i}} = \lim_{i\to\infty} \frac{x_{n_i} - x_{n_i}}{y_{n_{i+1}} - y_{n_i}}$$

The following result follows from Lemma 2 and Cauchy's Second Theorem on limits.

Proposition 9 *Let (x_n) be a number sequence such that $x_n > 0$ for all n, then*

$$stat - \lim \frac{x_{n+1}}{x_n} = stat - \lim(x_n)^{1/n}, \quad if\ it\ exists$$

REFERENCES

[1] Buck, R. C. *Generalised asymptotic density*, Amer.Jour.Math., 75 (1953), 335-346.

[2] Conner, J. S. *The statistical and strong p-Cesaro convergence of sequences*, Analysis 8 (1998), 47-63.

[3] Das, G. and Pattanayak, S. *Fundamentals of Mathematical Analysis*, Tata McGraw Hill Publ. Company Ltd. 1987.

[4] Fast, H. *Sur la convergence statistique*, Colloq. Math. 2 (1951).

[5] Fridy, J. A. *On statistical convergence*, Analysis, 5 (1985), 301-313.

[6] —–, *Statistical limit points*,Proc. Amer. Math. Soc. Vol. 118, no. 4 (1993), 1187-1192.

[7] Maddox, I. J., *Statistical convergence in a locally convex sequence space*, Math. Proc. Camb. Phil. Soc., 104 (1998), 141-145.

[8] Rath, D. and Tripathy, B.C., *On statistically convergent and statistically Cauchy sequences*, Ind. Jour. Pure & Appl. Math., 25 (4) (1994), 381-386.

[9] Šalăt, T., *On statistically convergent sequences of real numbers*, Math. Slovaca, 30, no.2(1980), 139-150.

[10] Schoenberg, I. J., *The integrability of some functions and related summability methods*, Amer. Math. Monthly, 66 (1959), 361-375.

[11] Tripathy, B.C. *Matrix transformations between some classes of sequences*, Jour. Math. Analysis & Appl. 205, no.2 (1997), 448-450.

[12] ——, *On statistically convergent sequences*, Bull. Calcutta Math. Soc., 90(4), (1998), 259-263).

[13] ——,*On statistical convergence*, Proc. Estonian Acad. Sci. Phy. Maths., 47 (4), (1998), 299-303.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 73–82

ON A GENERATION OF THE FERMAT EQUATION

B. G. Sloss
Department of Mathematics
The Royal Melbourne Institute of Technology
GPO Box 2476V
Melbourne 3001
Victoria, Australia
Fax: +61 3 9660 1748
E-mail: rmabs@gauss.ma.rmit.edu.au

(Received 24 August, 1998)

ABSTRACT New results are obtained concerning natural number solutions of the Diophantine equation $z^t = x^r + y^s$. Bounds are found on the exponents of this equation. Evidence is provided supporting the conjecture that if $(x, y) = (y, x) = (x, z) = 1$ then there are no solutions to this equation for $r, s, t \geq 3$. It is shown that the equation has no solutions for $r = t \geq \phi(y) + 1$ and $s < \phi(y) \log_y z$ when $(x, y) = (y, z) = 1$, where ϕ is Euler's totient function. Proof is given that if (x, y, z) also satisfies the equation $x^2 + y^2 = z^p$ then min $(pr/4, ps/4) \leq t \leq$ max $(pr/2/, ps/2)$. Also, an analogue of a theorem of Sophie Germain, concerning Fermat's Last Theorem, is given for the above equation.

AMS subject classification: Primary 11D41; Secondary 11D75.

Key words and phrases Generalized Fermat equation, Diophantine equation, Sophie Germain's theorem.

1. INTRODUCTION

The aim of this paper is to study the Diophantine equation

$$z^t = x^r + y^s \tag{1}$$

Conditions on solutions to this equation are derived. This paper provides evidence in favour of the conjecture that there does not exist a solution to equation (1) for $r, s, t > 2$ and $(x, y) = (y, z) = (z, x) = 1$. However, this conjecture appeares to be extremely difficult to prove, as it is generalization of Fermat's last theorem. The conjecture is discussed in [1], [5] and [6]. It is known that there are only a finite number of solutions for $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$ to equation (1), where $(x, y) = (y, z) = (z, x) = 1$, by a result of Darmon and Granville [1] (see[6]). Nevertheless, from Fermat's last theorem (see[9], [12]) we may assume that r, s and t do not have any common factor.

The results obtained herein are different from those of the well known paper by Darmon and Granville [1].

There has been interest about the problem of showing that when equation (1) has a solution (x, y, z) then there do not exist natural numbers r_1, s_1, t_1, which do not coincide with r, s or t in equation (1) such that

$$z^{t_1} = x^{r_1} + y^{s_1} \tag{2}$$

with particular conditions placed on x, y and z. For example, in 1956 Sierpinski [8] showed that if $x = 3$, $y = 4$ and $z = 5$ then equation (1) has only the solution $(r, s, t) = (2, 2, 2)$. Furthermore, Jesmanowicz [4] proved that the only positive integral solutions for equation (1) satisfying $(x, y, z) = (5, 12, 13)$ or $(7, 24, 25)$ or (9, 40, 41) or (11, 60, 61) are given by $(r, s, t) = (2, 2, 2)$ and the conjectured that if (x, y, z) are Pythagorean triples, i.e. natural numbers satisfying equation (1) with $(r, s, t) = (2, 2, 2)$, then equation (1) only has the solution $(r, s, t) = (2, 2, 2)$. Le partially proved Jesmanowicz's conjucture in [3]. Later Terai [10] conjectured that if $r, s, t \geq 2$ then for any (r_1, s_1, t_1) satisfying equation (2) then $r = r_1, s = s_1, t = t_1$, where suitable conditions must be placed on x, y and z.

Of a similar nature, Terai [11] conjectured that the equation

$$c^z = z^2 + b^y, \qquad x, y, z, b, c \in N$$

has only the solution $(x, y, z) = (a, 2, 2)$ where $a^2 + b^2 = c^2$. This conjecture was partially proved by both Le [2] and Terai [11].

This paper is arranged as follows. First, elementary methods are applied to equation (1). Then bounds are found on the exponents of this equation, which must be satisfied for a solution to exist. These bounds are proved by applying basic properties of Euler's totient function. The bounds are applied in Theorem 3, where it is proved that, in particular, equation (1) has no solution for $r = t \geq \phi(y)+1$ and $s < \phi(y) \log_y, \ z$, when $(x, y) = (y, z) = 1$, thus providing evidence in favour the conjecture generalizing Fermat's last theorem which was mentioned above. Theorems 4 and 5 contribute to the verification of the conjecture of Terai, by showing that if equation (1) and the equation $x^2+y^2 = z^p$ have common solutions then the constraint min $(pr/4, ps/4) \leq t \leq$ max $(pr/2, ps/2)$ must hold, where $p, r, s \geq 2$. The conditions for the solvability of this latter equation are given in Proposition 8.1 of [1]. However, this result is of of a different character to our result.

Finally, we prove Theorem 6, which is an anologue of a theorem of Sophie Germain. This proof is based on proofs of results due to Powell [7] and can be considered an application of his methods to equation (1). Nevertheless, we require the following conjecture to hold as a prerequisite for Theorem 6 to hold.

Conjecture A Assume that r, s and t are greater than 2 and that a solution (x, y, z) exists to equation (1) then there exists a positive constant c such that $x < c$, $y < c$ and $z < c$, where c is independent of r, s and t.

Note that results from the paper by Powell [7] are required for the proof of this Theorem 6. We have not able to prove Conjecture A at present, but it appears to be probable given the aforementioned result of Darmon and Granville.

A common after theorem 6 indicates that information to the asymptotic behaviour of solutions to the equation, which is considered in Theorem 6, can be obtained independently of Conjecture A.

In the following we let $N = \{$ non zero positive integers $\}$. In the sequel we assume $r, s, t, K, x, y, z \in N$ and let ϕ denote Euler's ϕ - function.

2. RESULTS INVOLVING EULER'S FUNCTION

The possibility of some special solutions to equation (1) are excluded by elementary considerations as in the following Theorem 1.

Theorem 1 *Equation (1) has no solution for* $(y, t) = (x, t) = 1$, $\ x \equiv z \pmod t$

) and $r = t + K\phi(t)$.

Proof Assume (1) holds then $y^s \equiv x^t(1 - x^{K\phi(t)}) \equiv 0 \pmod{t}$; a contradiction. $\Box$.

We give a simple corollary, for the special case when $t = p$, for p a prime natural number.

Corollary If $p \in N$ is a prime then there is no solution to the Diophantine equation

$$z^p = x^{p^2} + y^s, \quad \text{where}$$

$$x \equiv z \quad (\mathrm{mod} p),\ (x,p) = (y,\rho) = 1,\ s \in N$$

Proof Follows immediately from Theorem 1, by setting $K = p\Box$

Note that for equation (1) to hold $z^{t-\phi(x^r)}$ may not be an integer for z sufficiently large. After taking the lorarithms of both sides of equation (1), this may be shown as follows: Assume $x^r > y^s$ then, let n be the number of distinct prime factors of x. For $\log z > 2^{n+1}$, we have $t < 2\log_x x^r < \frac{2x^r}{\log z} < \frac{x^r}{2^n} \leq \phi(x^r)$. In the sequel, this limits the test of whether or not $z^{t-\phi(x^r)}$ is a natural number to small values of z.

In the following theorems bounds are found on the exponents of equation (1). These results are consequences of Euler's generalization of the lesser Fermat theorem. Only part 2 of this theorem will be used later.

Theorem 2 The following hold:

1. *If $(x,y) = (y,z) = 1$ and $x^{r-K\phi(y)} - z^{t-K\phi(y)} \in N$ then equation (1) satisfies $t\log_x z > r > \log_x y + K\phi(y)$.*

2. *If $t \leq r$, $(x,y) = (y,z) = 1$ and $z^{1-K\phi(y)} - x^{r-K\phi(y)} \in N$ then equation (1) implies thatt $\log_y z > s \geq K\phi(y)\log_y z$.*

3. *There is no solution to equation (1) for $(x,y) = (y,z) = 1$, $z > x$ and $z^{t-\phi(y^s)} - x^{r-\phi(y^s)} \in N$.*

4. *Equation (1) has no solution $(y,z) = 1$ and $x^r - z^{t-\phi(y^s)} \in N$ with $y^s \geq x^r$*

Proof We prove case 2, the other cases are proved similarly. Case 1 is proved directly and cases 3 and 4 are proved by contradiction. Firstly, note $z > x$ because $\log z > \frac{r}{t} \log x \geq x$. There exists $N_2 \in N$ such that

$$z^{t-K\phi(y)} - x^{r-K\phi(y)} = N_2 y$$

After multiplying both sides of this equation by $z^{K\phi(y)}$ we get

$$z^t = z^{K\phi(y)} x^{r-K\phi(y)} + N_2 y z^{K\phi(y)} > x^r + N_2 y z^{K\phi(y)}$$

So $y^s > N_2 y z^{K\phi(y)} > y z^{K\phi(y)}$. These inequalities constitute a contradiction unless $s - 1 > K\phi(y) \log_y z$. The remaining inequality follows since $z^t > y^s$.□

Corollary *There are no solutions of equation (1) for* $y = 2$, x, z *odd,* $t < r, r, t \geq 2$, $s < \log_2 z$ *and* $\log_x z > \frac{r-1}{t-1}$.

Proof $r, t \geq 2$ and $\log_x z > \frac{r-1}{t-1}$ ensure that $z^{t-1} - x^{r-1} \in N$.□

The following theorem, Theorem 3, provides evidence in favour of the generalization of Fermat's last theorem, which is mentioned above. Theorem 3 roughly expressed indicates that if $r = t$ and $\log_x z$ are large when compared with $\phi(y)$ and s is small with respect to $\phi(y)$ then there are no solutions to equation (1).

Theorem 3 *If* $(x, y) = (y, z) = 1$ *then there are no solutions to equation (1), when*

$$\log_x z + K\phi(y) > r \geq t \geq K\phi(y) + 1,$$

where

$$s < K\phi(y) \log_y z + 1$$

In particular, if $(x, y) = (y, z) = 1$, $r = t > \phi(y) + 1$ *and* $\log_x z > \phi(y) + 1$ *then there are no solutions to equation (1) for* $s < \phi(y) \log_y z + 1$.

Proof Assume $t - K\phi(y) \geq 1$, $r \geq t$ and $(x, y) = (y, z) = 1$ then $z^{t-K\phi(y)} - x^{r-K\phi(y)} \geq z - x^{r-K\phi(y)} > 0$, providing $\log_x z + K\phi(y) > r$. Therefore the conditions of Theorem 2 part 2 are satisfied. So no solution exists of equation (1) when $s < K\phi(y) \log_y z + 1$.

Following from above, if $\log_x z + (K-1)\phi(y) + 1$ for all $K \in N$, which occurs if and only if $\log_x z > \phi(Y) + 1$, then there are no solutions of equation (1) for $r = t > \phi(y)+1$, $s < \phi(y)\log_y z+1$ and $(x,y) = (y,z) = 1$, because the intervals, $[\log_x z + K\phi(y),\ K\phi(y)+1]$, overlap. □

3. ON TERAI'S CONJECTURE

The following two theorems provide constraints on t in equation (1) in terms of s, r and p, where x, y and z also satisfy $x^2 + y^2 = z^p$.

Theorem 4 *If $x^2+y^2 = z^p$ then equation (1) has no solution for $t >$ max $(pr/2, ps/2)$, where $r, s, p \geq 2,\ p, x, y, z \in N$.*

Proof Suppose there exists $x, y, z \in N$ such that $x^2 + y^2 = z^p$ and $x^r + y^s = z^t$. Then after eliminating z from these equations, we obtain the equation

$$(x^2 + y^2)^{t/p} = x^r + y^s \tag{3}$$

Now consider the two forms $f(X,Y) = (X^2+Y^2)^{t/p}$ and $g(X,Y) = X^r + Y^s$. Then $g(1,1) = 2 \leq 2^{t/p} = f(1,1)$. Let $fx(X,Y)$ denote the partial derivative of f with respect to X evaluated at the point (X,Y), and similarly define f_Y, g_X and g_Y. So $f_X(X,Y) = \frac{2Xt}{p}(X^2+Y^2)^{\frac{t-p}{p}} > rX^{r-1} = g_X(X,Y)$ for $X, Y > 1$ and $\frac{2t}{p} > r$ (which is equivalent to $t > \frac{pr}{2}$). Similarly for $t > \frac{ps}{2}, f_Y(X,Y) > g_Y(X,Y)$ and $X, Y > 1$. Consequently, f does not meet g for any real values of X and Y which are greater than 1. So, there are no natural number solutions to equation (3). □

Theorem 5 *If $x^2+y^2 = z^p$ then equation (1) has no solution for $t <$ min$(pr/4, ps/4)$, where $p \geq 2$ and $p, x, y, z \in N$.*

Proof Firstly, note that z^p is not equal to 2 for z an integer, therefore we may assume that both x and y do not equal 1. Now we show that there are no solutions to both of the equations.

$$1 + y^2 = z^p \qquad \text{and} \qquad 1 + y^s = z^t \tag{4}$$

where $t < \frac{sp}{4}$. We may assume that y is not equal to 2, since 5 is not equal to z^p for

z an integer. Assume equation (4) has a solution, then eliminating z from equation (4) we find that $(1+y^2)^t = (1+y^s)^p$. But $(1+Y^2)^{\frac{t}{p}} < (2Y^2)^{\frac{t}{p}} < Y^{\frac{3t}{p}} < 1+Y^s$ for $t < \frac{sp}{3}$ and $Y > 2$ a real number; which is a contradiction. Similarly, a similar contr adiction applies to equations involving the variable r. Hence, we may assume $x, y \geq 2$.

We argue similarly to Theorem 4. If Theorem 5 is false then there exists $x, y, z \in N$ such that

$$x^{2t} = (z^p)^{\frac{2t}{p}} = (x^2+y^2)^{\frac{2t}{p}} = (x^r+y^s)^2$$

As above consider $f(X,Y) = (X^2+Y^2)^{\frac{2t}{p}}$ and $g(X,Y) = (X^r+Y^s)^2$. The partial derivatives of f and g are denoted similarly to above.

We use the fact that $X^2+Y^2 < X^2Y^2$ for $X, Y \geq 2$. So that

$$\begin{aligned} f_X(X,Y) &= 2X\frac{2t}{p}(X^2+Y^2)^{\frac{2t-p}{p}} \\ &< 2X\frac{2t}{p}(XY)^{\frac{2}{p}(2t-p)} \\ &< 2rX^{r-1}(X^r+Y^s) \\ &= g_X(X,Y) \quad \text{if} \end{aligned}$$

$\frac{4t}{p} < r, \frac{2}{p}(2t-p) < s$ and $\frac{2t}{p} < r$. A similar inequality holds between f_Y and g_Y, and both inequalities hold for $t < \min(pr/4, ps/4)$. Also, $f(2,2) = 2^{\frac{6t}{p}} < 2^{2r} < (2^r+2^s)^2 = g(2,2)$ if $t < \frac{pr}{4} < \frac{pr}{3}$. So the theorem follows. □

4. AN ANALOGURE OF S. GERMAIN'S THEOREM

In the following theorem we prove a result similar in nature to a classical result of Sophie Germain (see [6]). Our result follows from Conjecture A by a method due to Poweel [7].

Theorem 6 *If we assume Conjecture A holds then for any even integer m for which $3\phi(m) > m$, if n is any positive odd integer sufficiently large for which $mn + 1 = q$, where q is a prime, then equation (1) has no solution in natural numbers x, y, z such that $r = n + r''$, $s = n + s''$ and $t = n + t''$, where $r'', s'', t'' \in N, (x,y) = (y,z) = (x,z) = 1$ and $2r'', 2s'', t'' < n.r'', s''$ and t'' are independent of n and $r'', s'' > t''$.*

Proof The proof follows the proof of Theorem 2 of Poweel [7]. Lemma 1 is a modification of the Lemma in Theorem 2 and Powell [7]. Lemma 1 is proved using the techniques of the proof of this lemma of Powell but assuming Conjecture A.

Lemma 1 *For any even integer m for which $3\phi(m) > m$, for any integers r_2, s_2 and t_2 for which $0 \leq r_2, s_2, t_2 < m$, and any prime number q sufficiently large, there does not exist an integer a which belongs to the exponent m (mod q) and for which $g(a) \equiv x^{r''}a^{r_2} \pm y^{s''}a^{s_2} \pm z^{t''}a^{t_2} \equiv 0$ (mod q. x, y, z, r'', s'', t'' are defined as above. The same holds true if $g(a) \equiv x^{r''}a^{r_2} \pm y^{s''}a^{s_2}$, $x^{r''}a^{r_2} \pm z^{t''}a^{t_2}$ and $y^{s''}a^{s_2} \pm z^{t''}a^{t_2}$, r'', s'' and t'' are defined in Theorem 6.*

Proof of Lemma 1 For Lemma 1 to hold we must show that the following four cases do not hold:

1. $x^{r-n} \equiv y^{s-n} + z^{t-n}$;
2. $x^{r-n} \equiv -y^{s-n} - z^{t-n}$;
3. $x^{r-n} \equiv -y^{s-n} + z^{t-n}$;
4. $x^{r-n} \equiv y^{s-n} - z^{t-n}$.

Firstly, we may assume $y > x$ by the symmetry of equation (1). Now $t \log z > s \log y$, from equation (1). So $\log z > \frac{s}{t} \log y > \log y$, since $s > t$. Thus $z > y$. Case 2 is false since the LHS > 0 and RHS < 0; a contradiction. Multiply both sides of the equation for case 1 by x^n and y^n. Therefore, $x^r = x^n(y^{s-n} + z^{t-n})$ and $y^s = y^n(x^{r-n} - z^{t-n})$. Sor from equation (1), $z^t = y^{s-n}x^{r-n}(x^{2n-r} + y^{2n-s}) + (x^n - y^n)z^{t-n}$. Thus, $z^{t-n}(z^n + y^n_z - x^n) = y^{s-n}x^{r-n}(x^{2n-r} + y^{2n-s}$. Since $(xy, z) = 1$, we have that $z^{t-n} = x^{2n-r} + y^{2n-s}$. Consequently, $z^t = z^n(z^{2n-r} + y^{2n-s}) > x^{3n-r} + y^{3n-s} > x^r + y^s = z^t$; a contradiction. As above, multiply both sides of the equation in case 3 by x^n. Thus, we obtain that $x^r = x^n(z^{t-n} - y^{s-n}) = z^t - y^s$, which is equivalent to $z^{t-n}(x^n - z^n) = y^{s-n}(x^n - y^n)$. Since $(y, z) = 1$ we have that $z^{t-n} = y^n - x^n$ and $y^{s-n} = z^n - x^n$. After substituting these resulting equations into the equation for case 3, we find that $x^{r-n} = y^n - z^n$. Therefore, $y > z$. But $x > y$; a contradiction. Now multiply the equation for case 4 above by x^n. We obtain that $y^{s-n}(x^n + y^n) = z^{t-n}(x^n + z^n)$. So, since $(z, y) = 1$, we have that $y^{s-n} = x^n + z^n < y^n$ and $z^{t-n} = x^n + y^n < z^n$. Subsituting the above expressions into the equation for case 4, we obtain that $x^{r-n} = z^n - y^n < x^n$. But then $x^n + y^n > z^n > z^n + y^n$; a contradiction. □

End of Proof of Theorem 6 The remainder of the proof is similar to the proof of Theorem 2 of Poweel [7]. Firstly, assume solutions (x, y, z) exist satisfying the conditions of the theorem. From Powell [7], the group of $\frac{q-1}{m}$ th power residues modulo q, is isomorphic modulo q to the cyclic group modulo q with m elements denoted by $\{a^i : a^m \equiv 1 \pmod q\}$ for some integer a. Thus if q does not divide xyz we have: $x^{r''}x^{\frac{q-1}{m}} \equiv x^{r''}a^{r_2} \pmod q$, $y^{s''}y^{\frac{q-1}{m}} \equiv y^{s''}a^{s_2} \pmod q$, $z^{t''}z^{\frac{q-1}{m}} \equiv z^{t''}a^{t_2}$ $\pmod q$, for some integers. So we have

$$x^{r''}a^{r_2} \pm y^{s''}a^{s_2} \pm z^{t''}a^{t_2} \equiv 0 \pmod q \tag{5}$$

From Lemma 1 the congruence (5) is impossible. Hence $a|xyz$, but we may choose $q > xyz$; a contradiction. □

Note that, by the method of proof of Theorem 6, any set of bounded triples of natural numbers, $A = \{(x, y, z) : x, y, z, c \in N, x, y, z < c\}$, also has the property that for any even integer m, for which $3\phi(m) > m$, if n is any positive odd integer sufficiently large for which $mn + 1 = q$, q a prime natural number, then none of the triples (x, y, z) is a solution of equation (1), where r, s and t are given as in Theorem 6. In this case q, and hence n, depends on the set A.

REFERENCES

[1] Darmon, H. and Granville, A. *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*. Bull. London Math. Soc. 27, (1995) 513-543.

[2] Le, M. *A note on the diophantine equation $x^2 + b^y = c^z$*, Acta Arith., 71, (1995) 253-257.

[3] Le, M. *A note on Jesmanowicz conjecture*, Colloquim Mathematicum, 69, (1995) 47-51.

[4] Jesmanowicz, L. *Kilka uwag o liczbach pitagorejskich,* [Some remarks on Pythagorean numbers], Wiadom. Mat., 1, (1956) 196-202.

[5] Murty, V. K. *Seminar on Fermat's last theorem*, AMS, Providence, Rhode Island, 1995.

[6] van der Poorten, A. *Notes on Fermat's Last Theorem*, Wiley, New York 1996.

[7] Powell, B. J. *Proof of the impossibility of the Fermat equation* $X^p + Y^p = Z^p$ *for special values of* p *and the more general equation* $bX^n + cY^n = dZ^n$, J. Number Theory, 18, (1984) 34-40.

[8] Sierpinski, W. *O rownaniu* $3^x + 4^y = 5^z$ *[On the equation* $3^x + 4^y = 5^z$*]*, Wiadow. Mat., 1, (1956) 194-195.

[9] Taylor, R. and Wiles, A. *Ring-theoretic properties of certain Hecke algebras*, Annals of Math., 141, (1995) 553-572.

[10] Terai, N. *The Diophantine Equation* $a^x + b^y = c^z$, Proc. Japan Acad., 70, Ser. A (1994) 22-26.

[11] Terai, N. *The Diophantine equation* $x^2 + q^m = p^n$, Acta Arith., 63 (1993) 351-358.

[12] Wiles, A. *Modular elliptic curves and Fermat's last theorem*, Annals of Math., 142, (1995) 443-551.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii (2000) pp. 83–104

BOOLEAN ALGEBRA WITH FUZZY SHELL AND GR_*-DANGEROUS SIGNAL RECOGNITION LOGIC [1]

Zheng Yalin, Zhang Winxiu
Institute of Information and System Science
Faculty of Science
Xi'an Jiaotong University
Xi'an, 710049
The People's Republic of China

(Received 19 November, 1998)

ABSTRACT In this paper, the new concept of Boolean algebras with Fuzzy shell is proposed, some important examples are given. A new implication operator, **Z**-implication operator, and a new kind of valuation lattices, **Z**-valuation lattices are made. And then, a new kind of nonclassical logic systems are established, the properties of this logic are investigated, some interesting results are obtained. Especially, it is discovered that for every α in this paper α **HS** and and α-**MP** must hold unconditionally.

Key Words Fuzzy logic; Boolean algebra with Fuzzy shell, Boolean heart; $\mathbf{GR}_*$- implication operator; $\mathbf{GR}_*$-valuation lattice; α-tautology; $\mathbf{GR}_*$-Dangerous signal recognition logic; Approximate reasoning; Control principle.

1. INTRODUCTION In order to give a strict logic foundation of fuzzy control and fuzzy reasoning, literatures [1-6] have established a new fuzzy logic system L^*, and linked the system with the kenel problems, Fuzzy modus Ponens and Fuzzy Modus Tollens, of fuzzy control and fuzzy reasoning meaningfully, thus provided a strong logic support for them. In the new fuzzy propositional logic system

[1]This project is supported by the Science and Technology Commission of Shaanxi Province (98-SL08)

L^*, the throught of semantic with degree is absorbing, such as $\sum-(\alpha$- tautology $)$[1-4], $\sum-(\alpha-\mathrm{MP})$ rule [1-3], $\sum-(\alpha-$ **HS**) rule [1-3], $\alpha-3\mathbf{I}$ algorithm [1-4], sustentation degree [1,4] theory and so on.

On the other hand, a variety of nonlinear ordered 6-valued logic system $K\frac{1}{6}$ has been used in dangerous signal recognition of circuit design successfully, but the investigation of its mathematical foundation is still immature. For the reason of lacking suitable implication operator the investigation of its semantic has not been found.

Enlightening by new fuzzy propositional logic and the limitation of 6-valued system $K\frac{1}{6}$ this paper deals with the generalization of $K\frac{1}{6}$ in amore general sense. We'll first propose the new abstract concepts of Boolean algebra with Fuzzy shell, its Boolean heart, its Fuzzy shell. Then We'll give some examples of this kind of lattices. Secondly, a new implication operator, $\mathbf{GR}_*-$ implication operator, is made, and a new valuation lattice, $\mathbf{GR}_*$ -valuation lattice, $\mathbf{GR}_*$ -valuation lattice as valuation lattice, and is called a $\mathbf{GR}_*$-dangerous signal recognition logic, is established. We'll give an elementary investigation of the logic system. Especially, We'll investigate the semantic of this logic and obtain some interesting results.

Our new logic system can be fractionized into two fragments, the Boolean heart, the Fuzzy shell. There will be two kind of logic structures with different and distinguished styles features and in our system, a kind of Gaines-Rescher logic systems based on usual Boolean algebras, and another kind of Fuzzy logic systems which takes Gaines-Rescher operator as the implication operator and based on extensive Fuzzy lattices. Of cause, there exist many complicated situations in the investigation of transfragments, it is a interesting attractor in this logic systems. We'll discover that for every α in the logic, both α-**HS** and α -**MP** must hold unconditionally.

2. BOOLEAN ALGEBRA WITH FUZZY SHELL First, we are going to establish the new concept of Boolean algebra with Fuzzy shell, give some examples of this algebra, and discuss the special properties.

Definition 2.1 A distributive lattice L is called a *Boolean algebra with Fuzzy shell*, if following conditions are satisfied:

(1) L has the greatest element 1 and the least element 0.

(2) L has an order-reversing involution $\neg$.

(3) L has an unigue maximal Boolean type sublattice $L^\#$ such that the greatest element $1^\#$ and the least element $0^\#$ are different with 1 and 0 respectively, and the restriction of $\neg$ on $L^\#$ just coincide with the Boolean complement' in $L^\#$.

$L^\#$ is called the *Boolean heart* of $L, \tilde{L} = L - L^\#$ is called the *Fuzzy shell* of L.

Example 2.2

(1) Suppose that B is any arbitrary Boolean algebra, $1^\#$ and $0^\#$ are the greatest element and the least element of B. Let $L = \left[0, \frac{1}{3}\right] \cup B \cup \left[\frac{2}{3}, 1\right]$, take usual ordering of real numbers in $\left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right]$. If $x \in \left[0, \frac{1}{3}\right]$, $y \in B$, $z \in \left[\frac{2}{3}, 1\right]$, then let, $x < y < z$. $\forall y \in B$, let $\neg\, y = y'$;$\forall x \in \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right]$, let $\neg\, x = 1 - x$. Then L is just a Boolean algebra with Fuzzy shell, where $L^\# = B$ is just the Boolean heart, and $\tilde{L} = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right]$ is just the Fuzzy shell.

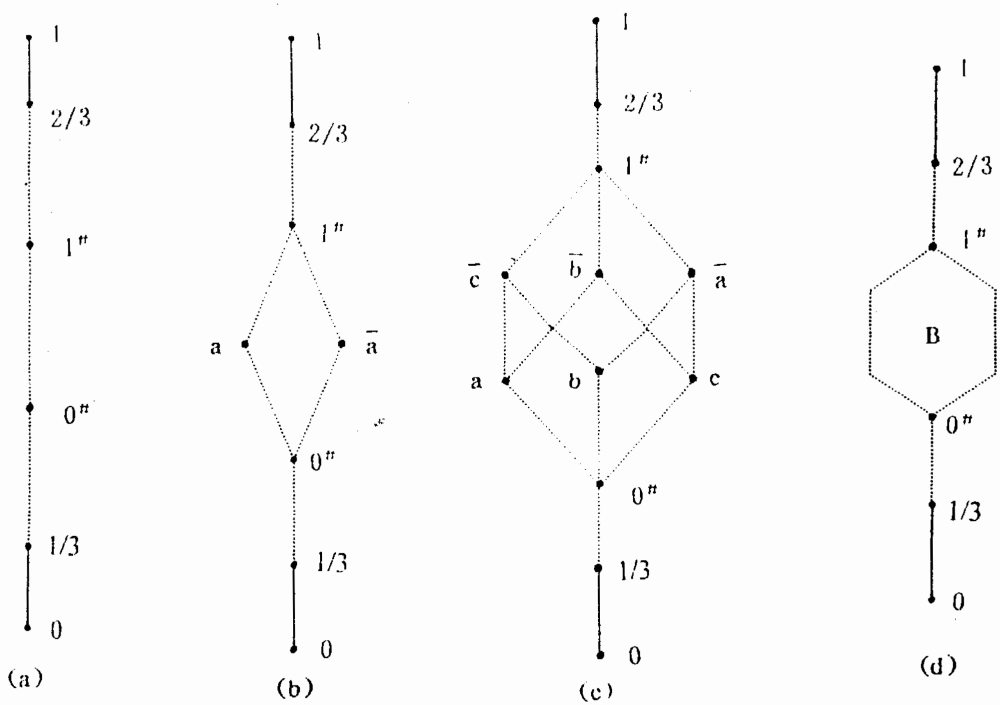

Figure 1. Boolean algebras with Fuzzy shell.

(a) Boolean heart: 2^1; Fuzzy shell: infinite.

(b) Boolean heart: 2^2; Fuzzy shell: infinite.

(c) Boolean heart: 2^3; Fuzzy shell: infinite.

(d) Boolean heart: $2^{|B|}$; Fuzzy shell: infinite.

There are some examples of Boolean algebras with Fuzzy shell in Figure 1, their Boolean hearts contain $2^1, 2^2, 2^3, \cdots, 2^{|B|}$ elements respectively, their Fuzzy shells are all infinite aggregations.

(2) Suppose that B is any arbitrary Boolean algebra, $1^\#$ and $0^\#$ are the greatest element and the least element of B respectively. Take $1.\ 0 \notin B$, denote $L = B \cup \{0,1\}$. $\forall x \in B$, let $0 < x < 1$; $\forall x \in B$, let $\neg x = x'$; and let $\neg 0 = 1, \neg 1 = 0$. Then L is just a Boolean algebra with Fuzzy shell, where $L^\# = B$ is just the Boolean heart, and $\tilde{L} = \{0,1\}$ is just the Fuzzy shell.

Figure 2 give such examples, their Boolean hearts also contain $2^1, 2^1, 2^3, \cdots, 2^{|B|}$ elements respectively, but their Fuzzy shells only contain two elements uniformly.

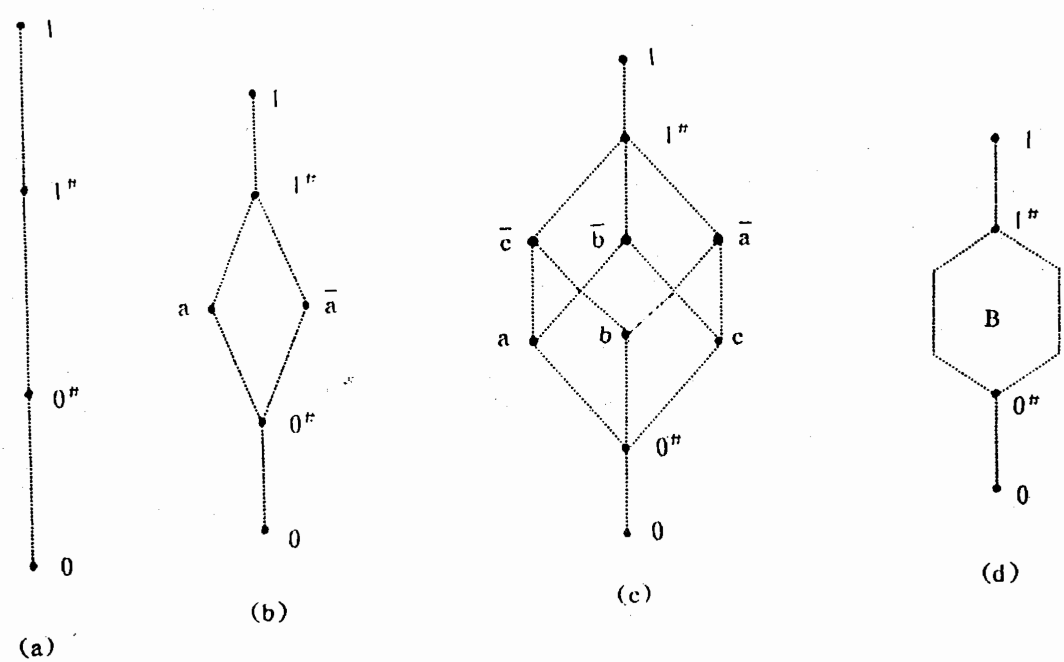

Figure 2. Boolean algebras with Fuzzy shell

(a) Boolean heart: 2^1; Fuzzy shell: 2.

(b) Boolean heart: 2^2; Fuzzy shell: 2.

(c) Boolean heart: 2^3; Fuzzy shell: 2.

(d) Boolean heart: $2^{|B|}$; Fuzzy shell: 2.

Lemma 2.3 In any Boolean algebra with Fuzzy shell, de Morgan dual laws hold:

(1) $\rightharpoondown (a \vee b) = \rightharpoondown a \wedge \rightharpoondown b$.

(2) $\rightharpoondown (a \wedge b) = \rightharpoondown a \vee \rightharpoondown b$.

Proposition 2.4 Suppose that L is a Boolean algebra with Fuzzy shell, $L^\#$ and $\tilde{L}$ are the Boolean heart and the Fuzzy shell respectively, then

(1) For every $x \in L, \rightharpoondown x \vee x \geq 1^\#, \rightharpoondown x \wedge x \leq 0^\#$
(2) For every $x \in L^\#, \rightharpoondown x \vee x = 1^\#, \rightharpoondown x \wedge x = 0^\#$
(3) For every $x \in \tilde{L}, \rightharpoondown x \vee x \leq 1, \rightharpoondown x \wedge x \geq 0$
(4) $\rightharpoondown 1 = 0, \rightharpoondown 0 = 1; \rightharpoondown 1^\# = 0^\#, \rightharpoondown 0^\# = 1^\#$

Proposition 2.5 In any Boolean algebra L with Fuzzy shell, does not exist any element e such that

$$\rightharpoondown e = e$$

Proof Suppose that there exists an element $e \in L$ such that $\rightharpoondown e = e$, then

$$\begin{aligned} e &= \rightharpoondown e \vee e \geq 1^\#, \\ &= \rightharpoondown e \vee \leq 0^\# \end{aligned}$$

But $1^\# \neq 0^\#$. This is a contradictory.

Note 2.6 Any Boolean algebra is not a Boolean algebra with Fuzzy shell. Any Boolean algebra with Fuzzy shell is not a Boolean algebra. But the Boolean heart

$L^{\#}$ of any Boolean algebra L with fuzzy shell must be a Boolean algebra, its Fuzzy shell $\tilde{L}$ is a bounded distributive latice with order reversing involution. If we deal with the Boolean heart $L^{\#}$ and the Fuzzy shell $\tilde{L}$ of a Boolean algebra L with Fuzzy shell seperately, then they obey the corresponding operation laws respectively. But our more interest is just in the combined or fused investigation.

3. ***GR***$_*$**-DANGEROUS SIGNAL RECOGNITION LOGIC** We are now going to establish a new kind of nonclassical logic, **GR**$_*$- implication operator as implication operator.

Definition 3.1 Suppose that L is a Boolean algebra with Fuzzy shell. Let us make a mapping

$$\mathbf{GR}_*: \ L \times L \to L$$

as following

$$\mathbf{GR}_*(a,b) = \begin{cases} 1, a \leq b, b \in \tilde{L}, \\ 1^{\#}, a \leq b, b \in L^{\#}, \\ 0, a \not\leq b, \end{cases}$$

and call the mapping **GR**$_*$ as **GR**$_*$-implication operator. If we take **GR**$_*$-implication operator **GR**$_*$ as the implication operator $\to$ in the Boolean algebra L with Fuzzy shell, then L is called a **GR**$_*$ -valuation lattice. A mapping $v: F(S) \to L$ is called a **GR**$_*$-valuation, if v is a homomorphism of type $\neg, \vee, \wedge, \mathbf{GR}_*$). Where $F(S)$ is the free algebra of type $(\neg, \vee, \wedge, \to)$ generated by a nonempty set S. We denote the set of all **GR**$_*$ -valuations from $F(S)$ to L by Ω_{GR_*}.

Definition 3.2 Suppose that $A \in F(S)$ and $\alpha \in L$. If for every **GR**$_*$-valuation $v \in \Omega_{GR_*}$, $v(A) \geq \alpha(A) > \alpha, v(A) > 0, v(A) = 1,\ v(A) = 1^{\#}, v(A) = 0^{\#}$, then the proposition A is called an α-tautology (a^+ -tautology, pretautology, tautology, $\hat{1}^{\#}$-tautology, $\hat{0}^{\#}$-tautology).

We denote the set of all α-tautologies (α^+-tautologies, pretautologies, tautologies, $\hat{1}^{\#}$-tautologies, $\hat{0}^{\#}$ -tautologies) by $\alpha - T(Z^{\#})(a^+ - T(Z^{\#}), QT(Z^{\#}), T(Z^{\#}), T(Z^{\#}),$ $\hat{1}^{\#} - T(Z^{\#}), \hat{0}^{\#} - T(Z^{\#}))$.

Definition 3.3 The octuple $Z = (F(S)), \Omega_{GR_*}, \alpha - T, a^+ - T, T, \hat{1}^\# - T, \hat{0}^\# - T)$ is called the *semantic of* $\mathbf{GR}_*$*-dnagerous signal recognition logic* $Z^\#$.

Definition 3.4: The ordered pair $\mathbf{Z}^\# = (\mathbf{E}, \mathbf{Z})$ is called a $\mathbf{GR}_*$*-dangerous signal recognition logic*, where E is the syntax of this logic.

Proposition 3.5 For every family $\{\alpha_t | t \in D\} \subset L$, we have

$$\bigcap_{t \in D}(\alpha_t - T(\mathbf{Z}^\#)) = (\bigcup_{t \in D} \alpha_t)) - T(\mathbf{Z}^\#)$$

Note In any $\mathbf{GR}_*$-valuation lattice L, $\mathbf{GR}_*$- implication operator $\mathbf{GR}_*$ doesn't coincide with Gaines-Rescher implication operator [1]$R_{GR} : L \times L \to L$,

$$R_{GR}(a, b) = \begin{cases} 1, a \leq b, \\ 0, a \not\leq b \end{cases}$$

Because for each element of c of the Boolean heart $L^\#$, $\mathbf{GR}_*(c, c) = 1^\# \neq 1$, that is $\mathbf{GR}_*(c, c) \neq R_{GR}(c, c)$.

Proposition 3.7 In the Boolean heart $L^\#$ of a $\mathbf{GR}_*$ -valuation lattice L, the restriction of $\mathbf{GR}_*$-implication operator $\mathbf{GR}_*$ on $L^\#$ is just equivalent to the revised Gaines-Rescher impliçation operator [1]$R_{GR} : L^\# \times L^\# \to L^\#$,

$$R_{GR}(a, b) = \begin{cases} 1^\#, & a \leq b, \\ 0, & a \not\leq b, \end{cases}$$

Proposition 3.8 In the Fuzzy shell $\tilde{L}$ of a $\mathbf{GR}_*$-valuation lattice L, the restriction $\mathbf{GR}_*$ -implication operator $\mathbf{GR}_*$ on $\tilde{L}$ is just equivalent to Gaines-Rescher implication operator [1]

$$R_{GR}(a, b) = \begin{cases} 1, & a \leq b, \\ 0, & a \not\leq b, \end{cases}$$

Proposition 3.9 In a $\mathbf{GR}_*$-valuation lattice L, if $\tilde{L} = \{0,1\}$, then the restriction of $\mathbf{GR}_*$-implication operator $\mathbf{GR}_*$ on $\tilde{L}$ just equivalent to Klenne-Dienes implication operator [1]$R_{KD} : \tilde{L} \times \tilde{L} \to \tilde{L}$,

$$R_{KD}(a,b) = \rightharpoondown a \vee b$$

and is also equivalent to Wang Guojun implication operator [1]$R_0 : \tilde{L} \times \tilde{L} \to \tilde{L}$,

$$R_0(a,b) = \begin{cases} 1, & a \leq b, \\ \rightharpoondown \vee b, & a \not\leq b \end{cases}$$

Proposition 3.10 In any $\mathbf{GR}_*$-valuation lattice L, following revised Dubois-Prade conditions are satisfied:

(1) If a $\leq a^*$, then $\mathbf{GR}_*(a,b) \geq \mathbf{GR}_*(a^*,b)$

(2) $\mathbf{GR}_*, (0,b) = \begin{cases} 1, & b \in \tilde{L} \\ 1^\#, & b \in L^\# \end{cases}$ $\quad \mathbf{GR}_*(0^\#,b) = \begin{cases} 1, & b \in \tilde{L}, 0^\# \leq b, \\ 1^\#, & b \in L^\#, \\ 0, & b \in \tilde{L}, 0^\# \not\leq b \end{cases}$

(3) $\mathbf{GR}_*, (1,b) = \begin{cases} 1, & b = 1 \\ 0, & b \neq 1 \end{cases}$ $\quad \mathbf{GR}_*(1^\#,b) = \begin{cases} 1, & b \in \tilde{L}, 1^\# \leq b, \\ 1^\#, & b = 1^\#, \\ 0, & \text{otherwise} \end{cases}$

(4) If $a \leq b$, then $\mathbf{GR}_*(a,b) \geq b$. If $a \not\leq b$, then $\mathbf{GR}_*(a,b) \leq b$.

(5) $\mathbf{GR}_*, (a,a) = \begin{cases} 1, & a \in \tilde{L}, \\ 1^\#, & a \in L^\# \end{cases}$

(6) $\mathbf{GR}_*(a,b) =$ iff $a \leq b$ and $b \in \tilde{L}$.$\mathbf{GR}_*(a,b) = 1^\#$ iff $a \leq b$ and $b \in L^\#$.

Proposition 3.11 In the Fuzzy shell $\tilde{L}$ of a $\mathbf{GR}_*$ -valuation lattice L,

$$\mathbf{GR}_*(a,b) = \mathbf{GR}_*(\rightharpoondown b, \rightharpoondown a)$$

Proof Suppose that $a \not\leq b$, then $\rightharpoondown b \leq \rightharpoondown a$ and so

$$\mathbf{GR}_*(a,b) = 1 = \mathbf{GR}_*(\rightharpoondown b, \rightharpoondown a)$$

Suppose that $a \not\leqq b$, then $\neg b \not\leqq \neg a$ and so

$$\mathbf{GR}_*(a,b) = 0 = \mathbf{GR}_*(\neg b, \neg a)$$

Thus completes the proof.

Proposition 3.12 In the Boolean heart $L^\#$ of a $\mathbf{GR}_*$ -valuation lattice L,

$$\mathbf{GR}_*(a,b) = \mathbf{GR}_*(\neg b, \neg a)$$

Proof Suppose that $a \leq b$, then $\neg b \leq \neg a$ and so

$$\mathbf{GR}_*(a,b) = 1^\# = \mathbf{GR}_*(\neg b, \neg a)$$

Suppose that $a \not\leqq b$, then $\neg b \not\leqq \neg a$ and so

$$\mathbf{GR}_*(a,b) = 0 = \mathbf{GR}_*(\neg b, \neg a)$$

This completes the proof.

Note 3.13 Generally, in a $\mathbf{GR}_*$-valuation lattice L,

$$\mathbf{GR}_*(a,b) \neq 1,\ \mathbf{GR}_*(\neg b,\ \neg a) = 1^\#$$

For example, take $a \in L^\#$ and $b \in \tilde{L}$ such that $a \leq b$, then $\neg b \leq \neg a$, $\neg a \in L^\#$, and so

$$\mathbf{GR}_*(a,b) = 1,\quad \mathbf{GR}_*(\neg b, \neg a) = 1^\#$$

where $\mathbf{GR}_*(a,b) \neq \mathbf{GR}_*(\neg b, \neg a)$.

Proposition 3.14 In any $\mathbf{GR}_*$-valuation lattice L, if $b \leq a$ or $a = 0$, then

$$\mathbf{GR}_*(a, \mathbf{GR}_*(b,a)) \geq 1^\#$$

Proof If $b \leq a$ and $a \in \tilde{L}$, then

$$\mathbf{GR}_*(a, \mathbf{GR}_*(b,a)) = \mathbf{GR}_*(a, 1) = 1$$

If $b \leq a$ and $a \in L^{\#}$, then

$$\mathbf{GR}_*(a, \mathbf{GR}_*(b, a)) = \mathbf{GR}_*(a, 1^{\#}) = 1^{\#}$$

If $b \not\leq a$ and $a = 0$, then

$$\mathbf{GR}_*(a, \mathbf{GR}_*(b, a)) = \mathbf{GR}_*(a, 0) = 1$$

If $b \leq a$ and $a = 0$, then

$$\mathbf{GR}_*(a, \mathbf{GR}_*(b, a)) = \mathbf{GR}_*(0, \mathbf{GR}_*(0, 0)) = \mathbf{GR}_*(0, 1) = 1$$

This completes the proof.

Proposition 3.15 In any $\mathbf{GR}_*$-valuation lattice L,

(1) If $a \leq b$ or $b \leq a$, then

$$\mathbf{GR}_*(a, b) \vee \mathbf{GR}_*(b, a) \geq 1^{\#}$$

(2) If $a \not\leq b$ and $b \not\leq a$, then

$$\mathbf{GR}_*(a, b) \vee \mathbf{GR}_*(b, a) = 0$$

Proof Suppose that $a \leq b$ and $b \in \tilde{L}$, then $\mathbf{GR}_*(a, b) = 1$ and so

$$\mathbf{GR}_*(a, b) \vee \mathbf{GR}_*(b, a) = 1$$

Suppose that $a \leq b$ and $b \in L^{\#}$, then $\mathbf{GR}_*(a, b) = 1^{\#}$ and

$$\mathbf{GR}_*(b, a) = \begin{cases} 0, b > a, \\ 1^{\#}, b = a, \end{cases}$$

or

$$\mathbf{GR}_*(a, b) \vee \mathbf{GR}_*(b, a) = 1^{\#}$$

This completes the proof of (1). (2) is clear.

Proposition 3.16 In any $\mathbf{GR}_*$-valuation lattice $L, \rightarrow a = \mathbf{GR}_*(a, 0)$ if and only if $a \in \{0, 1\}$.

Proof Suppose that $a \notin \{0,1\}$, then $\rightharpoondown a \notin \{0,1\}$ and so $\mathbf{GR}_*(a,0) = 0 \neq \rightharpoondown a$, Therefore it follows from $\rightharpoondown a = \mathbf{GR}_*(a,0)$ that $a \in \{0,1\}$.

The proof of the rest is straightforward.

Proposition 3.17 In any $\mathbf{GR}_*$-valuation lattice L,

(1) $b \vee \mathbf{GR}_*(a,b) = b$ if and ony if $a \leq b$ or $b = 0$.

(2) $b \vee \mathbf{GR}_*(a,b) = 0$ if and only if $a \not\leqq b$ or $b = 0$,

(3) If $b \neq 0$, then $b \vee \mathbf{GR}_*(a,b) = b$ if and only if $a \leq b$.

(4) If $b \neq 0$, then $b \vee \mathbf{GR}_*(a,b) = 0$ if and only if $a \not\leqq b$

Proposition 3.18 In any $\mathbf{GR}_*$-valuation lattice L,

(1) $b \vee \mathbf{GR}_*(a,b) = \mathbf{GR}_*(a,b)$ if and only if $a \leq b$ or $b = 0$.

(2) If $\not\leqq b$, then $b \vee \mathbf{GR}_*(a,b) = b$.

(3) If $b \neq 0$, then $b \vee \mathbf{GR}_*(a,b) = \mathbf{GR}_*(a,b)$ if and only if $a \leq b$.

Note 3.19 It doesn't follows from $b \vee \mathbf{GR}_*(a,b) = b$ that $a \not\leqq b$ generally. For example, take $a = b = 1$, then $b \vee \mathbf{GR}_*(a,b)$, but where $a \leq b$.

Proposition 3.20 In any $\mathbf{GR}_*$-valuation lattice L,

(1) $a \vee \mathbf{GR}_*(a,b) = a$ if and only if $a \leq b$.

(2) $a \vee \mathbf{GR}_*(a,b) = 0$ if and only if $a \not\leqq b$, or $a = 0$.

Proposition 3.21 In any $\mathbf{GR}_*$-valuation lattice L,

(1) $a \vee \mathbf{GR}_*(a,b) = \mathbf{GR}_*(a,b)$ if and only if $a \leq b$.

(2) $a \vee \mathbf{GR}_*(a,b) = a$ if and only if $a \not\leq b$, or $a = 1$, or $a = b = 1^\#$.

Theorem 3.22 In any $\mathbf{GR}_*$-valuation lattice L,

$$\mathbf{GR}_*(a, \mathbf{GR}_*(a,b)) = \mathbf{GR}_*(a,b)$$

Proof If $a \leq b$ and $b \in \tilde{L}$, then

$$\begin{aligned} &\mathbf{GR}_*(a, \mathbf{GR}_*(a,b)) \\ &= \mathbf{GR}_*(a,1) = 1 \\ &= \mathbf{GR}_*(a,b) \end{aligned}$$

If $a \leq b$ and $b \in L^\#$, then

$$\begin{aligned} &\mathbf{GR}_*(a, \mathbf{GR}_*(a,b)) \\ &= \mathbf{GR}_*(a,1^\#) = 1^\# \\ &= \mathbf{GR}_*(a,b) \end{aligned}$$

If $a \not\leq b$ then $a \neq 0$ and thus

$$\begin{aligned} &\mathbf{GR}_*(a, \mathbf{GR}_*(a,b)) \\ &= \mathbf{GR}_*(a,0) = 0 \\ &= \mathbf{GR}_*(a,b) \end{aligned}$$

This completes the proof.

Corollary 3.23 In any $\mathbf{GR}_*$-valuation lattice L,

(1) $\mathbf{GR}_*(a, \mathbf{GR}_*(a,b)) = b \vee \mathbf{GR}_*(a,b)$ if and only if $a \leq b$ or $b = 0$.

(2) If $b \neq 0$ then $\mathbf{GR}_*(a, \mathbf{GR}_*(a,b)) = b \vee \mathbf{GR}_*(a,b)$ if and only if $a \leq b$.

(3) $\mathbf{GR}_*(a, \mathbf{GR}_*(a,b)) = a \vee \mathbf{GR}_*(a,b)$ if and only if $a \leq b$.

Theorem 3.24 In any $\mathbf{GR}_*$-valuation lattice L,

$$\mathbf{GR}_*(a, b \wedge c) \geq (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c))$$

Proof

(1) Suppose that $a \leq b$ and $a \in \tilde{L}$, then $\mathbf{GR}_*(a,b) = 1$.

If $a \leq c$ and $c \in \tilde{L}$, then $a \leq b \wedge c, b \wedge c \in \tilde{L}$, and thus

$$\begin{aligned} \mathbf{GR}_*(a, b \wedge c) &= 1 = 1 \wedge 1 \\ &= (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c)) \end{aligned}$$

If $a \leq c$ and $c \in L^{\#}$, then $a \leq b \wedge c$ and thus

$$\mathbf{GR}_*(a, b \wedge c) = \begin{cases} 1, & b \wedge c \in \tilde{L}, \\ 1^{\#}, & b \wedge c \in L^{\#} \end{cases}$$

$$(\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c)) = 1 \wedge 1^{\#} = 1^{\#}$$

therefore

$$\mathbf{GR}_*(a,b) \wedge c \geq (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c))$$

If $a \nleqq c$, then $a \nleqq b \wedge c$ and thus

$$\begin{aligned} \mathbf{GR}_*(a, b \wedge c) &= 0 = 1 \wedge 0 \\ &= (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c)) \end{aligned}$$

(2) Suppose that $a \leq b$ and $b \in L^{\#}$, then $\mathbf{GR}_*(a,b) = 1^{\#}$

If $a \leq c$ and $c \in \tilde{L}$, then $a \leq b \wedge c$ and thus

$$\mathbf{GR}_*(a, b \wedge c) = \begin{cases} 1, & b \wedge c \in \tilde{L}, \\ 1^{\#}, & b \wedge c \in L^{\#} \end{cases}$$

$$(\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c)) = 1^{\#} \wedge 1 = 1^{\#}$$

therefore

$$\mathbf{GR}_*(a, b \wedge c) \geq (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c))$$

If $a \leq c$, then $c \in L^{\#}$ then $a \leq b \wedge c$ and $b \wedge c \in L^{\#}$, thus

$$\mathbf{GR}_*(a, b \wedge c) = 0 = 1^{\#} \wedge 1^{\#}$$

$$= (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c))$$

If $a \not\leq c$, then $a \not\leq b \wedge c$ and thus

$$\mathbf{GR}_*(a, b \wedge c) = 0 = 1^\# \wedge 0$$

$$= (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c))$$

(3) Suppose that $a \not\leq b$, then $a \not\leq b \wedge c$ and so

$$\mathbf{GR}_*(a, b \wedge c) = 0 = 0 \wedge (\mathbf{GR}_*(a,c))$$

$$= (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c))$$

This completes the proof.

Theorem 3.25 In any $\mathbf{GR}_*$-valuation lattice L,

$$\mathbf{GR}_*(a, b \wedge c) = (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c))$$

If and only if one of the following conditions holds:

(1) $a \not\leq b \wedge c$, that is a $\not{u}nderline{\leq} b$ or $b \not\leq c$

(2) $a \leq b \wedge c, b \in \tilde{L}, c \in \tilde{L}$

(3) $a \leq b \wedge c, b \in L^\#, b \in L^\#$

(4) $a \leq b \wedge c, b \in L^\#, b \wedge c \in L^\#$

(5) $a \leq b \wedge c, c \in L^\#, b \wedge c \in L^\#$

Theorem 3.26 In any $\mathbf{GR}_*$-valuation lattice L,

$$\mathbf{GR}_*(a, b \wedge c) > (\mathbf{GR}_*(a,b)) \wedge (\mathbf{GR}_*(a,c))$$

if and only if one of the following conditions holds:

(1) $a \leq b \wedge c, b \in \tilde{L}, c \in L^\#, b \wedge c \in \tilde{L}$

(2) $a \leq b \wedge c, b \in L^{\#}, c \in \tilde{L}, b \wedge c \in \tilde{L}$

Note 3.27 A $\mathbf{GR}_*$-valuation lattice L needn't be a Heyting algebra, because that $\mathbf{GR}_*(a, a) = 1$ does not holds generally. For example, if $c \in L^{\#}$, then

$$\mathbf{GR}_*(c, c) = 1^{\#} \neq 1$$

Proposition 3.28 In any $\mathbf{GR}_*$-valuation lattice L, suppose that $b \leq b^*$, then

$$\mathbf{GR}_*(a, b) \leq \mathbf{GR}_*(a, b^*)$$

if and only if one of the following conditions is satisfied:

(1) $a \leq b^*, b^* \in \tilde{L}$

(2) $a \leq b^*, a \leq b, b^* \in L^{\#}, b \in L^{\#}$

(3) $a \nleqq b$

(4) $a \nleqq b^*$

Proposition 3.29 In any $\mathbf{GR}_*$-valuation lattice L, suppose that $b \leq b^*$ then following conditions are equivalent:

(1) $\mathbf{GR}_*(a, b) \nleqq \mathbf{GR}_*(a, b^*)$

(2) $\mathbf{GR}_*(a, b) > \mathbf{GR}_*(a, b^*)$

(3) $a \leq b^*, a \leq b, b^* \in L^{\#}, b \in \tilde{L}$

(4) $\mathbf{GR}_*(a, b) = 1,\ \mathbf{GR}_*(a, b^*) = 1^{\#}$

Proposition 3.30 In any $\mathbf{GR}_*$-valuation lattice L,

$$\mathbf{GR}_*(\mathbf{GR}_*(a, b), b) = \mathbf{GR}_*(a, b)$$

if and only if one of the following conditions is satisfied:

(1) $b = 1$

(2) $b = 1^{\#}, a \leq b$

Proposition 3.31 In any $\mathbf{GR}_*$-valuation lattice L,

(1) If $a \leq b$ and $b \in \tilde{L}$, then

$$\mathbf{GR}_*(\mathbf{GR}_*(a,b),b) = \begin{cases} 1, b = 1 \\ 0, b \neq 1 \end{cases}$$

(2) If $a \leq b$ and $b \in L^{\#}$, then

$$\mathbf{GR}_*(\mathbf{GR}_*(a,b),b) = \begin{cases} 1^{\#}, b = 1^{\#} \\ 0, b \neq 1^{\#} \end{cases}$$

(3) If $a \not\leq b$, then

$$\mathbf{GR}_*(\mathbf{GR}_*(a,b),b) = \begin{cases} 1, b \in \tilde{L} \\ 1^{\#}, b \in L^{\#} \end{cases}$$

Corollary 3.32 In any $\mathbf{GR}_*$-valuation lattice L,

(1) If $b = 1$, then

$$\mathbf{GR}_*(\mathbf{GR}_*(a,b),b) = a \vee \mathbf{GR}_*(a,b)$$

(2) If $b = 1^{\#}$ and $a \leq b$, then

$$\mathbf{GR}_*(\mathbf{GR}_*(a,b),b) = a \vee \mathbf{GR}_*(a,b)$$

Corollary 3.33 In any $\mathbf{GR}_*$-valuation lattice L,

(1) If $b = 1$, then

$$\mathbf{GR}_*(\mathbf{GR}_*(a,b),b) = \mathbf{GR}_*(a, \mathbf{GR}_*(a,b))$$

(2) If $b = 1^{\#}$ and $a \leq b$, then

$$\mathbf{GR}_*(\mathbf{GR}_*(a, b), b) = \mathbf{GR}_*(a, \mathbf{GR}_*(a, b))$$

α-HS rule [1] means that from $\mathbf{GR}_*(a, b) \geq a$ and $\mathbf{GR}_*(b, c) \geq a$ refer $\mathbf{GR}_*(a, c) \geq a$.

Theorem 3.34 In any $\mathbf{GR}_*$-valuation lattice L,

(1) 1 - HS holds.

(2) $1^{\#}$ - HS holds.

Proof

(1) Suppose that $\mathbf{GR}_*(a, b) = 1$ and $\mathbf{GR}_*(a, c) = 1$, then $a \leq b, b \in \tilde{L}, b \leq c, c \in \tilde{L}$ and so $a \leq c, c \in \tilde{L}$, therefore $\mathbf{GR}_*(a, c) = 1$. This shows that 1-HS holds.

(2) Suppose that $\mathbf{GR}_*(a, b) \geq 1^{\#}$ and $\mathbf{GR}_*(b, c) \geq 1^{\#}$, $b \leq c, c \in L^{\#}$, and so $a \leq c, c \in L^{\#}$, thus $\mathbf{GR}_*(a, c) = 1^{\#}$.

If $\mathbf{GR}_*(a, b) = 1^{\#}$ and $\mathbf{GR}_*(b, c) = 1$, then $a \leq b, b \in L^{\#}$, $b \leq c, c \in \tilde{L}$, and so $a \leq c, c \in \tilde{L}$, thus $\mathbf{GR}_*(a, c) = 1$.

If $\mathbf{GR}_*(a, b) = 1$ and $\mathbf{GR}_*(b, c) = 1$, then it follows from (1) that $\mathbf{GR}_*(a, c) = 1$

If $\mathbf{GR}_*(a, b) = 1$ and $\mathbf{GR}_*(b, c) = 1^{\#}$, then $a \leq b$, $b \in \tilde{L}, b \leq c, c \in L^{\#}$, and so $a < 0^{\#}, b < 0^{\#}, a < c, c \in \tilde{L}$, thus $\mathbf{GR}_*(a, c) = 1^{\#}$.

These show that $1^{\#}$ - HS holds.

Of cause, 0-HS holds naturally, it's a trivial rule.

Because $\mathbf{GR}_*$-implication operator $\mathbf{GR}_*$ takes only three values, 1, $1^{\#}$, and 0, so we now can say that for all $a \in L, \alpha$-HS must hold.

Theorem 3.35 In any $\mathbf{GR}_*$ -valuation lattice L, for every $\alpha \in L$, α -HS must hold.

Proof Take any arbitrary $\alpha \in L$.

If $\alpha > 1^{\#}$, then if follows from Theorem 3.34 (1) that α-HS holds.

If $a > 0$, then it follows from Theorem 3.34 (2) that a-HS holds.

It had been mentioned that 0-HS must hold.

These complete the proof.

α-MP rule [1] means that from $\mathbf{GR}_*(a, b) \geq \alpha$ and $a \geq \alpha$ refer $b \geq \alpha$.

Theorem 3.36 In any $\mathbf{GR}_*$-valuation lattice L,

(1) 1-MP holds.

(2) $1^{\#}$ -MP holds.

Proof

(1) Suppose that $a = 1$ and $\mathbf{GR}_*(a, b) = 1$, then $a \leq b, b \in \tilde{L}$, and so $b = 1$. This shows that 1-MP holds.

(2) Suppose that $\mathbf{GR}_*(a, b) \geq 1^{\#}$ and $a \geq 1^{\#}$.

If $\mathbf{GR}_*(a, b)$ and $a = 1$, then it follows from (1) that $b = 1$.

If $1^{\#} \leq \mathbf{GR}_*(a, b) < 1$ and $1^{\#} \leq a < q$, then $\mathbf{GR}_*(a, b) = 1^{\#}, a = 1^{\#}$, and so $a \leq b, b \in L^{\#}$, thus $b = 1^{\#} \geq 1^{\#}$.

If $\mathbf{GR}_*(a, b) = 1$ and $1^{\#} \leq a < 1$, then $a \leq b, b \in \tilde{L}$, and so $b \geq 1^{\#}$.

If $1^{\#} \leq \mathbf{GR}_*(a, b) < 1$ and $1^{\#} \leq a < 1$, then $\mathbf{GR}_*(a, b) = 1^{\#}$, and so $a \leq b, b \in L^{\#}$, thus $a \leq L^{\#}$, this contradict to $a = 1$. Therefore we can say that $b \geq 1^{\#}$ according to classical logic.

These show that $1^{\#}$ - MP holds.

Of cause, 0-MP naturally holds, it is a trivial rule.

Because $\mathbf{GR}_*$-implication operator $\mathbf{GR}_*$ takes only three values, 1, $1^{\#}$, and 0, so we now can say that for all $a \in 1$, a - MP must hold.

Theorem 3.37 In any $\mathbf{GR}_*$ -valuation lattice L, for each $\alpha \in L$, α-MP must hold.

Proof Take any arbitrary $a \in L$.

Suppose that $\alpha > 1^\#$. If $\mathbf{GR}_*(a, b) \geq \alpha$ and $a \geq \alpha$, then $\mathbf{GR}_*(a, b) = 1$ and $a \leq b, b \in \tilde{L}$, so $b \geq \alpha$. This shows that α-MP holds.

Suppose that $\alpha > 0$. If $\mathbf{GR}_*(a, b) \geq \alpha$ and $a \geq \alpha$, then $\mathbf{GR}_*(a, b) = 1^\#$ or 1. If $\mathbf{GR}_*(a, b) = 1^\#$, then $a \leq b, b \in L$, and so $b \geq a$. If $\mathbf{GR}_*(a, b) = 1$, then $a \leq b, b \in \tilde{L}$, and also $b \geq a$. This shows that a-MP holds.

It had been mentioned that 0-MP naturally hold.

This completes the proof.

It is easy to see that

(1) $1 - T(\mathbf{Z}^\#) = T(\mathbf{Z}^\#) = QT(\mathbf{Z}^\#), 0 - T(\mathbf{Z}^\#) = F(S)$.

(2) $T(\mathbf{Z}^\#) \subset QT(\mathbf{Z}^\#) \subset F(S)$, i.e., $1 - T(\mathbf{Z}^\#) \subset 1^\# - T(\mathbf{Z}^\#) \subset 0 - T(\mathbf{Z}^\#)$.

Moreover, we have

Theorem 3.38 In any $\mathbf{GR}_*$-dangerous signal recognition logic $\mathbf{Z}^\#$, suppose that $A, B \in F(S), 1^\# < \alpha \leq 1$. Then $\mathbf{GR}_*(A, B)$ is an a-tautology if and only if $\mathbf{GR}_*(A, B)$ is a tautology.

Proof Suppose that $\mathbf{GR}_*(A, B)$ is an a-tautology, i.e., for every $\mathbf{GR}_*$-valuation $v \in \Omega_{GR}, v(\mathbf{GR}_*(A, B)) \geq a$. Therefore $\mathbf{GR}_*(v(A), v(B)) \geq a$. Because $1^\# < a \leq 1$ and $\mathbf{GR}_*$-implication operator $\mathbf{GR}_*$ takes only three values 1, $1^\#$, and 0, so we can say that $\mathbf{GR}_*(v(A), v(B)) = 1$ must hold. This shows that $\mathbf{GR}_*(A, B)$ is just a tautology.

On the other hand, suppose that $\mathbf{GR}_*(A, B)$ is a tautology, i.e., for every $\mathbf{GR}_*$-valuation $v \in \Omega_{GR}, v(\mathbf{GR}_*(A, B) = 1$ and so $\mathbf{GR}_*(v(A), v(B)) = 1$, of cause $\mathbf{GR}_*(v(A), v(B)) \geq a$. This shows $\mathbf{GR}_*(A, B)$ is an α-tautology.

These complete the proof.

Similarly, we have

Theorem3.39 In any $\mathbf{GR}_*$-dangerous signal recognition logic $\mathbf{Z}^\#$, suppose that $A, B \in F(S), 0 < \alpha \leq 1^\#$. Then $\mathbf{GR}_*(A, B)$ is an α-tautology if and only if $\mathbf{GR}_*$ is a $1^\#$-tautology.

Conclusion We have proposed the new concept, Boolean algebra with Fuzzy shell. Some important examples are given. We have made a new implication operator, $\mathbf{GR}_*$-implication operator, and a new valuation lattices, $\mathbf{GR}_*$-valuation lattices. Then a new kind of nonclassical logic system, $\mathbf{GR}_*$-dangerous signal recognition logic, is established. $1^\#$, the greatest element of the Boolean heart, plays a special and important role in proposed logic.

Our new logic can be fractionized into two fragments, the Fuzzy shell, the Boolean heart. There are two kinds of logic structures with different and distinguished styles and features in our new logic, Fuzzy logic, and Gaines-Rescher logic, they are fused and combined each other by the characteristic algebraic structures of Boolean algebra with Fuzzy shell and $\mathbf{GR}_*$-implication operator. In the Boolean heart, many features and styles of Gaines-Rescher logic are shown or reappeared. In the Fuzzy shell, many features and styles of a kind of Fuzzy logic are shown indirectly and full of cause, there exist many complicated situations in the investigation of transfragments, it is another interesting attractor in this logic. We have discovered that α-HS and α-MP hold unconditionally for every α in our logic.

Acknowledgement The authors would like to thank the referee for his careful and friendly suggestions.

REFERENCES

[1] Wang Guojun, *On the logic fundation of fuzzy reasoning*, Lecture Notes in Fuzzy Mathematica and Computer Science, Omaham, USA, Creighton University, 1997, 4:1 $\sim$ 48.

[2] Wang Guojun, *On the logic fundation of fuzzy modus ponens and fuzzy modus tollens,* The Internation Journal of Fuzzy Mathematics, 1997, 5: 29 ~ 250.

[3] Wang Guojun, *Logic on a kind of algebras (I)*, Journal of Shaanix Normal University (Natural Science Edition), 1997, 25(1), 1 ~ 8.

[4] Wang Guojun, *Logic on a kind of algebras (II),* Journal of Shaanxi Normal University (Natural Science Edition), 1997, 25(3): 1 ~ 8.

[5] Wang Guojun, He Yinyu, *On the structure of L^*-Lindenbaum algebra and a simplification system of axioms for L^*,* Journal of Engineering Mathematics, 1998, 15(1): 1 ~ 8.

[6] Wang Guojun, *Theory of $\sum$-(a-tautologies) in revised Kleene systems*, Science in China (Series E), 1998, 41(2): 188 ~ 195.

[7] WeWangmin, *Principles and Methods of Fuzzy Reasoning,* Guizhou Science and Technology Press, 1994.

[8] Zheng Chongyou, Fau Lei, Cui Hongbin, *Introduction to Frames and Continuous Lattices,* Capital Normal University Press, 1994.

[9] Zhang Wenxiu, Leung Yee, *The University Reasoning Principles,* Xi'an Jiaotong University Press, 1996.

[10] Zhang Wenxiu, Chen Yan, *Plausible Inference and Discovery Logic,* Guizhou Science and Technology Press, 1994.

[11] Zhang Wenxiu, Leung KS, *Fuzzy Control and Systems,* Xi'an Jiaotong University Press, 1998.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii (2000) pp. 105–114

PERTURBED-STEFFENSEN-AITKEN PROJECTION METHODS FOR SOLVING EQUATIONS WITH NONDIFFERENTIABLE OPERATORS

Ioannis K. Argyros
Cameron University
Department of Mathematics
Lawton, OK 73505 U.S.A.

Emil Cătinas and Ion Păaăloiu
Institutul de Calcul
Str. Republicii Nr. 37
P.O. Box 68, 3400 Cluj-Napoca, Romania.

(Received 31 July, 1999)

ABSTRACT In this study we use perturbed-Steffensen- Aitken methods to approximate a locally unique solution of an operator equation in a Banach space. Using projection operators we reduce the problem to solving a linear system of algebraic equations of finite order. Since iterates can rarely be computed exactly we control the residuals to guarantee convergence of the method. Sufficient convergence conditions as well as an error analysis are given for our method.

AMS (MOS) Subject Classification: 65J15, 47H17, 49D15.

Key Words and Phrases Steffensen-Aitken methods, Banach space, projection operator, residuals.

I. INTRODUCTION

In this study we are concerned with the problem of approximating a locally unique fixed point x^* of the nonlinear equation.

$$T(x) = x, \tag{1}$$

where T is a continuous operator defined on a convex subset D of a Banach space E with values in E. The differentiability of T is not assumed. Let T_1 be another nonlinear continuous operator from E into E, and let P be a projection operator $(P^2 = P)$ on E.

We introduce the perturbed-Steffensen-Aitken method

$$x_{n+1} = T(x_n) + PA_n(x_{n+1} - x_n) - z_n. \; A_n = [g_1(x_n), g_2(x_n)] \quad (n \geq 0), \tag{2}$$

where: $[x, y]$ denotes a divided difference of order one of T_1 at the points x, y satisfying

$$[x, y](y - x) = T_1(y) - T_1(x) \quad \text{for all} \quad x, y \in D \quad \text{with} \quad x \neq y \tag{3}$$

and

$$[x, x] = F'(x) \quad (x \in D) \tag{4}$$

if T_1 is Frechet-differentiable $D; g_1, g_2 : D \to E$ are continuous operators; the residual points $\{x_n\}(n \geq 0)$ are chosen in such a way that iteration $\{x_n\}(n \geq 0)$ generated by (2) converges to x^*. The important of studying perturbed Steffensen-Aitken methods comes from the fact that many commonly used variants can be considered procedures of this type. Indeed the above approximation characterizes any iterative process in which corrections are taken as approximate solutions of the Steffensen-Aitken equations. Moreover we note that if for example an equation on the real line is solved $x_n - T(x_n) \geq 0 (n \geq 0)$ and $I - PA_n$ overestimates the derivative, $x_n - (I - PA_n)^{-1}(x_n - T(x_n))$ is always *larger* than the corresponding Steffensen-Aitken iterate. In such cases, a positive $z_n (n \geq 0)$ correction term is appropriate.

For: $P = I (I$ is the identity operator on $E), T(x) = T_1(x)(x \in D), g_1(x) = g_2(x)(x \in D)$, and $z_n = 0(n \geq 0)$ we obtain the ordinary Newton method [1], [2]; $P = I, T_1(x) = T(x)(x \in D), g_1(x) = x(x \in D)$, and $z_n = 0(n \geq 0)$ we obtain Steffensen method [4], [5]; $P = I, T_1(x) = T(x)(x \in D), g_2(x) = g_1(x - T(x))(x \in D)$, and $z_n = 0(n \geq 0)$ we obtain Steffensen-Aitken method [4], [5].

It is easy to see that the solution of (2) reduces to solving certain operator equations in the space E_p. If moreover E_p is a finite dimensional space of dimension N, we obtain a system of linear algebraic equations of at most order N.

We provide sufficient convergence conditions as well as an error analysis for the Steffensen-Aitken method generated by (2).

II. CONVERGENCE ANALYSIS

We state the following semilocal convergence theorem.

Theorem *Let $T, T_1, g_1, g_2 : D \to E$ be continuous operators defined on a convex subset D of a Banach space E with values in E, and P be a projection operator on E. Moreover, assume:*

(a) there exists $x_0 \in D$ such that $B_0 = I - PA_0$ is invertible;

(b) there exist nonnegative numbers $a_i, R, \quad i = 0, 1, 2, \cdots, 9$ such that

$$\|B_0^{-1}P([x,y] - [v,w])\| \le a_0(\|x - v\| + \|y - w\|), \tag{5}$$

$$\|B_0^{-1}(x_0 - T(x_0))\| \le a_1, \tag{6}$$

$$\|B_0^{-1}P([x,y] - [g_1(x), g_2(x)])\| \le a_2(\|x - g_1(x)\| + \|y - g_2(x)\|), \tag{7}$$

$$\|B_0^{-1}(QT_1(x) - QT_1(y))\| \le a_3\|x - y\|, \quad Q = 1 - P, \tag{8}$$

$$\|B_0^{-1}(F(x) - F(y))\| \le a_4\|x - y\|, \quad F(x) = T(x) - T_1(x), \tag{9}$$

$$\|x - g_1(x)\| \le a_5\|B^{-1}(x)(x - T(x) - z(x))\|, \quad B(x) = I - PA(x),$$
$$for\ some\ continuous\ function\ \ z : D \to E, \tag{10}$$

$$\|x - g_2(x)\| \le a_6\|B^{-1}(x)(x - T(x) - z(x))\|, \tag{11}$$

$$\|B_0^{-1}(z_n - z_{n-1})\| \le a_7\|x_n - x_{n-1}\| \quad (n \ge 1), \tag{12}$$

$$\|g_1(x) - g_1(y)\| \le a_8\|x - y\|, \quad a_8 \in [0, 1), \tag{13}$$

and

$$\|g_2(x) - g_2(y)\| \leq a_9\|x - y\|, \quad a_9 \in [0,1), \tag{14}$$

for all x, y, v, $w \in U(x_0, R) = \{x \in E \| \|x - x_0\| \leq R\} \subseteq D$;

(c) the sequence $\{z_n\}(n \geq 0)$ *is null;*

(d) there exists a minumum nonnegative number r^* *satisfying*

$$G(r^*) \leq r^* \quad and \quad r^* \leq R \tag{15}$$

where

$$G(r) = a_1 + \frac{a_2(1 + a_8 + a_9)r + (a_3 + a_4 + a_7)}{[a - a_0(a_8 + a_9)r][1 - a_2(a_5 + a_6)r\beta(r)]}\, r; \tag{16}$$

and

$$\beta(r) = [1 - a_0(a_8 + a_9)r]^{-1} \tag{17}$$

(e) the numbers r^*, R *also satisfy*

$$r^* < \frac{1}{a_2(a_5 + a_6) + a_0(a_8 + a_9)} \tag{18}$$

$$r^* \geq \frac{\|g_1(x_0) - x_0\|}{1 - a_8} \tag{19}$$

$$r^* \geq \frac{\|g_2(x_0) - x_0\|}{1 - a_9} \tag{19}$$

$$b = \alpha(r, R) < 1. \tag{21}$$

where

$$\alpha(s,t) = \frac{a_2(1 + a_8 + a_9)(s + t) + a_3 + a_4}{[1 - a_0(a_8 + a_9)s][1 - a_2(a_5 - a_6)(s + t)\beta(s)]}, \quad s, t \in [0, R] \tag{22}$$

and

$$\lim_{n\to\infty} q_n = 0 \tag{23}$$

where

$$q_n = \sum_{m=0}^{n} b^{n-m} c_m, \quad c_m = \|z_n\|, \quad B_n = I - PA_n \quad (n \geq 0) \tag{24}$$

Then

(i) the scalar sequence $\{t_n\}$ $(n \geq 0)$ *generated by*

$$t_0 = 0, \quad t_1 = a_1 \geq \|x_1 - x_0\|, \tag{25}$$

$$t_{n+1} = t_n + \frac{a_2(1 + a_8 + a_9)(t_n - t_{n-1}) + a_3 + a_4 + a_7}{[1 - a_0(a_8 + a_9)t_n][1 - a_2(a_5 + a_6)(t_n - t_{n-1}\beta_n]}(t_n - t_{n-1}) \quad (n \geq 1) \tag{26}$$

is monotonically increasing, bounded above by r^* *and* $\lim_{n\to\infty} t_n = r^*$, *with* $\beta_n = [1 - a_0(a_8 + a_9)t_n]^{-1}$ $(n \geq 0)$.

(ii) The perturbed-Steffensen-Aitken method generated by (2) is well defined, remains in $U(x_0, r^*)$ *for all* $n \geq 0$, *converges to a unique fixed point* x^* *of* T *in* $U(x_0, R)$.

Moreover the following error bounds hold:

$$\|x_{n+1} - x_n\| \leq \frac{a_2(1 + a_8 + a_9)\|x_n - x_{n-1}\| + a_3 + a_4 + a_7}{[1 - a_0(a_8 + a_9)\|x_n - x_0\|][1 - a_2(a_5 + a_6)\|x_n - x_{n-1}\|\beta_n]} \|x_n - x_{n-1}\| (n \geq 1) \tag{27}$$

$$\|x_{n+1} - x_n\| \leq t_{n+1} - t_n \quad (n \geq 0) \tag{28}$$

and

$$\|x_n - x^*\| \leq r^* - t_n \quad (n \geq 0), \tag{29}$$

where $\bar{\beta}_n = [1 - a_0(a_8 - a_9)\|x_n - x_0\|]^{-1}$ $(n \geq 0)$

Proof (i). By (15) and (25) we get $0 \leq t_0 \leq t_1 \leq r^*$. Let us assume $0 \leq t_{k-1} \leq t_k \leq r^*$ for $k = 1, 2, \cdots, n$. It follows from (18) and (26) that $0 \leq t_k \leq t_{k+1}$. Hence, the sequence $\{t_n\}(n \geq 0)$ is monotonically increasing. Moreover using (26) we get in turn

$$\begin{aligned} t_{k+1} &\leq t_k + \frac{a_2(1+a_8+a_9)r^* + a_3 + a_4 + a_7}{[1 - a_0(a_8+a_9)r^*][1 - a_2(a_5+a_6)r^*\beta(r^*)]} (t_k - t_{k-1}) \\ &\leq \cdots \leq a_1 + \frac{a_2(1+a_8+a_9)r^* a_3 + a_4 + a_7}{[1 - a_0(a_8+a_9)r^*][a - a_2(a_5+a_6)r^*\beta(r^*)]} (t_k - t_0) \\ &\leq G(r^*) \leq r^* \quad (\text{by } (15)) \end{aligned}$$

That is the sequence $\{t_n\}(n \geq 0)$ is also bounded above by r^*. Since r^* is the minimum nonnegative number satisfying $G(r^*) \leq r^*$, it follows that $\lim_{n\to\infty} t_n = r^*$.

(ii) By hypothesis (15) and the choice of a_1 it follows that $x_1 \in U(x_0, r^*)$. From (19) and (20) we get $g_1(x_0)$, $g_2(x_0) \in U(x_0, r^*)$. Let us assume $x_{k+1}, g_1(x_k)$, $g_2(x_k) \in U(x_0, r^*)$ for $k = 0, 1, \cdots, n-1$. Then from (13), (14), (19) and (20) we get

$$\|g_1(x_k) - x_0\| \leq \|g_1(x_k) - g_1(x_0)\| + \|g_1(x_0) - x_0\| \leq a_8\|x_k - x_0\| + \|g_1(x_0) - x_0\|$$

$$\leq a_8 r^* + \|g_1(x_0) - x_0\| \leq r^*$$

and

$$\begin{aligned} \|g_2(x_k) - x_0\| &\leq \|g_2(x_k) - g_2(x_0)\| + \|g_2(x_0) - x_0\| \leq a_9\|x_k - x_0\| + \|g_2(x_0) - x_0\| \\ &\leq a_9 r^* + \|g_2(x_0) - x_0\| \leq r^* \end{aligned}$$

Hence $g_1(x_n)$, $g_2(x_n) \in U(x_0, r^*)$. Using (5), (13), (14) and (17) we obtain

$$\|B_0^{-1}(B_k - B_0)\| \leq a_0(\|g_1(x_0) - g_1(x_k)\| + \|g_2(x_0) - g_2(x_k)\|)$$

$$\leq a_0(a_8+a_9)\|x_0 - x_k\| \leq a_0(a_8+a_9)r^* < 1$$

It follows from the Banach lemma on invertible operators [3] that B_k is invertible and

$$\|B_k^{-1}B_0\| \leq \frac{1}{1 - a_0(a_8+a_9)\|x_k - x_0\|} = \bar{\beta}_k \tag{30}$$

Using (2) we obtain the approximation

$$x_{k+1} - x_k = B_k^{-1}(T(x_k) - x_k - z_k) = (B_k^{-1}B_0)B_0^{-1}$$
$$\{(PT_1(x_k) - PT_1(x_{k-1}) - P[g_1(x_{k-1}),\ g_2(x_{k-1})]\ (x_k - x_{k-1})$$
$$+(QT_1(x_k) - QT_1(x_{k-1}) + (F(x_k) - F(x_{k-1})) + (z_{k-1} - z_k)\} \tag{31}$$

From (7), we get

$$\|B_0^{-1}[PT_1(x_k) - PT_1(x_{k-1}) - PA_{k-1}(x_k - x_{k-1})]\| \leq \|B_0^{-1}P([x_{k-1}, x_k] - A_{k-1})(x_k - x_{k-1})\|$$

$$\leq a_2(\|x_{k-1} - g_1(x_{k-1})\| + \|x_k - g_2(x_{k-1})\|)\|x_k - x_{k-1}\| \tag{32}$$

and since by (10), (11), (13), (14)

$$\begin{aligned}
\|x_{k-1} - g_1(x_{k-1})\| &\leq \|x_{k-1} - x_k\| + \|g_1(x_k) - g_1(x_{k-1})\| + \|x_k - g_1(x_k)\| \\
&\leq \|x_k - x_{k-1}\| + a_8\|x_k - x_{k-1}\| + a_5\|B_k^{-1}(x_k - T(x_k) - z_k\| \\
\|x_k - g_2(x_{k-1})\| &\leq x_k - g_2(x_k)\| + \|g_2(x_k) - g_2(x_{k-1})\| \\
&\leq a_6\|B_k^{-1}(x_k - T(x_k) - z_k)\| + a_9\|x_k - x_{k-1}\|
\end{aligned}$$

(32) gives

$$\|B_0^{-1}[PT_1(x_k) - PT_1(x_{k-1}) - PA_{k-1}(x_k - x_{k-1})\| \leq a_2(1 + a_8 + a_9)\|x_k - x_{k-1}\|^2$$

$$+ a_2(a_5 + a_6)\|B_k^{-1}(x_k - T(x_k) - z_k)\|\|x_k - x_{k-1}\| \tag{33}$$

Moreover from (8), (9) and (12) we obtain respectively

$$\|B_0^{-1}(QT_1(x_k) - QT_1(x_{k-1})\| \leq a_3\|x_k - x_{k-1}\| \quad (k \geq 1) \tag{34}$$

$$\|B_0^{-1}(F(x_k) - F(x_{k-1}))\| \leq a_4\|x_k - x_{k-1}\| \quad (k \geq 1) \tag{35}$$

and

$$\|B_0^{-1}(z_k - z_{k-1})\| \leq a_7\|x_k - x_{k-1}\| \quad (k \geq 1) \tag{36}$$

Furthermore (31) because of (30), (33)-(36) finally gives (27) for $n = k$.

Estimate (28) is true for $n = 0$ by (25). Assume (28) is true for $k = 0, 1, 2, \cdots, n-1$. Then from (26), (27) and the induction hypothesis it follows that (28) is true for $k = n$. By (28) and part (i) it follows that iteration $\{x_n\}(n \geq 0)$ is Cauchy in a Banach space E and as such it converges to some $x^* \in U(x_0, r^*)$ (since $U(x_0, r^*)$ is a closed set). Using hypothesis (c) and letting $n \to \infty$ in (2) we get $x^* = T(x^*)$. That is x^* is a fixed point of T. Estimate (29) follows immediately from (28) using standard majorization techniques [2], [3].

Finally to show uniqueness let us assume $y^* \in U(x_0, R)$ is a fixed point of equation (1). As in (31) we start from the approximation.

$$\begin{aligned} x_{n+1} - y^* &= (B_n^{-1} B_0) B_0^{-1} \{[PT_1(x_n) - PT_1(y^*) - PA_n(x_n - y^*)] \\ &\quad + [QT_1(x_n) - QT_1(y^*)] + [F(x_n) - F(y^*)] - \quad z_n\} \end{aligned}$$

and using (5), (7)-(11), (13), (14), (21), (22) and (24) we get

$$\|x_{n+1} - y^*\| \leq b\|x_n - y^*\| + c_n \leq \cdots \leq b^{n+1}\|x_0 - y^*\| + q_n \quad (n \geq 0) \tag{37}$$

By letting $n \to \infty$ as using (21) and (23) we get $\lim_{n\to\infty} x_n = y^*$. It follows from the uniqueness of the limit that $x^* = y^*$.

That completes the proof of the Theorem.

Remarks

(1) Conditions (19) and (20) guarantee $g_1(x), g_2(x) \in U(x_0, r^*)$ for $x \in U(x_0, r^*)$. Hence condition (7) can be dropped and we can set $a_2 = a_0$. However it is hoped that $a_2 \leq a_0$.

(2) It can easily be seen that the first inequality in (15) can be replaced by the system of inequalities (17), (18) and

$$f(r^*) \leq 0$$

where

$$f(r) = d_2 r^2 + d_1 r + d_0$$

with

$$b_1 = a_2(1 + a_8 + a_9), \quad b_2 = a_3 + a_4 + a_7, \quad b_3 = a_0(a_8 + a_9) + a_2(a_5 + a_6)$$

$$\begin{aligned} d_2 &= b_1 + b_3 \\ d_1 &= b_1 - 1 - b_3 a_1 \end{aligned}$$

and $d_0 = a_1$.

(3) Condition (23) is satisfied if and only if $z_n = 0 (n \geq 0)$

(4) It can easily be seen from (10) and (11) that conditions (19) and (20) will be satisfied if $a_5 + a_8 \leq 1$ and $a_6 + a_9 \leq 1$ for $r^* \neq 0$. Indeed from (10) we have $\|x_0 - g_1(x_0)\| \leq a_5 \|x_1 - x_0\| \leq a_5 r^*$. Hence (19) will be certainly satisfied if $a_5 r^* \leq (1 - a_8) r^*$. That is if $a_5 + a_8 \leq 1$. We argue similarly for (20).

REFERENCES

[1] Argyros, I.K. *On some projection methods for the solution of nonlinear operator equations with non-differentiable operators*, Tamkang J. Math. 24, 1, (1993), 1-8.

[2] Argyros, I. K. and Szidarovszky, F. *The theory and application of iteration methods,* C.R.C. Press, Inc. Boca Raton, Florida, 1993.

[3] Kantorovich, L.V. and Akilov, G.P. *Functional analysis in normed spaces,* Academic Press, New York, 1978.

[4] Păvăloiu, I. *Sur une generalisation de la methode de Steffensen,* Revue d'analyse Numerique et de theorie de l'approximation, 21, 1, (1992), 59-65.

[5] Păvăloiu, I. *Bilateral approximations for the solutions of scalar equations,* Revue d'analyse numerique et de theorie de l'approximation, 23, 1, (1994), 95-100.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 115–124

A CERTAIN CLASS OF MEROMORPHIC MULTIVALENT FUNCTIONS WITH POSITIVE AND FIXED SECOND COEFFICIENTS

M. K. Aouf, H. M. Hossen and H. E. El-Attar
Department of Mathematics
Faculty of Science
University of Mansoura
Mansoura, Egypt
E-mail: Sinfac@num.mans.eun.eg

(Received 2 March, 2000)

ABSTRACT: In this paper we consider the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$ consisting of functions analytic and multivalent in the punctured disc $U^* = \{z : 0 < |z| < 1\}$ and with the fixed second coefficient. In the present paper we have obtained coefficient inequalities for the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$. Also we have shown that this class is closed under arithmetic mean and convex linear combinations. Lastly we have obtained the radius of convexity.

AMS (1991) Mathematics Subject Classification: 30C45 and 30C50.

Key Words and Phrases: Analytic, p-valent, meromorphic.

1. INTRODUCTION: Let $\sum_p$ denote the class of functions of the form

$$f(z) = \frac{1}{z^p} + \sum_{n=1}^{\infty} a_{p+n-1} z^{p+n-1} (a_{p+n} \geq 0; \quad p \in N = \{1, 2, \cdots, \}) \tag{1.1}$$

which are analytic and p-valent in the punctured disc $U^* = \{z : 0 < |z| < 1\}$. For a function $f(z)$ in $\sum_p$, and for $-1 \leq A < B \leq 1, \quad 0 < B \leq 1, \quad 0 \leq \alpha < 1, \quad 0 <$

$\beta \leq 1$ and $\frac{B}{(B-A)} < \gamma \leq \frac{B}{(B-A)\alpha}$ if $\alpha \neq 0$ and $\frac{B}{(B-A)} < \gamma \leq 1$ if $\alpha = 0$, we say that $f(z) \in \sum_p(A, B, \alpha, \beta, \gamma)$ if and only if

$$\left| \frac{\frac{zf'(z)}{f(z)} + p}{(B-A)\gamma\left(\frac{zf'(z)}{f(z)} + \alpha\right) - B\left(\frac{zf'(z)}{f(z)} + p\right)} \right| < \beta, z \in U^* \tag{1.2}$$

The class $\sum_p(A, B, \alpha, \beta, \gamma)$ was studied by Joshi and Aouf [3].

Meromorphic multivalent functions have been extensively studied by Uralegaddi and Ganigi [9], Aouf ([1, 2]) and Mogra ([4, 5]).

We begin by recalling the following lemma due to Joshi and Aouf [3].

Lemma 1: Let the function $f(z)$ be defined by (1.1). Then $f(z)$ is in the class $\sum_p(A, B, \alpha, \beta, \gamma)$ if and only if

$$\sum_{n=1}^{\infty} C(p, A, B, \alpha, \beta, \gamma, n) a_{p+x-1} \leq D(p, A, B, \alpha, \beta, \gamma) \tag{1.3}$$

where

$$\begin{aligned} C(p, A, B, \alpha, \beta, \gamma, n) = (2p+n-1) + \beta\{(B-A)\gamma(p+n-1+\alpha) \\ - B(2p+n-1)\} \quad (n = 1, 2, \cdots) \end{aligned} \tag{1.4}$$

and

$$D(p, A, B, \alpha, \beta, \gamma) = (B-A)\gamma\beta(p-\alpha) \tag{1.5}$$

The result is sharp.

In view of Lemma 1, we can see that the functions $f(z)$ defined by (1.1) in the class $\sum_p(A, B, \alpha, \beta, \gamma)$ satisfy the coefficient inequality.

$$a_p \leq \frac{D(p, A, B, \alpha, \beta, \gamma)}{C(p, A, B, \alpha, \beta, \gamma, 1)} \tag{1.6}$$

Hence we may take

$$a_p = \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)}, \quad 0 \le k \le 1 \tag{1.7}$$

Let $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$ denote the subclass of $\sum_p(A, B, \alpha, \beta, \gamma)$ consisting of functions of the form

$$f(z) = z^{-p} + \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} z^p + \sum_{n=2}^{\infty} a_{p+n-1} z^{p+n-1} \tag{1.8}$$

where $a_{p+n-1} \ge 0$ and $0 \le k \le 1$.

The object of the present paper is to determine coefficient inequalities for the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$. Further we show that this class is closed under arithmetic mean and convex linear combination. Lastly we have obtained radius of convexity. Various results obtained in this paper are shown to be sharp. Techniques used are similar to those of Silverman and Silvia [7], Uralegaddi [8] and Owa, Darwish and Aouf [6].

2. COEFFICIENT INEQUALITIES:

Theorem 1: Let the function $f(z)$ be defined by (1.8). Then $f(z)$ is in the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$ if and only if

$$\sum_{n=2}^{\infty} C(p, A, B, \alpha, \beta, \gamma, n) a_{p+n-1} \le D(p, A, B, \alpha, \beta, \gamma)(1-k) \tag{2.1}$$

The result is sharp.

Proof: Putting

$$a_p = \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)}, \quad 0 \le k \le 1 \tag{2.2}$$

in (1.3) and simplifying we get the result. The result is sharp for the function

$$f(z) = z^{-p} + \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} z^{p} +$$

$$\frac{D(p, A, B, \alpha, \beta, \gamma)(1-k)}{C(p, A, B, \alpha, \beta, \gamma, n)} z^{p+n-1} \qquad (n \geq 2) \tag{2.3}$$

Corollary 1: Let the function $f(z)$ defined by (1.8) be in the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$. Then

$$a_{p+n-1} \leq \frac{D(p, A, B, \alpha, \beta, \gamma)(1-k)}{C(p, A, B, \alpha, \beta, \gamma, n)}, \quad (n \geq 2) \tag{2.4}$$

The result is sharp for the function $f(z)$ given by (2.3)

3. CLOSURE THEOREMS: In this section, we shall show that the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$ is closed under arithmetic mean and convex linear combination.

Theorem 2: Let the functions

$$f_j(z) = z^{-p} + \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} z^{p} +$$

$$\sum_{n=2}^{\infty} a_{p+n-1,j} z^{p+n-1} \quad (a_{p+n-1,j} \geq 0) \tag{3.1}$$

be in the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$ for every $j = 1, 2, \cdots, m$. Then the function

$$g(z) = z^{-p} + \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} z^{p} +$$

$$\sum_{n=2}^{\infty} b_{p+n-1} z^{p+n-1} \qquad (b_{p+n-1} \geq 0) \tag{3.2}$$

is also in the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$, where

$$b_{p+n-1} = \frac{1}{m}\sum_{j=1}^{m} a_{p+n-1,j} \tag{3.3}$$

Proof: Since $f_j(z) \in \sum_{p,k}(A, B, \alpha, \beta, \gamma)$ it follows from Theorem 1 that

$$\sum_{n=2}^{\infty} C(p, A, B, \alpha, \gamma, n) a_{p+n-1}, j \leq D(p, A, B, \alpha, \beta, \gamma)(1-k) \tag{3.4}$$

for every $j = 1, 2, \cdots, m$. Hence

$$\sum_{n=2}^{\infty} C(p, A, B, \alpha, \beta, \gamma, n) b_{p+n-1} =$$

$$\sum_{n=2}^{\infty} C(p, A, B, \alpha, \beta, \gamma, n)\left(\frac{1}{m}\sum_{j=1}^{m} a_{p+n-1,j}\right) =$$

$$\frac{1}{m}\sum_{j=1}^{m}\sum_{n=2}^{\infty} C(p, A, B, \alpha, \beta, \gamma, n) a_{p+n-1,j} \leq D(p, A, B, \alpha, \beta, \gamma)(1-k) \tag{3.5}$$

and the result follows.

Theorem 3: Let

$$f_p(z) = z^{-p} + \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} z^p \tag{3.6}$$

and

$$f_{p+n-1} = z^{-p} + \frac{D(a, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} z^p +$$

$$\frac{D(p, A, B, \alpha, \beta, \gamma)(1-k)}{C(p, A, B, \alpha, \beta, \gamma, n)} z^{p+n-1} \quad (n \geq 2) \tag{3.7}$$

Then $f(z)$ is in the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$ if and only if it can be expressed in the form

$$f(z) = \sum_{n=1}^{\infty} \lambda_{p+n-1} f_{p+n-1}(z), \tag{3.8}$$

where

$$\lambda_{p+n-1} \geq 0 \quad \text{and} \quad \sum_{n=1}^{\infty} \lambda_{p+n-1} = 1$$

Proof: Let

$$f(z) = \sum_{n=1}^{\infty} \lambda_{p+n-1} \quad f_{p+n-1}(z)$$

$$= z^{-p} + \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} z^{p} +$$

$$\sum_{n=2}^{\infty} \frac{D(p, A, B, \alpha, \beta, \gamma)(1-k)}{C(p, A, B, \alpha, \beta, \gamma, n)} \lambda_{p+n-1} z^{p-n-1} \tag{3.9}$$

Since

$$\sum_{n=2}^{\infty} \frac{D(p, A, B, \alpha, \beta, \gamma)(1-k)\lambda_{p+n-1}}{C(p, A, B, \alpha, \beta, n)} \frac{C(p, A, B, \alpha, \beta, \gamma, n)}{D(p, A, B, \alpha, \beta, \gamma)}$$

$$= (1-k) \sum_{n=2}^{\infty} \lambda_{p+n-1} = (1-k)(1-\lambda_p) \leq 1-k \tag{3.10}$$

hence, by Theorem 1, we have $f(z) \in \sum_{p,k}(A, B, \alpha, \beta, \gamma)$

Conversely, we suppose that $f(z)$ defined by (1.8) is in the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$. Then by using (2.4), we get

$$a_{p+n-1} \leq \frac{D(p, A, B, \beta, \alpha, \beta, \gamma)(1-k)}{C(p, A, B, \alpha, \beta, \gamma, n)} \quad (n \geq 2) \tag{3.11}$$

Setting

$$\lambda_{p+n-1} = \frac{C(p, A, B, \alpha, \beta, \gamma, n)}{D(p, A, B, \alpha, \beta, \gamma)(1-k)} a_{p+n-1} \quad (n \geq 2) \tag{3.12}$$

and

$$\lambda_p = 1 - \sum_{n=2}^{\infty} \lambda_{p+n-1} \tag{3.13}$$

We have (3.8). This completes the proof of Theorem 3.

Theorem 4: Let the function $f(z)$ defined by (1.8) be in the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$. Then $f(z)$ is mermorphically p-valent convex in $0 < |z| < r = r(p, A, B, \alpha, \beta, \gamma, k)$, where $r(p, A, B, \alpha, \beta, \gamma, k)$ is the largest value for which

$$\frac{3p^2 D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} r^{2p} +$$
$$\frac{(p+n-1)(3p+n-1)D(p, A, B, \alpha, \beta, \gamma)(1-k)}{C(p, A, B, \alpha, \beta, \gamma, n)} r^{2p+n-1} = p^2 \qquad (4.1)$$

The result is sharp for the function

$$f_{p-n-1}(z) = z^{-p} \frac{D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, 1)} z^p +$$
$$\frac{D(p, A, B, \alpha, \beta, \gamma)(1-k)}{C(p, A, B, \alpha, \beta, \gamma, n)} z^{p+n-1} \quad \text{for some n} \qquad (4.2)$$

Proof: It is sufficient to show that

$$\left| \frac{(zf'(z))' + pf'(z)}{f'(z)} \right| \leq p \quad \text{for} \quad 0 < |z| < r = r(p, A, B, \alpha, \beta, \gamma, k)$$

Note that

$$\left| \frac{(zf'(z))' + pf'(z)}{f'(z)} \right| \leq$$
$$\frac{\frac{2p^2 D(p,A,B,\alpha,\beta,\gamma)k}{C(p,A,B,\alpha,\gamma,1)} r^{2P} + \sum_{n=2}^{\infty}(p+n-1)(2p+n-1)a_{p+n-1}r^{2p+n-1}}{p - \frac{pD(p,A,B,\alpha,\beta,\gamma)k}{C(p,A,B,\alpha,\beta,\gamma,1)} r^{2P} - \sum_{n=2}^{\infty}(p+n-1)a_{p+n-1}r^{2p+n-1}} \leq p \qquad (4.3)$$

for $0 < |z| \leq r$ if and only if

$$\frac{3p^2 D(p, A, B, \alpha, \beta, \gamma)k}{C(p, A, B, \alpha, \beta, \gamma, 1)} r^{2P} + \sum_{n=2}^{\infty}(p+n-1)(3p+n-1)a_{P+n-1}r^{2P+n-1} \leq P^2 \quad (4.4)$$

Since $f(z)$ is in the class $\sum_{p,k}(A, B, \alpha, \beta, \gamma)$, from (2.1) we may take

$$a_{P+n-1} = \frac{D(p, A, B, \alpha, \beta, \gamma)(1-k)\lambda_{P+n-1}}{C(p, A, B, \alpha, \beta, \gamma, n)} \qquad (4.5)$$

$$\sum_{n=2}^{\infty} \lambda_{P+n-1} \leq 1 \tag{4.6}$$

For each fixed r, we choose the positive integer $n_0 = n_0(r)$ for which $\frac{(p+n-1)(3p+n-1)}{C(p,A,B,\alpha,\beta,\gamma,n)}$ r^{2P+n-1} is maximal. Then it follows that

$$\sum_{n=2}^{\infty}(p+n-1)(3p+n-1)a_{P+n-1}r^{2p+n_0-1} \leq$$

$$\frac{(p+n_0-1)(3p+n_0-1)D(p,A,B,\alpha,\beta,\gamma)(1-k)}{C(p,A,B,\alpha,\beta,\gamma,n_0)}r^{2p+n-1} \tag{4.7}$$

Hence $f(z)$ is meromorphically p-valent convex in $0 < |z| < r(p,A,B,\alpha,\beta,\gamma,k)$ provided that

$$\frac{3p^2 D(p,A,B,\alpha,\beta,\gamma)k}{C(p,A,B,\alpha,\beta,\gamma,1)}r_0^{2P}+$$

$$\frac{(p+n_0-1)(3p+n_0-1)D(p,A,B,\alpha,\beta,\gamma)(1-k)}{C(p,A,B,\alpha,\beta,\gamma,n_0)}r_0^{2P+n_0-1} \leq p^2 \tag{4.8}$$

We find the value $r_0 = r_0(p,A,B,\alpha,\beta,k)$ and the integer $n_0(r_0)$ so that

$$\frac{3p^2 D(p,A,B,\alpha,\beta,\gamma)k}{C(p,A,B,\alpha,\beta,\gamma,1)}r_0^{2P}+$$

$$\frac{(p+n_0-1)(3p+n_0-1)D(p,A,B,\alpha,\beta,\gamma)(1-k)}{C(p,A,B,\alpha,\beta,\gamma,n_0)}r_0^{2p+n-1} = p^2 \tag{4.9}$$

Then this value r_0 is the radius of meromorphically p-valent convex for functions $f(z)$ belonging to the class $\sum_{p,k}(A,B,\alpha,\beta,\gamma)$.

REFERENCES

[1] M. K. Aouf, *A generalization of meromorphic multivalent functions with positive cefficients*, Math. Japon. 35 (1990), no.4, 609-614.

[2] M. K. Aouf, *On a class of meromorphic multivalent functions with positive coefficients,* Math. Japon. 35 (1990). 4, 603-608.

[3] S.B. Joshi and M.K. Aouf, *A certain class of meromorphic multivalent functions with positive coefficients,* An.Stiint. Univ. "Al.I.Cuza" lasi Set. I. a Mat. (N.S.) (1995), 221-228.

[4] M.L. Mogra, *Meromorphic multivalent functions with positive coefficients,* I, Math. Japan. 35 (1990), no. 1, 1-11.

[5] M.L. Mogra, *Meromorphic multivalent functions with positive coefficients,* II, Math. Japon, 35 (1990), no.6, 1089-1098.

[6] S. Owa, H. E. Darwish and M. K. Aouf, *Meromorphic multivalent functions with positive and fixed second coefficients,* Math. Japon, 46(1997) no. 2,231-236.

[7] H. Silverman and E. M. Silvia, *Fixed coefficients for subclasses of starlike functions,* Houston J. Math. 7(1981), 129-136.

[8] B.A. Uralegaddi, *Meromorphically starlike functions with positive and fixed second coefficients,* Kyungpook Math. J. 29 (1989), no. 1, 64-68.

[9] B.A. Uralegaddi and M.D. Ganigi, *Meromorphic multivalent functions with positive coefficients,* Nep. Math. Sci. Rep. 11 (1986), 95-102.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 125–134

EQUIVALENT BINARY QUADRATIC FORMS AND THE ORBITS OF $Q^*(\sqrt{p})$ UNDER MODULAR GROUP ACTION

Imrana Kousar
Lahore College for Women, Lahore.

S. M. Husnine & A. Majeed
Department of Mathematics
Punjab University, Lahore.

ABSTRACT In this paper we have proved that if $\bar{\alpha}$ is in the orbit α^G where $a = \frac{a+\sqrt{p}}{c}$, $b = \frac{a^2-p}{c}$ then $p \equiv 1 \pmod 4$ and the quadratic form $f = cx^2 - 2axy + by^2$ is equivalent to $-f$.

INTRODUCTION Let G be a group of 2×2 matrices with integral element and determinant 1. The two quadratic forms $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = Ax^2 + Bxy + Cy^2$ are said to be equivalent, if there is an $M = \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \in G$ such that $g(x,y) = f(Px + Qy, \ \ Rx + Sy)$.

In this case we say that M takes f to g and we write $f \sim g$. The co-efficients of g in terms of co-efficients of f are as follows:

$$\begin{aligned} A &= aP^2 + bPR + cR^2 \\ B &= 2aPQ + b(PS + QR) + 2cRS \\ C &= aQ^2 + bQS + cS^2 \end{aligned}$$

The effect of this change of variables is made clear by making systematic use of matrix multiplication.

Let

$$F = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}, \quad H = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \end{pmatrix}$$

Then $X^tFX = (f(x,y))$

Similarly, $X^tHX = (g(x,y))$ our definition of g states that we obtain g by evaluationg f with x replaced by MX.

That is

$$\begin{aligned} (MX)^tF(MX) &= (g(x,y)) \\ X^t(M^tFM)X &= (g(x,y)) \end{aligned}$$

Since the co-efficient matrix H of quadratic form g is uniquely determined by the co-efficients of g we must have $M^tFM = H$.

In our subsequent work we shall use the following known results of number theory.

1.1: Let p be a prime number, then p can be written as a sum of two squares if and only if $p = 1 \pmod 4$.

1.2: If a positive integer n can be written as a sum of squares of two rational numbers then it can be written as a sum of squares of two integers.

1.3: For any prime p the Diophantine equation $x^2 - py^2 = -1$ has integral solution if and only in $p \equiv 1 \pmod 4$.

1.4: If the equation $x^2 - py^2 = -1$ has integral solution x_1, Y_1 then $(x_1, Y_1) = 1$.

1.5: Every quadratic irrational number $\frac{a'+b'\sqrt{n}}{c'}$, where n' is a non-square can be uniquely represented as $\frac{a+\sqrt{n}}{c}$ where $\frac{a^2-n}{c} = b$ is an integer and $(a,b,c) = 1$.

(See Q. Mushtaq [3]). We denote the set of all such numbers for a particular n by $Q^*(\sqrt{n})$.

Imrana Kausar, S. M. Husnine, A. Majeed in [5] and [6] have investigated the behaviour of ambiguous and totally positive or totally negative elements of $Q^*(\sqrt{n})$

under the action of modular group and the group $H =< t,\ y : t^3 = y^3 = 1 >$ on the quadratic field. The same authors in [7] classify the elements of $Q^*(\sqrt{p})$ for any odd prime p with respect to the odd-even nature of a, b, c. For the number theoretic result we refer the readers to [1] and [2].

In this paper we have proved that if $\alpha = \frac{a+\sqrt{p}}{c}$ is mapped onto $\bar{\alpha}$ then the quadratic from $f = cx^2 - 2axy - by^2$ is equivalent to $-f$ and $p \equiv 1 \pmod 4$.

We start with the following lemma.

Lemma For any quadratic form $f(x, y) = Ax^2 + Bxy + Cy^2$ if $\alpha = \frac{a+\sqrt{n}}{c}$ and $\bar{\alpha} = Q^*(\sqrt{n})$ are the roots of f then there is a rational number λ such that

$$f(x, y) = \lambda(cx^2 - 2axy + by^2)$$

Proof Let

$$\alpha = \frac{a+\sqrt{n}}{c}, \quad \bar{\alpha} \in Q^*(\sqrt{n}), \quad b = \frac{a^2 - n}{c}$$

be the roots $f(x, y) = Ax^2 + Bxy + Cy^2$ So that

$$\frac{a \pm \sqrt{n}}{c} = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

Then

$$\frac{a}{c} = \frac{-B}{2A} \quad \text{and} \quad \frac{B^2 - 4AC}{4A^2} = \frac{n}{c^2}$$
$$\frac{a^2}{c^2} = \frac{B^2}{4A^2} \quad \text{and} \quad \frac{B^2}{4A^2} - \frac{C}{A} = \frac{n}{c^2}$$

For these equations, we have

$$\frac{C}{A} = \frac{a^2 - n}{c^2} = \frac{b}{c} \quad \text{as} \quad b = \frac{a^2 - n}{c}$$

Hence

$$\begin{aligned} f(x, y) &= A\left(x^2 + \frac{B}{A}xy + \frac{C}{A}y^2\right) \\ &= \frac{A}{c}\ (cx^2 - 2axy + by^2) \end{aligned}$$

$f(x,y) = \lambda(cx^2 - 2axy + by^2)$ where $\lambda = \frac{A}{c}$, a rational number.

Theorem (A) Under the action of modular group PSL $(2, Z)$ on $Q^*(\sqrt{p})$, α is mapped on to $\bar{\alpha}$, where $\alpha = \frac{a+\sqrt{p}}{c}$, $b = \frac{a^2-p}{c}$, $(a,b,c) = 1$ If and only if the quadratic form $f = cx^2 - 2axy + by^2$ is equivalent to $-f$.

Proof Suppose $\alpha = \frac{a+\sqrt{p}}{c} \in Q^*(\sqrt{p})$, mapped onto $\bar{\alpha}$ under the action of modular group G, then we show that the binary quadratic form f is equivalent to $-f$. Since α is mapped onto $\bar{\alpha}$, so there exist an element $g = \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \in G P, Q, R, S \in Z$ and $PS - QR = 1$

such that $g(\alpha) = \bar{\alpha}$

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix}(\alpha) = \bar{\alpha}$$

$$\frac{P\alpha + Q}{R\alpha + S} = \bar{\alpha}$$

$$p\alpha + Q = R\alpha\bar{\alpha} + S\bar{\alpha}$$

$$P\left(\frac{a+\sqrt{p}}{c}\right) + Q = R\frac{b}{c} + S\left(\frac{a-\sqrt{p}}{c}\right)$$

$$Pa + P\sqrt{p} + cQ = bR + Sa - S\sqrt{P} = 0$$

$$[a(P-S) + cQ - bR] + (P+S)\sqrt{p} = 0$$

$$\Rightarrow a(P-S) + cQ - bR = 0 \quad \text{and} \quad P + S = 0$$

$$\begin{aligned} cQ &= -aP + aS + bR & \qquad S = -P \\ cQ &= -aP + aS + bR \\ Q &= \frac{-aP + aS + bR}{c} \end{aligned}$$

$$\text{Put} \quad S = -P, \quad Q = \frac{-2aP + bR}{c} = \frac{2aP - bR}{-c}$$

$$PS - QR = 1$$

$$-p^2 - \left(\frac{2aP - bR}{-c}\right) R = 1 \quad \text{or} \quad cP^2 - (2ap - bR)R = -c$$

or

$$CP^2 - 2aPR + bR^2 = -c \tag{1}$$

Now $Q = \frac{2aP-bR}{-c}$ implies that $2aP - bR + CQ = 0$ or $-2aS = bR - cQ$

$$-2aQS = bQR - cQ^2 \tag{2}$$

and

$$PS - QR = 1 \Rightarrow -S^2 - QR = 1$$

or

$$-S^2b - bRQ = b \tag{3}$$

From (2) and (3)

$$\begin{array}{r}
-2aQS = bRQ - cQ^2 \\
b = -bRQ \quad - S^2b \\
\hline
b - 2aQS = -cQ^2 \;-\; S^2b
\end{array}$$

$$b = -cQ^2 + 2aQS - S^2b \tag{4}$$

Also

$$Q = \frac{2aP - bR}{-c} \Rightarrow 2aP - bR + cQ = 0$$

or

$$2aP^2 - bRP + cPR = 0 \tag{5}$$

$$PS - QR = 1 \Rightarrow -P^2 - QR = 1$$

or

$$-1 - QR = P^2$$

From (5)

$$2a(-1 - QR) + bRS + cPQ = 0$$

$$-2a = 2aQR - bRS - cPQ \tag{6}$$

$$2aP - bR + cQ = 0 \Rightarrow 2aPS - bRS + cQS = 0$$

or

$$2aPS - bRS - cPQ = 0 \tag{7}$$

From (6) and (7)

$$-2a = 2aQR - bRS - cPQ$$

$$\underline{0 = 2aPS - bRS - cPO}$$

$$-2a = 2a(PS + QR) - 2bRS - 2cPQ \tag{8}$$

Let α, $\bar{\alpha}$ be the roots of binary quadratic form f then by previous lemma for $\lambda = 1$ we have

$$f(x,y) = cx^2 - 2axy + by^2$$

$$\begin{aligned} f(Px+Qy, Rx+Sy) &= c(Px+Qy)^2 - 2a(Px+Qy)(Rx+Sy) + b(Rx+Sy)^2 \\ &= (cP^2 - 2aPR + bR^2)x^2 + [2cPQ - 2a \\ &\quad (PS+QR) + 2bRS]xy + \ (cQ^2 - 2aQS + bS^2)y^2 \\ &= -cx^2 - 2axy - by^2 (using\ (1),(4),(8)) \\ &= -(cx^2 - 2axy + by^2) \\ &= -f(x,y) \end{aligned}$$

Hence f is equivalent to $-f$.

Conversely, let $\alpha = \frac{a+\sqrt{p}}{c} \in Q^*(\sqrt{p})$ and the quadratic form $f(x,y) = cx^2 - 2axy + by^2$ is equivalent to $-f(x,y)$. We show that α is mapped onto $\bar{\alpha}$. Since the quadratic form $g(x,y) = cx^2 - 2axy + by^2$ is equivalent to $f(x,y) = -cx^2 + 2axy - by^2$, so there is an element $g = \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \in G$ such that $PS - QR = 1, P, Q, R, S \in Z$.

The co-efficients of g in terms of co-efficients of f are

$$c = cP^2 + 2aPR + bR^2 \tag{1}$$

$$-2a = -2cPQ + 2a(PS + QR) - 2bRS$$

or

$$-a = -cPQ + a(PS + QP) - bRS \tag{2}$$

$$b = -cQ^2 + 2aQS - bS^2$$

or

$$2aQs = b + bS^2 + cQ^2 \tag{3}$$

$$1 = PS - QR \tag{4}$$

$$\underline{0 = 2aPS - bRS - cPO}$$

$$-2a = 2a(PS + QR) - 2bRS - 2cPQ \tag{8}$$

Let α, $\bar{\alpha}$ be the roots of binary quadratic form f then by previous lemma for $\lambda = 1$ we have

$$f(x, y) = cx^2 - 2axy + by^2$$

$$\begin{aligned} f(Px + Qy, Rx + Sy) &= c(Px + Qy)^2 - 2a(Px + Qy)(Rx + Sy) + b(Rx + Sy)^2 \\ &= (cP^2 - 2aPR + bR^2)x^2 + [2cPQ - 2a \\ &\quad (PS + QR) + 2bRS]xy + \ (cQ^2 - 2aQS + bS^2)y^2 \\ &= -cx^2 - 2axy - by^2 (using\ (1), (4), (8)) \\ &= -(cx^2 - 2axy + by^2) \\ &= -f(x, y) \end{aligned}$$

Hence f is equivalent to $-f$.

Conversely, let $\alpha = \frac{a+\sqrt{p}}{c} \in Q^*(\sqrt{p})$ and the quadratic form $f(x, y) = cx^2 - 2axy + by^2$ is equivalent to $-f(x, y)$. We show that α is mapped onto $\bar{\alpha}$. Since the quadratic form $g(x, y) = cx^2 - 2axy + by^2$ is equivalent to $f(x, y) = -cx^2 + 2axy - by^2$, so there is an element $g = \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \in G$ such that $PS - QR = 1, P, Q, R, S \in Z$.

The co-efficients of g in terms of co-efficients of f are

$$c = cP^2 + 2aPR + bR^2 \tag{1}$$

$$-2a = -2cPQ + 2a(PS + QR) - 2bRS$$

or

$$-a = -cPQ + a(PS + QP) - bRS \tag{2}$$

$$b = -cQ^2 + 2aQS - bS^2$$

or

$$2aQs = b + bS^2 + cQ^2 \tag{3}$$

$$1 = PS - QR \tag{4}$$

Multiply (2) by S and (4) by $-cQ$ and subtracting

$$-aS = -cSPQ + aS(PS+QR) - bRS^2$$

$$\underline{\mp cQ = \mp cSPQ \qquad\qquad \pm cQ^2R}$$

$$\begin{aligned}
-aS + cQ &= aS(PS+QR) - bRS^2 - cQ^2R \\
&= aPS^2 + aSQR - bRS^2 - cQ^2R \\
&= aPS^2 + R(aSQ - bS^2 - cQ^2) \\
&= aPS^2 + R(b - aQS) \quad \textit{using } (3) \\
&= aPS^2 + bR - aQRS \\
&= aS(PS - QR) + bR \\
-aS + cQ &= aS + bR \\
2aS &= cQ - bR
\end{aligned}$$

Multiply it by Q

$$2aQS = cQ^2 - QRb$$

$$\underline{-2aQS = -cQ^2 \pm bS^2 \pm b}$$

$$0 = -QR - bS^2 - b$$

$$0 = -QR - S^2 - 1 \qquad \text{or} \qquad -1 = QR + S^2$$

$$-1 = QR + S^2$$

$$\underline{1 = -QR + PS}$$

$$\begin{aligned}
0 &= S^2 + PS \Rightarrow S(S+P) = 0, \quad S = 0 \quad \text{or} \quad P + S = 0 \\
S &= 0 \quad \text{or} \quad S = -P \\
\text{Put} \quad S &= -P \quad \text{in } (4) \\
I &= -P^2 - QR
\end{aligned}$$

$$I + P^2 = -QR \tag{5}$$

From (1)

$$\begin{aligned} c(1+P^2) &= R(2aP-bR) \\ c(-QR) &= R(2aP-bR) \quad using\ (5) \\ -cQ &= 2aP-bR \\ Q &= \frac{2aP-bR}{c} = \frac{1+P^2}{-R} \end{aligned}$$

$$PS-QR=1$$

$$-p^2-\left(\frac{2aP-bR}{-c}\right)R=1$$

or

$$\frac{2a}{c}PR-\frac{b}{c}R^2=1+P^2=-QR$$

$$\frac{2a}{c}\ P-\frac{b}{c}R+Q=0$$

$$p(\alpha+\bar{\alpha})-\alpha\bar{\alpha}R+Q=0$$

or

$$p\alpha+Q=-p\bar{\alpha}+\alpha\bar{\alpha}R$$

$$P\alpha+Q=\bar{\alpha}(-P+R\alpha)$$

or

$$\frac{P\alpha+Q}{R\alpha-P}=\bar{\alpha} \qquad \text{or} \qquad \frac{P\alpha+Q}{R\alpha-S}=\bar{\alpha}$$

Hence, α is mapped onto $\bar{\alpha}$

Theorem (B) Let $\bar{\alpha}$ be in the orbit of α^G that is, α is mapped onto $\bar{\alpha}$ under the action of modular group PSL $(2,Z)$ on $Q^*(\sqrt{p})$, where $\alpha=\frac{a+\sqrt{p}}{c}$ then $p\equiv 1$ (mod 4).

Proof Suppose that α is mapped onto $\bar{\alpha}$ under the action of modular group, then there exist an element $g=\begin{pmatrix} P & Q \\ R & S \end{pmatrix}\in G$ $P,Q,R,S\in Z$ and $PS-QR=1$ such that $g(\alpha)=\bar{\alpha}$. From theorem (A) we have $S=-P, Q=\frac{2aP-bR}{-c}$.

Now $PS - QR = 1$, forces that

$$-P^2 - \left(\frac{2aP - bR}{-c}\right) R = 1$$

$$\frac{2aPR}{c} - \frac{b}{c}R^2 = 1 + P^2$$

$$P\left(\frac{2a}{c}\right) R - \left(\frac{a^2 - p}{c^2}\right) R^2 = 1 + P^2 \qquad \therefore \; b = \frac{a^2 - p}{c}$$

$$\Rightarrow p\frac{R^2}{c^2} = P^2 - \frac{2a}{c}PR + \frac{a^2R^2}{c^2} + 1$$

$$p = \frac{c^2P^2}{R^2} - P\frac{2ac}{R} + a^2 + \frac{c^2}{R^2}$$

$$p = \left(\alpha - \frac{cP}{R}\right)^2 + \left(\frac{c}{R}\right)^2$$

Hence, by known results 1.1 and 1.2 we have $p \equiv 1 \pmod 4$.

REFERENCES

[1] Ivan Niven, Herbert S. Zuckerman, *The theory of numbers,* John Willey and Sonc Inc (1991).

[2] Willaim Judson Leveque, *Topics in number theory,* Volume 1, Addision Wesley Publishing Company, Inc. (1965).

[3] Q. Mushtaq, *Modular group acting on real quadratic fields,* Bull Austral Math Soc 37 (1988), 303-309.

[4] Q. Mushtaq, *Reduced Indefinite binary quadratic forms and orbits of the modular group,* Radovi Mathematicki Volume 4 (1988) 331-336.

[5] Imrana Kausar, S. M. Husnine, A. Majeed, *Behaviour of Ambiguous and Totally Negative elements of $Q^*(\sqrt{n})$ under the action of the Modular Group,* Punjab University Journal of Mathematics, Vol. XXX (*1997), 11-34.

[6] Imrana Kousar, S. M. Husnine, A. Majeed, *Action of the group* $H = < t, y : \; t^3 = y^3 = 1 >$ *on the Quadratic Fields,* Punjab University Journal of Mathematics, Vol. XXX (1997), 47-66.

[7] Imrana Kousar, S. M. Husnine, A. Majeed, *Classification of the elements of* $Q^*(\sqrt{p})$ *and a partition of* $Q^*(\sqrt{p})$ *under the action of Modular Group PSL (2, Z),* Punjab University Journal of Mathematics, Vol. XXXI(1998).

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 135–144

FIXED POINT AND BEST APPROXIMATION THEOREMS FOR *-NONEXPANSIVE MAPS

A. R. Khan
Department of Mathematical Sciences
King Faud University of Petroleum and Minerals
Dhahran 31261
Saudi Arabia
E-mail: arahim@kfupm.edu.sa
(On leave from Bahauddin Zakariya University, Multan 60800, Pakistan

N. Hussain
Center for Advanced Studies in Pure and Applied Mathematics
Bahauddin Zakariya University
Multan 60800, Pakistan
E-mail: mnawab@yahoo.com

(Received 20 May, 2000)

In this paper we obtain fixed point and best approximation theorems for

*-nonexpansive multivalued maps defined on a closed convex (not necessarily bounded) subset of a Banach space under certain boundary conditions. The results herein contain those of Husain and Tarafdar. Husain and Latif, Park, Singh and Watson, Xu and others.

We gather together some definitions and facts which will be used in this paper. Let C be a nonempty subset of a Banach space X. We denote by 2^X, $CB(X)$ and $K(X)$ the families of all nonempty, nonempty closed bounded and nonempty compact subsets of X respectively. The Hausdorff metric on $CB(X)$ induced by the metrix d on X is defined as

$$H(A,B) = \max\left\{ \sup_{a\epsilon A} d(a,B), \quad \sup_{b\epsilon B} d(b,A) \right\}$$

for A, B in $CB(X)$, where $d(a,B) = \inf_{b\in B} d(a,b)$.

A multivalued map $T : C \to CB(X)$ is called nonexpansive if $H(Tx,Ty) \le d(x,y)$ for all x, y in C. A multivalued map $T : C \to 2^X$ is said to be

(i) Weakly nonexpansive [4, 5] if given $x \in C$ and $u_x \in Tx$ there is a $u_y \in T_y$ for each $y \in C$ such that $d(u_x, u_y) \le d(x,y)$

(ii) *-nonexpansive [5, 14] if for all x, y in C and $u_x \in Tx$ with $d(x, u_x) = d(x, Tx)$ there exists $u_y \in Ty$ with $d(y, u_y) = d(y, Ty)$ such that $d(u_x, u_y) \le d(x,y)$.

(iii) Upper semicontinuous (usc) (lower semicontinuous (Isc)) if

$T^{-1}(B) = \{x \in C : \; Tx \cap B \neq \phi\}$ is closed (open) for each closed (open) subset B of X, T is continuous if T is both usc and Isc.

(iv) Weakly inward if $Tx \subset$ cl $(I_c(x))$ for all $x \in C$, where the inward set $I_C(x)$ of C at $x \in X$ is defined by $I_C(x) = \{x + \gamma(y - x) : y \in C \text{ and } \gamma \ge 0\}$ and 'cl' means taking closure.

(v) Satisfy the Leray-Schauder conditions (in case C has nonempty interior) if there is point z in interior of C such that for each $y \in Tx$.

$$y - z \neq \lambda(x - y) \quad \text{for all} \quad x \in BdC \quad \text{and} \quad \lambda > 1$$

For given $T : C \to 2^X$, we say that C is (KR)-bounded with respect to (w.r.t) T (cf. [8] and [10]) if for some bounded set $A \subset C$ the set

$$G(A) = \cap_{a\in A} G(a, Ta)$$

is either empty or bounded where $G(a, Ta) = \bigcup_{y\in Ta} G(a,y)$ and $G(a,y)$ $= \{z \in C : \|z - a\| \ge \|z - y\|\}$. In what follows, we denote by $P_T(x)$ the (possibly empty) set $\{u_x \in Tx : d(x, u_x) = d(x, T(x)\}$ for each $x \in X$ (cf. [14]). A single valued map $f : C \to X$ is said to be a selector of T if $f(x) \in Tx$ for each $x \in C$.

Bd, and Int, denote the boundary and interior respectively.

The concept of *-nonexpansiveness is different from continuity and hence nonexpansiveness for multivalued mappings $T : C \to 2^X$, as is clear from the following example.

Example Let $X = R^2$ be equipped with Euclidean norm and $C = \{(a,0) : 1/\sqrt{2} \le a \le 1\} \cup \{(0,0)\}$

Define $T : C \to 2^X$ by

$$T(a,0) = \begin{cases} (0,1), & \text{if } a \neq 0 \\ L = \text{the line Segment } [(0,1),(1,0)], & \text{if } a = 0 \end{cases}$$

The $P_T(a,0) = \{(0,1)\}$ for all $(a,0) \neq (0,0)$ in C and $P_T(0,0) = \{(1/2,1/2)\}$. This clearly implies that T is *-nonexpansive. But T is not continuous multifunction (cf. [12], p.537).

Also note that $u_x = (1,0) \in T(0,0)$. For any $y = (a,0) \in C$ with $a \neq 0$, $u_y = (0,1)$ such that $|u_x - u_y| = |(1,0)-(0,1)| = \sqrt{2} > |x-y|$. Thus T is not weakly nonexpansive.

A particular form of Theorem 4 due to Park [9] stated below will be needed (see also Theorem A[10]).

Theorem A Let X be a uniformly convex Banach space, C a nonempty closed convex subset of X and $f : C \to X$ a nonexpansive map such that C is (KR) -bounded. Suppose that one of the following holds:

(a) f is weakly inward.

(b) $0 \in \text{Int } C$ and $fx \neq \lambda$ for all $x \in BdC$ and $\lambda > 1$ (i.e. f satisfies Leray-Schauder condition).

Then f has a fixed point.

The following is due to Reich [11].

Theorem B Let C be a closed convex subset of a Banach space X such that the metric projection is usc. If $f : C \to X$ is continuous $f(C)$ is relatively compact, then there is a $y \in C$ such that $\|y - fy\| = d(fy, C)$.

Results The proof of following general theorem is based on Theorem A.

Theorem 1 Let C be a nonempty closed convex subset of a uniformly convex Banach space X and $T : C \to 2x$ closed convex valued *-nonexpansive map such that C is (KR) -bounded with respect to T. Then T has a fixed point under each one of the following boundary conditions.

(1) T is weakly inward.

(2) $\lim_{h\to 0+} d[(1-h)x + hy, C]/h = 0$ for all $x \in C$ and $y \in Tx$.

(3) $0 \in$ Int C and $y \neq \gamma x$ for all $x \in BdC, y \in T_x$ and $\gamma > 1$.

(4) $T(BdC) \subset C$.

Proof Since $T(x)$ is a nonempty closed convex subset of a uniformly convex Banach space X, therefore each u_x in $P_T(x)$ is unique. Thus by the definition of *-nonexpansiveness of T, there is $u_y = P_T(y) \in Ty$ for all y in C such that

$$\|P_T(x) - P_T(y)\| = \|u_x - u_y\| \leq \|x - y\|$$

So $P_T : C \to X$ is nonexpansive. The (KR) boundedness of C w.r.t. T clearly implies that C is (KR)-bounded w.r.t. P_T.

(1) As T is weakly inward so for each $x \in C$, $Tx \subset$ cl $(I_C(x))$. Since $P_T(x) \in Tx$ for each $x \in C$ therefore $P_T(x) \in$ cl $(I_C(x))$ for all $x \in C$. Hence $P_T : C \to X$ is weakly inward. Theorem A(a) implies that P_T has a fixed point. That is there is some x_0 in C such that $P_T(x_0) = x_0$. But $P_T(x) \in Tx$ for each $x \in C$ so $x_0 = P_T(x_0) \in T(x_0)$ as required.

(2) It is known (cf.[10]), p.654) that $f : C \to X$ is weakly inward if and only if $\lim_{h\to 0+} d[(1-h)x + hf(x), C]/h = 0$ for all x in a closed convex subset C of a Banach Space. As $P_T(x) \in T_x$ for all $x \in C$ so $\lim_{h\to 0+} d[(1-h)x + hP_T(x), C]/h = 0$ for $x \in C$. This implies that $P_T : C \to X$ is weakly inward. Now the result is obvious from (1).

(3) As $P_T(x) \in Tx, P_T(x) \neq \gamma x$ for all $x \in BdC$ can $\gamma > 1$. Thus P_T satisfies Leray- Schauder condition. So by Theorem $A(b)$, P_T and therefore T has a fixed

point.

(4) Since $C \subset I_C(x)$ for all $x \in C$ and $I_C(x) = X$ if x is an interior point, therefore T is weakly inward. The conclusion now follows from (1).

This completes the proof.

For single valued map T the concepts of nonexpansiveness and *-nonexpansiveness coincide. Thus we have the following;

Corollary 2 Let C be a nonempty closed convex subset of a uniformly convex Banach space X and $T : C \to X$ a nonexpansive map such that C is (KR)-bounded w.r.t. T. Then T has a fixed point provided one of the boundary conditions (1)-(4) of Theorem 1 holds.

Corollary 2 extends Theorem 3 (4), (8) and (LS) due to Park [10] from Hilbert space set up to that of uniformly convex Banach space. Here we also obtain conclusions of Corollary 15[3] and Remarks 3.9(iv) [15] when C is closed convex and (KR)-bounded.

In case $T : C \to 2^C$ in Theorem 1, we have;

Corollary 3 Let C be a nonempty closed convex subset of a uniformly convex Banach space X and $T : C \to 2^C$ a closed convex valued *-nonexpansive map such that C is (KR)-bounded w.r.t. T. Then T has a fixed point.

Remark 4(i) In Theorem 3.2 [5], the same conclusion was proved under assumptions of the boundedness of C and Opial's condition of X. Here we obtained the same conclusion if C is (KR)-bounded w.r.t. T.

(ii) Corollary 3 provides the conclusion of Corollary 1 [14] for uniformly convex Banach space X without the boundedness of C (see also Remark 3 [14]).

(iii) *-nonexpansive multivalued maps need not be continuous so Theorem 1 applies to the fixed point theory of multifunctions which are not necessarily continuous.

Corollary 5[1] Let C be a nonempty weakly compact convex subset of a uniformly convex Banach space and $T : C \to C$ a nonexpansive map. Then T has a fixed point.

Multivalued analogues of Ky Fan's best approximation theorem have been considered by researchers and interesting applications towards fixed point theory of multifunctions are given by them. We establish a version of this important theorm for *-nonexpansive multivalued maps as follows.

Theorem 6 Let C be a nonempty closed convex subset of a uniformly convex Banach space X. If $T : C \to 2^X$ is closed convex valued *-nonexpansive map and $T(C)$ is relatively compact, then T possesses a nonexpansive selector f such that

$$\|y - fy\| = d(fy, C) \quad \text{for some} \quad y \in C$$

If in addition $\|fy - Qfy\| = d(Ty, C)$ then $d(y, Ty) = d(Ty, C)$, where Q is projection map of X onto C.

Proof If C is closed and convex subset of a uniformly convex Banach space X, then the projection map $Q : X \to 2^C$ defined by

$$Q(x) = \{y \in C : \|x - y\| = d(x, C)\}$$

is single valued and continuous (see [12]), p.535). As in Theorem 1, $P_T : C \to X$ is nonexpansive selector of T. Since $T(C)$ is relatively compact and $P_T(C) \subseteq T(C)$, therefore $P_T(C)$ is relatively compact. By Theorem B, there exists $y \in C$ such that

$$\|y - P_T(y)\| = d(P_T(y), C)$$

By definition of P_T we have $d(x, P_T x) = d(x, U_x) = d(x, T_x)$ for each $x \in C$. Thus $d(y, P_T y) = d(y, Ty)$ and hence $d(y, Ty) = d(y, P_T y) = d(P_T y, C) = \|P_T y - Q\ P_T y\| = d(Ty, C)$ as desired.

If $T : C \to X$, then we have the following extension of Theorem 5 due to Singh and Watson [13].

Theorem 7 Let C be a nonempty closed convex subset of a uniformly convex Banach space X. If $T : C \to X$ is nonexpansive map and $T(C)$ is relatively compact, then there exists a point y in C such that

$$\|y - Ty\| = d(Ty, C)$$

As an application of Theorem 7, we get the following fixed point result, which generalized Theorem 6 and 7 [13].

Corollary 8 Let C be a nonempty closed convex subset of a uniformly convex Banach space X. If $T : C \to X$ is nonexpansive map, $T(C)$ is relatively compact and T satisfies any one of the following conditions:

(1) For each x on the boundary of C, $\|Tx - y\| \leq \|x - y\|$ for some y in C.

(2) For any u on the boundary of C with $u = Q_0T(u)$, that u is a fixed point of T.

Then T has a fixed point in C.

In case $T : C \to 2^C$ in Theorem 6, we have the following fixed point result for

*-nonexpansive maps which provides the same conclusion as of Cor. 3 with different conditions that $T(C)$ is relatively compact.

Corollary 9 Let Cbe a nonempty closed convex subset of a uniformly convex Banach space X and $T : C \to 2^C$ a closed convex valued *-nonexpansive map such that $T(C)$ is relatively compact. Then T admits a fixed point.

Note that if T is single valued then the conclusion of Corollary 5 holds for closed and convex set C.

Following generalizes Theorem 3.2[5], corresponding results in [4] and [6] and Theorem 2 by Xu [4].

Theorem 10 Let X be a Banach space satisfying Opial's condition and C be a weakly compact starshaped subset of X. Then each *-nonexpansive compact valued map $T : C \to 2^C$ has a fixed point.

Proof Since for each $x \in C, Tx$ is nonempty and compact so $P_T(x)$ is nonempty and compact. As in Theorem 1, $P_T : C \to 2^C$ is nonexpansive. Thus P_T and hence T has a fixed point by Corollary 3.11 [15].

Remarks 11 (i) If T is single valued, then the conclusion of Corollary 5 holds for weakly compact starshaped subset of a Banach space satisfying Opial's condition.

(ii) All Hilbert spaces and l^p spaces $(1 < p < \infty)$ satisfy Opial's condition but $L^p[0,1](p \neq 2)$ are uniformly convex Banach spaces which do not satisfy Opial's condition.

Acknowledgement The author A. R.Khan acknowledges gratefully the support provided by King Fahd University of Petroleum and Minerals during this research.

REFERENCES

[1] F. E. Browder, *Nonexpansive nonlinear Operators in a Banach space,* Proc. Nat. Acad. Sci. U.S.A., 54(1965), 1041-1044.

[2] F. E. Browder and W. V. Petryshyn, *Construction of fixed points of nonlinear mappings in Hilbert spaces,* J. Math. Anal., 20 (1967), 197-228.

[3] T. H. Chang and C.L. Yen, *Some fixed point theorems in Banach space,* J. Math. Anal. Apple. 138 (1989) 550-558.

[4] T. Husain and E. Tarafdar, *Fixed point theorems for multivalued mappings of nonexpansive type*, Yokoh. Math. J, 28 (1980) 1-6.

[5] T. Husain and A. Latif, *Fixed points of multivalued nonexpansive maps*, Math. Japonica, 33, No. 3 (1988), 385-391.

[6] T. Husain and A. Latif, *Fixed points of multivalued nonexpansive maps*, Intern. J. Math & Math. Sci, 14 (1991), 421-430.

[7] W. A. Kirk, *A fixed point theorem for mappings which do not increase distances,* Amer. Math. Monthly, 72(1965), 1004-1006.

[8] W. A. Kirk and W. O. Ray, *Fixed point theorems for mappings defined on*

unbounded sets in Banach spaces, Studia Math., 64 (1979), 127-138.

[9] Sehie Park, *On a problem of Gulevich on nonexpansive maps in uniformly convex Banach spaces, comment.* Math. Univ. Carolinae, 37 (1996), 263-268.

[10] —, *Best approximations and fixed points of nonexpansive maps in Hilbert spaces,* Numer. Funct. Anal. and Optimiz., 18 (5 & 6) (1997), 649-657.

[11] S. Riech, *Approximate selection, best approximations, fixed points and invariant sets,* J.Math. Anal. Appl, 62 (1978), 104-113.

[12] V. M. Sehgal and S. P. Singh, *A generalization to multifunctions of Fan's best approximation theorem,* Proc. Amer. Math. Soc., 102 (1988), 534-537.

[13] S. P. Singh and B. Watson, *Proximity maps and fixed points*, J. Approx. Theory 39 (1983), 72-76.

[14] H. K. Xu, *On weakly nonexpansive and *-nonexpansive multivalued mappings,* Math. Japonica, 36, No.3 (1991), 441-445.

[15] S. Zhang, *Star-shaped sets and fixed points of multivalued mappings,* Math. Japonica, 36, No. 2(1991), 327-334.

Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. xxxiii(2000) pp. 145–152

RSA CIPHERS WITH MAPLE

Farasat Tahir
Mathematics Department
Government Postgraduate College for Women
Satellite Town, Gujranwala (Pakistan)

Muhammad Tahir
Mathematics Department
Government College
Gujranwala (Pakistan)

(Received 27 August, 1999)

ABSTRACT Although other programming languages are equally good and can be used to handle RSA cipher, Maple provides a more friendly environment in computational works. This paper demonstrates how nicely RSA cipher system works with Maple.

1. INTRODUCTION The widespread use of electronic communications in a commercial environment means that a great deal of data which was sent in a fairly secure manner in the past is now sent by communications links to which many people potentially have access. The aim of security measure is to minimize the vulnerability of assets and resources hence there is a need for concealing the contents of a message and for detecting any tempering with a message. Ciphers are more universal methods of transforming messages into a format whose meaning is not apparent. The most important technique is RSA cipher. As far as RSA system is concerned, there is no faster method of attack than factorization. In 1988 Caron and Silverman managed to factorize a 90-digit number into two prime numbers of 41 and 49 digits, with the add of 24 SUN-workstations. The required processing time was about six weeks. In the same year Lenstra and Manasse successfully factorized a prime number of 96 digits. They employed a large number of computers, which were interconnected by a combination of local area networks and electronic mail. The whole operation took 23 days, which effectively worked out to 10 years of CPU time.

Despite the algorithms for reducing the total number of calculations, the RSA system still requires considerable computational power for processing such large numbers. For this reason in practice the RSA system is not especially well suited for real-time encryption of large amounts of data. The RSA system is therefore often used for enciphering limited amounts of data, for instance for the transportation of secret keys. In this paper we use Maple (computational package of mathematics) to program RSA cipher.

2. BASIC TERMINOLOGY We suppose that one person, the sender, wishes to send another person, the recipient, a message which he/she wants to keep secret from an eavesdropper. The message must be transmitted over an inseure channel, to which it must be presumed the eavesdropper has access. The message is called the plaintext. It is enciphered or encrypted by an algorithm or a set of rules called the encryption algorithm. This algorithm is controlled by a string of symbols called the key. The key is kept secret from every one except the sender and recipient and it should be easily changed in case it has somehow been discovered by the eavesdropper. The output from this algorithm is called the cipher, ciphertext or cryptogram. The inverse process called decryption or deciphering applies the same or a different mathematical function to change the ciphertext back to the original plaintext. It is also controlled by a key. The breaking of a cipher system by an eavesdropper is called cryptanalysis. The difference between cryptanalysis and decryption is that the cryptanalyst has to manage without the decryption key. A cipher system has following components:

1. plaintext message space, M.
2. ciphertext message space, C.
3. key space, K.
4. family of enciphering algorithms, $E_k : M \to C$, where $k \in K$.
5. family of deciphering algorithms, $D_k : C \to M$, where $k \in K$.

Cipher systems must satisfy three general requirements:

1. The enciphering and deciphering algorithms must be efficient for all keys.
2. The system must be easy to use.
3. The security of the system should depend only on the secrecy of the keys and not on the secrecy of the enciphering and deciphering algorithms.

Different cipher systems have different levels of security, depending on how hard they are to break. The security is directly related to the difficulty associated with inverting encryption transformation of a system. Now we will take a look at some methods used in encryption.

2.1. Simple-Substitution Cipher This cipher replaces each character of plaintext with a corresponding character called its substitute. A single one-to-one mapping from plaintext to ciphertext character is used to encipher an entire message.

2.2. Block Cipher Let M be aplaintext message. A block cipher breaks M into successive blocks $M_1, M_2, \cdots$, and enciphers each M_1 with the same key k. Each block is typically several characters long.

2.3. Running Key Cipher In a running-key cipher, the key is as long as the plaintext message. Assume that the letters of plaintext are represented by integers in the ciphertext. The letters are then regarded as integers from 1 to 26 with a = 1 and z = 26 and a blank space is given by the value 27.

2.4. Public Key Cipher In a public-key cryptosystem, the public- key algorithm uses an encryption key different from the decryption key. Since the public key is published, a stranger can use it to encrypt a message which can be decrypted only by the the owner of the private key. For this reason public-key systems are also referred to as non symmetric or one-way.

RSA Cipher [1] The RSA cipher named after its discoverers, Rivest, Shamir and Adleman. The RSA cipher is based on the fact that it is relatively easy to calculate the product of two prime numbers, but that determining the original prime numbers, given the product, is far more complicated.

The encryption and decryption procedure is as follows:

1. Find two large primes p and q, each about 100 digits long and define n by $n = pq$.

2. Compute the unique integer e in the range $1 \leq e \leq (p-1)(q-1)$ that is coprime to $(p-1)(q-1)$. This should be easy if e is prime and is not a factor of $(p-1)(q-1)$.

3. Finally the value of e is used to determine another number, d, for which $ed \equiv 1 \pmod{(p-1)(q-1)}$. The numbers n, e and d are referred to as the modulus, encryption and decryption exponents respectively.

4. Release the pair of integers (e, n) as public key while keeping the numbder d safe to decrypt.

5. Represent M, the message to be transmitted, into an integer, break M into blocks if it is too big.

6. Encrypt M into ciphertext C by the rule $C \equiv M^e \pmod{n}$.

7. Decrypt by using the private key d and the formula $D \equiv C^d \pmod{n}$.

Theorem [2] Consider a message M, which is enciphered according to the RSA system, resulting in a ciphertext $C \equiv M^e \pmod{n}$. The receiver deciphers this message into $D \equiv C^d \pmod{n}$, ensuring that $ed \equiv 1 \pmod{(p-1)(q-1)}$. Then for all cases: $D = M$.

The security of this system relies on the fact that it is almost impossible to calculate the value of d if only the public key (e, n) is known. Thus, the person who issues the public key (e, n) is the only person who knows the precise value of d and therefore also the only person able to decipher encrypted texts.

4. MAPLE WORKSHEET (RSA Cipher)

Computation of n and d

Enter any two large integers.

Now we have all the parameters for encryption and decryption. Load the Maple routines for encoding and decoding the message to number and number to message respectively. If the message is too long then break the message into successive blocks and encipher each block with the same key (e, n).

> read 'getnum.m': read 'getmess.m': # See Appendix

Example As an example we consider the message 'I am happy' and encode it as a number M.

> M := get _ number ('iamhappy'):

$$M := 9270113270801161625$$

Encrypt M into a cryptogram C.

> C :=Power (M, e) mod n;

$$C := 124585816767712890537317519095 9$$

Decrypt C by using the private key d.

> M :=Power (C, d) mod n;

$$M := 9270113270801161625$$

Get original message.

> get _ message (M);

i am happy

which was the original message.

Appendix

Maple routine for encryption:

> get _ number:=proc(msg)

> local II, nn, ss, ii, alpha;

> alpha: = table $['a' = 1,'b' = 2,'c' = 3,'d' = 4,'e' = 5,'f' = 6,'g' = 7,'h' = 8,'i' =$

> $9,'j' = 10,'k' = 11,'I' = 12,'m' = 13,'n' = 14,'o' = 15,'p' = 16,$

> $'q' = 17,'r' = 18,'s' = 19,'t' = 20,'u' = 21,'v' = 22,'w' = 23,'x' = 24,'y' = 25,'z' =$

```
> 26, => 27]) :
> if (not type(msg, string)) then ERROR('wrong number (or type) of arguments') fi;
> II:= length (msg);
> if II = 0 then RETURN (0) fi;
> nn:=1
> for ii from 1 to II do
>       ss:=alpha [substring(msg,ii..ii)];
>       if(not type(ss,numeric)) then ERROR('wrong number (or type) of arguments')fi;
>      nn:=100* nn + ss;
> od;
> end;
> save 'getnum.m':
```

Maple routine for decryption

```
> get-message: = proc(num)
> local ss, mm, II, ii, ans, a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,
> y,z,'',beta;
> beta:=table([1 = a,2 = b,3 = c,4 = d,5 = e,6 = f,7 = g,8 = h,9 = i,10 = j,11 =
> k,12 = I,
> 13 = m,14 = n,15 = o,16 = p,17 = q,18 = r,
> 19=s, 20=t, 21=u, 22=v, 23=w, 24=x, 25=y, 26=z, 27='']):
> mm:=num;
> if(not type(num,integer)) then ERROR('wrong number(or type) of arguments')fi;
> II = floor(trunc(evalf(log 10(mm)))/2)+1;
> ans:='';
> for ii from 1 to II do
>         mm:=mm/100
>        ss:=beta[frac(mm)*100];
>          if(not type(ss,string)) then ERROR('wrong number (or type) of arguments')
```

```
>            fi;
>         ans:=cat(ss,ans);
>        mm:=trunc(mm);
> od;
> ans;
> end;
> save 'getmess.m'.
```

REFERENCES

[1] Rivest, R.L., Shamir, A., and Adleman,L. *A method for obtaining digital signatures and public-key cryptosystems,* Communications of the ACM, 21, No.2, 1978,120-126.

[2] Van Der Lubbe, J.C.A. *Basic Methods of Cryptography,* Cambridge University Press, United Kingdom, 1998.

[3] Monagan, M.B., Geddes, K.O., Heal, K.M., Labahn, G., and Vorkoetter, S. *Maple V Programming Guide,* Springer-Verlag New York, 1996.

Published by Chairman Department of Mathematics for the University of the Punjab, Lahore-Pakistan

Composed by
Scholars Composing Centre
Muslim Town Mor, Lahore
042-7573130, 7533310

Printed by
ZEENINE Advertising
042-7569477

CONTENTS