Albanian Journal of Mathematics

Për një Shqipëri të shkencës dhe kulturës.

Volume 3, 2009

www.albanian-j-math.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 19–24
ISSN 1930-1235: (2009)

ON A GENERALIZED CLASS OF ANALYTIC FUNCTIONS WITH BOUNDED TURNING

Khalida Inayat Noor

COMSATS Institute of Information Technology
Mathematics Department
Islamabad, Pakistan
khalidanoor@hotmail.com

Abstract. In this paper, we consider the classes of analytic functions which are defined by conditions joining ideas of analytic functions with generalized bounded turning and bounded boundary rotation. Inclusion and radii results for these classes are studied.

1. Introduction

Let A denote the class of functions f, given by,

$$f(z) = z + \sum_{n=2}^{\infty} a_n z^n, \tag{1}$$

analytic in the unit disc $E = \{z : |z| < 1\}$. Let $P_k(\beta), k \geq 2, 0 \leq \beta < 1$, be the class of functions $p(z)$, with $p(0) = 1$, and defined as

$$p(z) = \left(\frac{k}{2} + \frac{1}{2}\right) p_1(z) - \left(\frac{k}{2} - \frac{1}{2}\right) p_2(z), \tag{2}$$

where $Re\{p_i(z)\} > 0, \quad i = 1, 2$, and $z \in E$.

The class $P_k(0) \equiv P_k$ was introduced in [4], and $P_2(0) \equiv P$ is the class of functions with positive real part.

Let

$$J(\alpha, f) = (1 - \alpha) f'(z) + \alpha \left(1 + \frac{z f''(z)}{f'(z)}\right), \tag{3}$$

for α real and $f \in A$.

Then we define the classes $N_\alpha(k, \beta)$ and $P_k^{'}(\beta)$, for $0 \leq \beta < 1$, as follows.

$$\begin{aligned} N_\alpha(k, \beta) &= \{f \in A, \quad J(\alpha, f) \in P_k(\beta), \quad z \in E\} \\ P_k^{'}(\beta) &= \{f \in A, \quad f' \in P_k(\beta), \quad z \in E\}. \end{aligned}$$

We note that $N_1(k, 0) \equiv V_k$, the well-known class of functions with bounded boundary rotation and with $k = 2$, we obtain the class $N_\alpha(2, \beta) \equiv H_\alpha(\beta)$ discussed in

2000 *Mathematics Subject Classification.* Primary 30C45; Secondary 93C50.
Key words and phrases. Analytic functions; bounded turning; convolution; positive real part.

[6]. The class $N_0(2,0) \equiv P_2^{'}(2)$ is the class $P^{'}$ consisting of functions with bounded turning [1, p 101].

Lemma 1.1[2]. Let $u = u_1 + iu_2$ and $v = v_1 + iv_2$ and $\Psi(u,v)$ be a complex -valued function satisfying the conditions:
(i). $\Psi(u,v)$ is continuous in a domain D
(ii). $(1,0) \in D$ and $\Psi(1,0) > 0$.
(iii). $Re\{\Psi(iu_2, v_1) \leq 0$ whenever $(iu_2, v_1) \in D$ and $v_1 \leq \frac{-1}{2}(1+u_2^2)$.

Let $p(z) = 1 + c_1 z + c_2 z^2 + \ldots$, regular in the unit disc E, such that $(p(z), zp'(z)) \in D, \quad \forall z \in E$. If $Re\{\Psi(p(z), zp'(z))\} > 0$ for $z \in E$, then $Rep(z) > 0, \quad z \in E$.

Lemma 1.2 [5]. Let p be analytic function in E with $p(0) = 1$ and $Re\{p(z)\} > 0, \quad z \in E$. Then, for $s > 0$ and $\nu \neq -1$(complex),

$$Re\left\{p(z) + \frac{szp'(z)}{p(z)+\nu}\right\} > 0,$$

for $|z| < r_0$, where r_0 is given by

$$\begin{aligned} r_0 &= \frac{|\nu+1|}{\sqrt{A + \sqrt{(A^2 - |\nu^2 - 1|^2}}}, \\ A &= 2(s+1)^2 + |\nu|^2 - 1, \end{aligned}$$

and this radius is best possible.

2. Main Results

Theorem 2.1. For $0 < \alpha \leq \gamma \leq \frac{3}{2}\alpha < 1, \quad N_\alpha(k,\gamma) \subset P_k^{'}(\beta)$, where

$$\beta = \beta(\alpha,\gamma)\left[\frac{2\alpha}{(2\alpha-\gamma) + \sqrt{(2\alpha-\gamma)^2 + 4\alpha(1-\alpha)}}\right]. \tag{4}$$

Proof. Let $f \in N_\alpha(k,\gamma)$. Then $J(\alpha, f) \in P_k(\gamma), \quad z \in E$. Let

$$f'(z)p(z) = (1-\beta)h(z) + \beta. \tag{5}$$

where $p(z), h(z)$ are analytic in E and $p(0) = h(0) = 1$.

From definitions and (5), we have

$$\left[\frac{1-\alpha}{1-\gamma}p(z) + \frac{\alpha}{(1-\gamma)}\left\{1 + \frac{zp'(z)}{p(z)}\right\} - \frac{\gamma}{1-\gamma}\right] \in P_k, \quad z \in E. \tag{6}$$

We can write

$$\begin{aligned} \left[\tfrac{1-\alpha}{1-\gamma}p(z) + \tfrac{\alpha}{1-\gamma}\right] &= \tfrac{1-\alpha}{1-\gamma}\left[p(z) + \tfrac{\frac{\alpha}{1-\alpha}zp'(z)}{p(z)}\right] \\ &= \tfrac{(1-\alpha)(1-\beta)}{(1-\gamma)}\left[h(z) + \tfrac{\alpha}{(1-\alpha)(1-\beta)}\tfrac{zh'(z)}{h(z)+\frac{\beta}{1-\beta}} + \tfrac{\beta}{1-\beta}\right]. \end{aligned} \tag{7}$$

Let

$$\begin{aligned}\frac{\alpha}{(1-\alpha)(1-\beta)} &= \alpha_1, \quad \frac{\beta}{1-\beta}=\beta_1,\\ h(z) &= \left(\frac{k}{4}+\frac{1}{2}\right)-\left(\frac{k}{4}-\frac{1}{2}\right)\Longrightarrow\\ \Longrightarrow h(z) &= \left(\frac{k}{4}+\frac{1}{2}\right)h_1(z)-\left(\frac{k}{4}-\frac{1}{2}\right)h_g(z)\end{aligned}$$

Define

$$\Phi_{\alpha_1,\beta-1}(z)=\frac{1}{1-\beta_1}\frac{z}{(1-z)^{\alpha_1+1}}+\frac{\beta_1}{1+\beta_1}\frac{z}{(1-z)^{\alpha_1+2}}.$$

Then, using convolution technique, we have

$$\begin{aligned}\left(h\star\frac{\Phi_{\alpha_1,\beta_1}}{z}\right)(z) &= \left[h(z)+\frac{\alpha_1 z h'(z)}{h(z)+\beta_1}\right]\\ &= \left(\frac{k}{4}+\frac{1}{2}\right)\left\{h_1(z)+\frac{\alpha_1 z h_1'(z)}{h_1(z)+\beta_1}\right\}\\ &\quad -\left(\frac{k}{4}-\frac{1}{2}\right)\left\{h_2(z)+\frac{\alpha_1 z h_2'(z)}{h_2(z)+\beta_1}\right\}.\end{aligned}\tag{8}$$

Thus, using (7) and (8), we can write (6) as

$$\begin{aligned}&\frac{(1-\alpha)(1-\beta)}{(1-\gamma)}\left[\left(\frac{k}{4}+\frac{1}{2}\right)\left\{h_1(z)+\frac{\alpha_1 z h_1'(z)}{h_1(z)+\beta_1}+\frac{\alpha-\gamma+\beta(1-\alpha)}{(1-\alpha)(1\beta)}\right\}\right]\\ &-\frac{(1-\alpha)(1-\beta)}{(1-\gamma)}\left[\left(\frac{k}{4}-\frac{1}{2}\right)\left\{h_2(z)+\frac{\alpha_1 z h_2'(z)}{h_2(z)+\beta_1}+\frac{\alpha-\gamma+\beta(1-\alpha)}{(1-\alpha)(1-\beta)}\right\}\right]\end{aligned}$$

and therefore it follows that

$$Re\left\{h_i+\frac{\alpha_1 z h_i'(z)}{h_i+\beta_1}+\frac{\alpha-\gamma+\beta(1-\alpha)}{(1-\alpha)(1-\beta)}\right\}>0, \quad z\in E.\tag{9}$$

We now formulate the functional $\Psi(u,v)$ by taking $u=h_i, \quad v=zh_i'$ in (9) and note that the first two conditions of Lemma 1.1 are clearly satisfied. We verify condition (iii) as follows.

$$\begin{aligned}Re\left\{\Psi(iu_2,v_1)\right\} &= \frac{\frac{\alpha}{(1-\alpha)(1-\beta)}\left(\frac{\beta}{1-\beta}\right)v_1}{\left(\frac{\beta}{1-\beta}\right)^2+u_2^2}+\frac{(\alpha-\beta)+\beta(1-\alpha)}{(1-\alpha)(1-\beta)}\\ &\leq \frac{\frac{-\alpha\beta}{1-\beta}\left(1+u_2^2\right)+2\left[\frac{\beta^2}{(1-\beta)^2}+u_2^2\right][\alpha-\gamma+\beta(1-\alpha)]}{2(1-\alpha)(1-\beta)\left[\left(\frac{\beta}{1-\beta}\right)^2+u_2^2\right]}\\ &= \frac{A_1+Bu_2^2}{2C},\end{aligned}$$

where

$$\begin{aligned} A_1 &= \frac{-\alpha\beta}{1-\beta} + \frac{2\beta^2}{(1-\beta)^2}\left[\alpha-\gamma+\beta(1-\alpha)\right] \\ B &= \frac{-\alpha\beta}{1-\beta} + 2\left[(\alpha-\gamma)+\beta(1-\alpha)\right], \\ C &= (1-\alpha)(1-\beta)\left[\left(\frac{\beta}{1-\beta}\right)^2 + u_2^2\right] > 0. \end{aligned}$$

Now $Re\{\Psi(iu_2, v_1)\} \leq 0$ if $A_1 \leq 0$ and $B \leq 0$. For $A_1 \leq 0$, we find β as given by (4) with $0 < \alpha \leq \gamma \leq \frac{3}{2}\alpha < 1$ and $B \leq 0$ gives us $0 < \beta < 1$. This shows that condition (iii) of Lemma 1.1 holds. Applying Lemma 1.1, we see that

$$Re\{h_i(z)\} > 0; \quad i = 1, 2, \quad z \in E.$$

Consequently $h \in P_k$ and therefore $p \in P_k(\beta)$, where β is given by (4) This completes the proof. □

We now discuss some special cases.

Special Cases

(i) Let $\alpha = \gamma$ Then $\beta = \frac{2\alpha}{\alpha+\sqrt{\alpha(4-3\alpha)}}$. This improves a result proved in [6] for the case $k = 2$.

(ii) Let $\gamma = \frac{3}{2}\alpha$. Then we have $\beta = \frac{4\alpha}{\alpha+\sqrt{\alpha(16-15\alpha)}}$.

By taking $\alpha = \frac{1}{2}$, we get $\beta = \frac{4}{1+\sqrt{7}}$. If we take $\beta = 0$ and $\alpha \leq \gamma < 1$, then $A_1 = 0, \quad B = 2(\alpha-\gamma) \leq 0$ and Lemma 1.1. is applicable. This gives a result proved in [6] for $k = 2$.

With similar technique used in Theorem 2.1, we can easily prove the following.

Theorem 2.2. Let, for $0 < \alpha < 1, \quad f \in N_\alpha(k, \frac{1}{2})$. Then $f \in P_k^{'}(\frac{1}{2}), \quad z \in E$.

Theorem 2.3. For $0 \leq \alpha_2 < \alpha_1 < 1, \quad N_{\alpha_1}(k, \frac{1}{2}) \subset N_{\alpha_2}(k, \frac{1}{2})$.

Proof. Since

$$(1-\alpha_2)f'(z) + \alpha_2(1+\frac{zf''(z)}{f'(z)} = \left(1-\frac{\alpha_2}{\alpha_1}\right)f'(z) + \frac{\alpha_2}{\alpha_1}\left[(1-\alpha_1)f'(z) + \alpha_1\left(1+\frac{zf''(z)}{f'(z)}\right)\right],$$

the result follows by using Theorem 2.2 and the fact that $P_k(\frac{1}{2})$ is a convex set, see [3]. □

Theorem 2.4. Let, for $0 < \alpha < 1, \quad 0 \leq \beta < 1, \quad f \in P_k^{'}(\beta$. Then $\quad f \in N_\alpha(k, \beta_1)$, for $|z| < r_0$, where

$$\beta_1 = \beta + \alpha(1-\beta),$$

r_0 is given as in Lemma 1.2 with

$$s = \frac{a\alpha}{(1-\alpha)(1-\beta)}, \quad \nu = \frac{\beta}{1-\beta}.$$

The value of r_0 is exact.

Proof. Let $f \in P_k^{'}(\beta)$. Then

$$f'(z) = (1-\beta)p(z) + \beta, \quad p \in P_k. \tag{10}$$

Now

$$J(\alpha, f) = (1-\alpha)f'(z) + \alpha\left(1 + \frac{zf''(z)}{f'(z)}\right).$$

Using (10), we have

$$\frac{1}{(1-\alpha)(1-\beta)}\left[J(\alpha, f) - \{\beta + \alpha(1-\beta)\}\right] = p(z) + \frac{\frac{\alpha}{(1-\alpha)(1-\beta)}zp'(z)}{p(z) + \frac{\beta}{1-\beta}}.$$

This gives us

$$\frac{1}{1-\beta_1}\left[J(\alpha, f) - \beta_1\right] = p(z) + \frac{szp'(z)}{p(z)+\nu},$$

where

$$\beta_1 = \beta + \alpha(1-\beta), \quad s = \frac{\alpha}{(1-\alpha)(1-\beta)}, \quad \nu = \frac{\beta}{1-\beta}.$$

Writing

$$p(z) = \left(\frac{k}{4} + \frac{1}{2}\right)p_1(z) - \left(\frac{k}{4} - \frac{1}{2}\right)p_2(z)$$

and using convolution technique as before, we can write

$$\begin{aligned}\frac{1}{1-\beta_1}\left[J(\alpha, f) - \beta_1\right] &= \left(\frac{k}{4} + \frac{1}{2}\right)\left[p_1(z) + \frac{szp_1'(z)}{p_1(z)+\nu}\right] \\ &\quad - \left(\frac{k}{4} - \frac{1}{2}\right)\left[p_2(z) + \frac{szp_1'(z)}{p_2(z)+\nu}\right], \quad p_i \in P, \quad i = 1, 2. \end{aligned} \tag{11}$$

We now apply Lemma 1.2 to have

$$Re\left\{p_i(z) + \frac{szp_i'(z)}{p_i(z)+\nu}\right\} > 0$$

for $|z| < r_0$, and using this in (11), we obtain the required result. □

As a special case, with $\beta = \frac{1}{2}$, $\alpha = \frac{1}{2}$, we note that $f \in P_k^{'}(\frac{1}{2})$ implies that $f \in N_{\frac{1}{2}}(k, \frac{3}{4})$ for $|z| < r_0$, where

$$r_0 = \frac{2}{\sqrt{\frac{9}{2} + \sqrt{\frac{81}{4}}}} = \frac{2}{3}.$$

We can prove easily the following special case independently.

Theorem 2.5. Let $f \in P_k^{'}(\frac{1}{2})$. Then $f \in N_{\frac{1}{2}}(k, \frac{1}{2})$ for $|z| < \frac{1}{2}$. The value $\frac{1}{2}$ is exact.

Acknowledgement. The author would like to thank Dr. S. M. Junaid Zaidi, Rector, CIIT, for providing excellent research facilities.

References

[1] A. W. Goodman, Univalent Functions, Vol. I, II, Polygonal Publishing House, New Jersey, 1983.
[2] S. S. Miller, Differential inequalities and Caratheodory functions, Bull. Amer. Math. Soc. **81**(1975), 79-81.
[3] K. Inayat Noor, On subclasses of close-to-convex functions of higher order, Inter. J. Math. Math. Sci. **15**(1992), 279-290.
[4] B. Pinchuk, Functions with bounded boundary rotation, Isr. J. Math. **10**(1971), 7-16.
[5] S. Ruscheweyh and V. Singh, On certain extremal problems for functions with positive real part, Proc. Amer. Math. Soc., **61**(1976), 329-334.
[6] S. Singh, S. Gupta and S. Singh, On a problem of univalence of functions satisfying a differential inequality, Math. Inequal. Appl. **10**(2007), 95-98.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 3–11
ISSN 1930-1235: (2009)

RANK 2 ARITHMETICALLY COHEN-MACAULAY VECTOR BUNDLES ON $K3$ AND ENRIQUES SURFACES

E. Ballico

Dept. of Mathematics
University of Trento
38050 Povo (TN), Italy
ballico@science.unitn.it

Abstract. Here we study arithmetically Cohen-Macaulay rank 2 vector bundles with trivial determinant on $K3$ and Enriques surfaces.

1. Introduction

Let X be either an Enriques surface or a $K3$-surface defined over an algebraically closed field $\mathbb{K}$ such that $\mathrm{char}(\mathbb{K}) \neq 2$. Let η_+ denote the set of all ample line bundles on X. Let E be any vector bundle on X. We will say that E is WACM or that it is *weakly arithmetically Cohen-Macaulay* if $h^1(X, E \otimes L) = h^1(X, E \otimes L^*) = 0$ for all $L \in \eta_+$. We will say that E is ACM or that it is *arithmetically Cohen-Macaulay* if it is WACM and $h^1(X, E) = 0$. We will say that E is SACM or that it is *strongly arithmetically Cohen-Macaulay* if it is ACM and $h^1(X, E \otimes \omega_X) = 0$. Hence on a $K3$ surface a vector bundle is ACM if and only if it is SACM. This definition is very natural, but different from the usual one (unless X is a $K3$ surface with $\mathrm{Pic}(X) \cong \mathbb{Z}$) in which we fix an ample $H \in \mathbb{Z}$ and only require $h^1(X, E \otimes H^{\otimes t}) = 0$ for all $t \in \mathbb{Z}$ (see [6] and references therein for many papers using the classical definition on varieties with $\mathrm{Pic}(X) \neq \mathbb{Z}$). To state our results we introduce a few definitions. We recall that an Enriques surface X is said to be *nodal* if there is an integral curve T such that $T^2 < 0$. A generic Enriques surface is not nodal ([3], Th. 4).

Theorem 1. *Let X be a non-nodal Enriques surface and E a rank 2 ACM vector bundle on X such that $\det(E) \cong \mathcal{O}_X$. Then one of the following cases occurs.*

(i) *$c_1(E) = 1$ and E is a member of the family of ACM vector bundles described in Example 1;*
(ii) *E is an extension of a line bundle A^* by its dual A.*

In case (ii) $c_2(E) = -A^2$ is an even integer. If $E \neq A \oplus A^*$ and we are in case (ii), then $c_2(E) \in \{0, 2\}$.

1991 *Mathematics Subject Classification.* 14J28; 14J60.
Key words and phrases. vector bundle; ACM vector bundle; arithmetically Cohen-Macaulay vector bundle; Enriques surface; $K3$-surface.
The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

Roughly speaking, the family $\{E_1\}$ of ACM vector bundles described in Example 1 depends from two parameters: each E_1 uniquely determines a point $Z \in X$ and a very general point $Z \in X$ determines one of these vector bundles.

We will say that a $K3$-surface X has Property (+) if X contains no smooth rational curve, i.e. (adjunction formula) no integral curve T such that $T^2 = -2$. The adjunction formula shows that X has Property (+) if and only if there is no effective divisor D on X such that $D^2 < 0$. Hence X has Property (+) if and only if every effective divisor is nef. If $\mathbb{K} = \mathbb{C}$, then a global Torelli theorem makes easy to construct $K3$-surfaces with Property (+) (see [7], Lemma 4.3, for a construction of an elliptic $K3$ surface with $\rho = 2$ and Property (+)).

Theorem 2. *Let X be a $K3$-surface with Property (+) and not quasi-elliptic. Let δ be the minimal self-intersection of an ample line bundle on X. δ is a positive even integer. Let E be a rank 2 ACM vector bundle on X such that $\det(E) \cong \mathcal{O}_X$. Then one of the following cases occurs:*

(i) *There is an integer t such that $2 \le t \le \delta/2 + 2$ and E is one of the vector bundles E_t described in Example 2; in this case $c_2(E) = t$;*
(ii) *E is an extension of a line bundle A^* by its dual A.*

In case (ii) $c_2(E) = -A^2$ is an even integer. If $E \neq A \oplus A^*$ and we are in case (ii), then $c_2(E) \in \{0, 2, 4\}$.

If $\mathrm{char}(\mathbb{K}) \neq 2, 3$, then no surface is quasi-elliptic. Fix any integer t such that $2 \le t \le \delta/2 + 2$. Roughly speaking, the set $\{E_t\}$ of ACM vector bundles described in Example 2 for the integer t depends from $2t+(t-1)$ parameters: each E_t uniquely determines a length t zero-dimensional subschemes of X and a very general length t zero-dimensional subschemes of X determines a $(t-1)$-dimensional family of non-isomorphic bundles contained in the set $\{E_t\}$.

Remark 1. Let X be a $K3$-surface with Property (+). Assume that X has no elliptic pencil. Equivalently, assume that there is no integral curve T such that $T^2 \le 0$. If this condition is satisfied we will say that X has Property (++). Assume that X has Property (++). This assumption implies that every effective divisor $D \neq 0$ on X is nef and big. We have $h^0(X, D) \ge D^2/2 + 2$ and hence the linear system $|D|$ covers X. Fix any integral curve $T \subset X$. If T is not contained in a divisor of $|D|$, then $D \cdot T > 0$, because $|D|$ covers X. If T is contained in a divisor of $|D|$, then $D \cdot T > 0$, because $T^2 > 0$. Hence D is ample by Nakai criterion ([5], Th. 1.5.1). Use also Riemmann-Roch to see that if X has Property (++) and $L \in \mathrm{Pic}(X)$, then the following conditions are equivalent:

(i) $L \in \eta_+$;
(ii) $h^0(X, L) > 0$ and $L \neq \mathcal{O}_X$;
(iii) $h^0(X, L) \ge 2$;
(iv) $L^2 \ge 0$, $L \neq \mathcal{O}_X$, and $L^* \notin \eta_+$;
(v) $L^2 > 0$ and $L^* \notin \eta_+$.

Theorem 3. *Let X be a $K3$-surface with Property (++). Let E be a rank 2 vector bundle on X such that $\det(E) \cong \mathcal{O}_X$ and $c_2(E) \le 0$. Then one of the following cases is true:*

(i) *$E \cong \mathcal{O}_X^{\oplus 2}$;*
(ii) *E there is $L \in Pic(X)$ such that L is ample and ACM, $c_2(E) = -L^2 < 0$ and $E \cong L \oplus L^*$.*

2. X an Enriques surface

In this section X is an Enriques surface defined over an algebraically closed field $\mathbb{K}$ such that $\mathrm{char}(\mathbb{K}) \neq 2$. Hence $\omega_X \neq \mathcal{O}_X$ and $\omega_X^{\otimes 2} \cong \mathcal{O}_X$ ([4], p. 76). Since $\mathrm{char}(\mathbb{K}) \neq 2$, $h^i(X, \mathcal{O}_X) = 0$ for $i = 1, 2$, $\omega_X \neq \mathcal{O}_X$ (i.e. ω_X has order 2) and ω_X is the only non-trivial torsion line bundle on X ([4], p. 76). The intersection product on $NS(X)$ is a perfect pairing of $\mathbb{Z}$-modules ([4], p. 78).

Let $T \subset X$ be an integral curve such that $T^2 < 0$. Since $T \cdot \omega_X = 0$, $T^2 = -2$ and $p_a(T) = 0$, i.e. $T \cong \mathbf{P}^1$. X is said to be *nodal* if there is an integral curve T such that $T^2 < 0$. A generic Enriques surface is not nodal ([3], Th. 4).

For any $M \in \mathrm{Pic}(X)$ and any rank 2 vector bundle E on X Riemann-Roch says $\chi(M) = M^2/2 + 1$ and $\chi(E) = c_1(E)^2/2 - c_2(E) + 2$. Fix any $L \in \eta_+$. Kodaira vanishing gives $h^i(X, L^*) = 0$, $i = 0, 1$ (see [3], Th. 2.6, when L is nef and big). Nakai criterion of ampleness ([5], I.5.1) shows that $\omega_X \otimes L$ is ample. Hence Kodaira vanishing ([3], Th. 2.6) and Serre duality gives $h^i(X, L) = 0$, $i = 1, 2$. Hence Rieman-Roch gives $h^0(X, L) = 1 + L^2/2$. We just checked that both $\mathcal{O}_X$ and ω_X are SACM.

Remark 2. Fix any $A \in \mathrm{Pic}(X)$. Serre duality gives that A is SACM if and only if both A and A^* are ACM.

Example 1. Fix an integer $t \geq 2$ and $L \in \eta_+$ such that $L^2/2 + 1 \geq t$. We just saw that $h^0(X, L) = L^2/2 + 1$. Since $t \leq h^0(X, L)$ and $h^1(X, L) = 0$, we have $h^1(X, \mathcal{I}_Z \otimes L) = 0$ for a general $Z \subset X$ such that $\sharp(Z) = t$. Now assume that $\mathbb{K}$ is uncountable. Since $\mathrm{Pic}^0(X)$ is countable, there are only countably many ample line bundles on X. Hence there is a non-empty set W_t of the Hilbert scheme $\mathrm{Hilb}^t(X)$ of all zero-dimensional length t subschemes of Z such that $\mathrm{Hilb}^t(X) \backslash W_t$ is a union of countably many proper algebraic subsets of $\mathrm{Hilb}^t(X)$, each $Z \in W_t$ is locally a complete intersection and $h^1(X, \mathcal{I}_Z \otimes L) = 0$ for all $L \in \eta_+$ such that $L^2/2 + 1 \geq t$ and all $Z \in W_t$. Fix any $Z \in W_t$ and consider the general extension

$$0 \to \mathcal{O}_X \to E_t \to \mathcal{I}_Z \to 0 \tag{1}$$

Since $h^0(X, \omega_X) = 0$, the Cayley-Bacharach condition is satisfied ([1], Th. 1.4) and hence E_t is locally free. Since $h^1(X, \mathcal{O}_X) = 0$, [1], Th. 1.4, gives that the set of all non-trivial extensions is parametrized by a $(t-1)$-dimensional projective space. Two non-proportional extensions gives non-isomorphic vector bundles, because $h^0(X, E_t) = 1$ and hence each E_t fits in a unique extension (1). In particular, if $t = 1$, then the point Z gives, up to isomorphisms, a unique vector bundle E_t. Now take any t. Since $Z \neq \emptyset$, $h^0(X, E_t) = 1$. Thus E_t uniquely determines Z as the scheme-theoretic locus at which any non-zero section of E_t drops rank. We have $\det(E_t) \cong \mathcal{O}_X$, $c_2(E_t) = t$ and E_t is slope properly semistable with respect to any polarization on X. Since $\mathcal{O}_X$ is spanned, $h^0(X, \mathcal{O}_X) = 1$ and $h^1(X, \mathcal{O}_X) = 0$, we have $h^1(X, \mathcal{I}_Z) = t - 1$. Hence (1) gives $h^1(X, E_1) = 0$ and $h^1(X, E_t) = t - 1 > 0$ if $t > 1$. Fix $L \in \eta_+$. We saw that $h^1(X, L) = 0$. Since $Z \in W_t$, $h^1(X, \mathcal{I}_Z \otimes L) = 0$. Hence $h^1(X, E_t \otimes L) = 0$. Since $\det(E_t) \cong \mathcal{O}_X$ and $\mathrm{rank}(E_t) = 2$, $E_t^* \cong E_t$. Hence $h^1(X, E \otimes L^*) = h^1(X, E \otimes (L \otimes \omega_X))$. Since $L \otimes \omega_X \in \eta_+$ by Nakai criterion of ampleness ([5], I.5.1), we get that E_t is WACM and it is ACM if and only if $t = 1$. Tensor the case $t = 1$ of (1) with ω_X. Since $h^0(X, \omega_X) = h^1(X, \omega_X) = 0$, we get $h^1(X, E_1 \otimes \omega_X) = 1$. Hence E_1 is not SACM. Obviously, if E_t is as above, then $E_t \otimes \omega_X$ is WACM. Since $\mathrm{rank}(E) = 2$ and

$\omega_X^{\otimes 2} \cong \mathcal{O}_X$, $\det(E_t \otimes \omega_X) \cong \mathcal{O}_X$. Hence $(E_t \otimes \omega_X)^* \cong E_t \otimes \omega_X$. By tensoring (1) with the numerically trivial line bundle ω_X we get $c_2(E_t \otimes \omega_X) = t$. Serre duality gives $h^1(X, E_t \otimes \omega_X) = h^1(X, (E_t \otimes \omega_X)^* \otimes \omega_X) = h^1(X, E_t)$. Hence $E_t \otimes \omega_X$ is ACM if and only if $t = 1$. $E_t \otimes \omega_X$ is properly semistable in the sense of Mumford-Takemoto with respect to any polarization of X. By tensoring (1) with ω_X we get that $h^0(X, E_t \otimes \omega_X) = 0$. Hence E_t and $E_t \otimes \omega_X$ are not isomorphic. Now assume $t \geq 2$. Fix any $Z \in W_t$ and consider a general extension

$$0 \to \omega_X \to G_t \to \mathcal{I}_Z \to 0 \tag{2}$$

Since $h^0(X, \mathcal{I}_{Z'}) = 0$ for any length $t-1$ subscheme Z' of Z, the Cayley-Bacharach condition is satisfied and hence G_t is locally free. We need to exclude the case $t = 1$, because in this case the Cayley-Bacharach condition is not satisfied and hence the middle term of any such extension is not locally free. $\det(G_t) \cong \omega_X$ and $c_2(G_t) = t$. As above we see that G_t is WACM, but not ACM. G_t is properly semistable with respect to any polarization of X. Again, each Z_t determines a $(t-1)$-dimensional family of vector bundles G_t and each of them uniquely determine Z as the scheme at which any non-zero section of $H^0(X, G_t \otimes \omega_X^*)$ drops rank. Fix $H \in \eta_+$.

Claim: E_t and G_t are not an extensions of two line bundles.

Proof of the Claim: We will only write down the proof for E_t, since the one for G_t requires only notational modifications (e.g. using $h^0(X, G_t \otimes \omega_X)$ instead of $h^0(X, E_t)$). In order to obtain a contradiction we assume that E is an extension of a line bundle M^* by M. Here we use $\det(E_t) \cong \mathcal{O}_X$. Set $z := M \cdot H$. Notice that E_t is properly H-semistable. Hence $z \leq 0$. Since $h^0(X, E_t) > 0$, either $h^0(X, M) > 0$ or $h^0(X, M^*) > 0$. First assume $z < 0$. Hence $h^0(X, M) = 0$. Thus $h^0(X, M^*) > 0$. However, any non-zero section σ of E drops rank exactly at the non-zero zero-dimensional scheme Z. Since $h^0(X, M) = 0$, σ drops rank on the zero locus D of the section σ' of M^* induced by σ. Since D has pure codimension one, we got a contradiction. Now assume $z = 0$. Since $H \in \eta_+$, $H \cdot M^* = -H \cdot M = 0$, and $h^0(X, M) + h^0(X, M^*) > 0$, M must be trivial. Thus $c_2(E_t) = 0$, contradiction.

Proposition 1. *Fix an integer $t \geq 2$ and $L \in \eta_+$. The following conditions are equivalent:*

(a) $t \leq L^2/2 + 1$;
(b) $h^1(X, E_t \otimes L) = 0$;
(c) $h^1(X, E_t \otimes L^*) = 0$;
(d) $h^1(X, G_t \otimes L) = 0$;
(e) $h^1(X, G_t \otimes L^*) = 0$.

Proof. We will do the proofs for E_t, since the proofs for G_t require only notational modifications. First assume $t \leq L^2/2 + 1$. We saw that $h^1(X, L) = 0$. Since $Z \in W_t$, $h^1(X, \mathcal{I}_Z \otimes L) = 0$. Hence $h^1(X, E_t \otimes L) = 0$, i.e. (a) implies (b). Since $\det(E_t) \cong \mathcal{O}_X$ and $\operatorname{rank}(E_t) = 2$, $E_t^* \cong E_t$. Hence $h^1(X, E \otimes L^*) = h^1(X, E \otimes (L \otimes \omega_X))$. Since $L \otimes \omega_X \in \eta_+$ by Nakai criterion of ampleness ([5], I.5.1) and $(L \otimes \omega_X)^2 = L^2$, the definition of the set W_t gives that (a) implies (c). Now assume $t \geq L^2/2 + 2 = 1 + h^0(X, L)$. Hence $h^1(X, \mathcal{I}_Z \otimes L) > 0$. Since $h^1(X, L) = 0$ ([3], Th. 2.6), tensoring (1) with L we get $h^1(X, L) = 0$. Since $(L \otimes \omega_X)^2 = L^2$, we also get $h^1(X, E \otimes (\omega_X \otimes L) > 0$. Since $E_t^* \cong E_t$, Serre duality gives $h^1(X, E_t \otimes L^*) > 0$. Since $L^2 = (L \otimes \omega_X)^2$, we also see that (a), (b) and (c) are equivalent. □

Proof of Theorem 1. Let E be a rank 2 ACM vector bundle on X such that $\det(E) \cong \mathcal{O}_X$. Since $\chi(\mathcal{O}_X) = 1$ and ω_X and $\det(E)$ are numerically trivial, Riemann-Roch gives $\chi(F) = c_1(E)^2/2 - c_2(E) + 2$. Since $h^1(X, E) = 0$ and $c_1(E)$ is numerically trivial, we get $h^0(X, E) + h^2(X, E) - c_2(E) + 2 \geq 0$. Fix $H \in \eta_+$ and let A be the rank 1 subsheaf of E such that $w := A \cdot H$ is maximal. The maximality of the integer w and the ampleness of H gives that A is saturated in E. Since $\det(E) \cong \mathcal{O}_X$, we get an exact sequence

$$0 \to A \to E \to \mathcal{I}_Z \otimes A^* \to 0 \tag{3}$$

with Z a zero-dimensional subscheme of X and $c_2(E) = \text{length}(Z) - A^2$. Since $h^1(X, E) = 0$, we get $h^1(X, \mathcal{I}_Z \otimes A^*) \leq h^2(X, A)$ and $h^1(X, A) \leq h^0(X, \mathcal{I}_Z \otimes A^*)$. Serre duality gives $h^2(X, A) = h^0(X, A^* \otimes \omega_X)$.

(a) Here we assume $w = 0$. Since H is ample and ω_X has order 2, $h^0(X, A^* \otimes \omega_X) > 0$ if and only if $A \cong \omega_X$. Hence $h^1(X, \mathcal{I}_Z \otimes A^*) = 0$ if $A \neq \omega_X$. For the same reason $h^0(X, A) + h^0(X, A^*) > 0$ if and only if $A \in \{\mathcal{O}_X, \omega_X\}$. First assume $A \notin \{\mathcal{O}_X, \omega_X\}$. We get $h^1(X, \mathcal{I}_Z \otimes A^*) = 0$. Hence $h^1(X, A^*) = 0$ and $\text{length}(Z) \leq h^0(X, A^*) = 0$. Thus E is an extension of A^* by A.

(a1) Here we assume $h^1(X, A^{\otimes 2}) > 0$. If $h^0(X, A^{\otimes 2}) = h^2(X, A^{\otimes 2}) = 0$, then Riemann-Roch gives $A^2 < 0$ and hence $A^2 = -2$. Now assume $h^0(X, A^{\otimes 2}) + h^2(X, A^{\otimes 2}) > 0$ and that X is not nodal. Since X has no curve with negative self-intersection, every effective divisor is nef. Since $h^0(X, A^{\otimes 2}) + h^2(X, A^{\otimes 2}) > 0$ and ω_X is numerically trivial, we get that $A^{\otimes 2}$ is nef. Hence $A^2 \geq 0$. Riemann-Roch gives that either $h^0(X, A) > 0$ or $h^0(X, A^* \otimes \omega_X) > 0$. Hence either $h^0(X, A^{\otimes 2}) > 0$ or $h^0(X, A^{\otimes -2}) > 0$. Since $w = 0$ any of these inequalities implies $A^{\otimes 2} \in \{\mathcal{O}_X, \omega_X\}$. We cannot have $A^{\otimes 2} \cong \omega_X$, because $\text{Tors}(X) \cong \mathbb{Z}/2\mathbb{Z}$ is generated by ω_X. Hence $A^{\otimes 2} \cong \mathcal{O}_X$, contradicting the assumption $h^1(X, A^{\otimes 2}) > 0$. In summary, if $w = 0$, $A \notin \{\mathcal{O}_X, \omega_X\}$ and $E \neq A \oplus A^*$, then $A^2 = -2$.

(a2) Here we assume $h^1(X, A^{\otimes 2}) = 0$. Hence (4) splits. Hence both A and A^* are ACM. Remark 2 gives that both A and A^* are SACM. Hence E is SACM.

(a3) Here we assume $A \in \{\mathcal{O}_X, \omega_X\}$. First assume $Z \neq \emptyset$. Since $\text{length}(Z) \leq h^2(X, A)$, we get $A \cong \mathcal{O}_X$ and that Z is a point. Hence E is one of the vector bundles E_1 described in Example 1. If $Z = \emptyset$, then $E \cong A \oplus A^*$, because $h^1(X, \mathcal{O}_X) = 0$.

(b) Here we assume $w > 0$. Hence $h^0(X, A^*) = 0$. Serre duality gives $h^2(X, A) = 0$. Hence $Z = \emptyset$ and $h^1(X, A) = h^1(X, A^*) = 0$. Thus Riemann-Roch gives $h^0(X, A) = A^2/2 + 1$ and $h^2(X, A^*) = A^2/2 + 1$. Hence $A^2 \geq -2$. Since $h^0(X, A^*) = h^2(X, A) = 0$, (4) gives $h^0(X, E) = h^0(X, A)$ and $h^2(X, E) = h^2(X, A^*)$. Since $Z = \emptyset$, (4) gives $c_2(E) = -A^2$. Since $\det(E) \cong \mathcal{O}_X$, $\chi(E) = -c_2(E) + 2 = A^2 + 2$.

(b1) Here we assume $h^1(X, A^{\otimes 2}) > 0$. As in case (a1) we get $A^2 = -2$ if $h^0(X, A^{\otimes 2}) = h^2(X, A^{\otimes 2}) = 0$. Now assume $A^2 \geq 0$ and that X is not nodal. Riemma-Roch gives $h^0(X, A^{\otimes 2}) + h^2(X, A^{\otimes 2}) > 0$. Hence either $h^0(X, A^{\otimes 2})) > 0$ or $h^0(X, A^{\otimes -2} \otimes \omega_X) > 0$. The latter inequality cannot occur, because $w > 0$. Hence $A^{\otimes 2}$ is effective. Since X is not nodal, $A^{\otimes 2}$ is nef. Hence the assumption $h^1(X, A^{\otimes 2}) > 0$ and the vanishing theorem [3], Theorem 2.6, for nef and big effective divisors gives $A^2 = 0$.

(b2) Here we assume $h^1(X, A^{\otimes 2}) = 0$. Hence (4) splits. Hence both A and A^* are ACM. Remark 2 gives that both A and A^* are SACM. Hence E is SACM.

(c) Here we assume $w < 0$. Hence E is H-stable in the sense of Mumford and Takemoto. Since $c_1(E) \cdot H = 0$, this implies $h^0(X, E) = 0$. Since E is H-stable,

$E^* \otimes \omega_X$ is an H-stable with trivial determinant. Hence $h^0(X, E \otimes \omega_X) = 0$, i.e. $h^2(X, E) = 0$. Since E is ACM, Riemman-Roch gives $-c_2(E) + 2 = \chi(E) = 0$, i.e. $-A^2 + \text{length}(Z) = 2$. Riemann-Roch for A gives that A^2 is an even integer. Since $w < 0$, $h^2(X, A) = 0$. Hence $h^1(X, E) = 0$ implies $h^1(X, \mathcal{I}_Z \otimes A^*$. Hence $h^1(X, A^*) = 0$ and $h^0(X, A^*) \geq \text{length}(Z)$. Thus $Z = \emptyset$ if $h^0(X, A^*) = 0$. Hence $h^0(X, A^*) = 0$ implies $c_2(E) = -A^2 = 2$.

(c1) Here we assume that X is not nodal. Assume $h^0(X, A^*) > 0$. Since X is not nodal, $A^2 \geq 0$. Hence if X is not nodal and $Z \neq \emptyset$, then $\text{length}(Z) = 2$ and $A^2 = 0$. However, $h^1(X, A^*) = 0$ and $A^2 = 0$, gives $h^0(X, A^*) \leq 1 < \text{length}(Z)$. Hence if X is not nodal, then $Z = \emptyset$, $c_2(E) = 2 = A^2$ and E is an extension of A^* by A. □

Remark 3. Fix $A, B \in \text{Pic}(X)$. Let E be the middle term of an extension ϵ of B by A. If $\epsilon = 0$ and $A \cong B$, then $h^0(X, End(E)) = 4$. If $\epsilon = 0$ and $A \neq B$, then $h^0(X, End(E)) = 2$ and any element of $H^0(X, End(E))$ may be put is a diagonal form. Now assume $\epsilon \neq 0$ and $h^0(X, E \otimes A^*) = 1$. The latter condition is satisfied if there is an ample line bundle H such that either $A \cdot H > B \cdot H$ or $A \neq B$ and $A \cdot H = B \cdot H$. Then $h^0(X, End(E)) = 1 + h^0(X, A \otimes B^*)$ and every element of $H^0(X, End(E))$ may be put in a triangular form with the same constant on the two diagonal elements and an element of $H^0(X, A \otimes B^*)$ as the $(1, 2)$-entry.

3. X a $K3$-surface

In this section X is a smooth and projective $K3$-surface. Hence $\omega_X \cong \mathcal{O}_X$, $h^1(X, \mathcal{O}_X) = 0$, $b_2(X) = 22$ and $\text{Pic}(X) \cong \mathbb{Z}^\rho$ for some integer ρ such that $1 \leq \rho \leq 22$. If $\text{char}(\mathbb{K}) = 0$, then $\rho \leq 20$. For any $L \in \text{Pic}(X)$ and any rank 2 vector bundle on X we have $\chi(L) = L^2/2 + 2$ and $\chi(E) = \det(E)^2/2 - c_2(E) + 4$ (Rieman-Roch). Hence L^2 is always an even integer. Now assume $L \in \eta_+$. Hence $h^0(X, L^*) = h^2(X, L) = 0$. Kodaira vanishing gives $h^1(X, L) = h^1(X, L^*) = 0$. In positive characteristic we use [8] to get Kodaira vanishing. However, to apply [8], Cor. 8, we need to assume that X is not quasi-elliptic. We just recall that no surface is quasi-elliptic if $\text{char}(\mathbb{K}) \neq 2, 3$. Hence $h^0(X, L) = L^2/2 + 2$ for every $L \in \eta_+$ if $\text{char}(\mathbb{K}) \neq 2, 3$.

Example 2. Set $\delta := \min\{L^2 : L \in \eta_+\}$. δ is a positive even integer. Fix an integer t such that $2 \leq t \leq \delta/2 + 2$. Fix $L \in \eta_+$. Since $L^2 \geq \delta$, we have $h^0(X, L) = L^2/2 + 1 \geq t$. Since $h^0(X, L) \geq t$ and $h^1(X, L) = 0$, we have $h^1(X, \mathcal{I}_Z \otimes L) = 0$ for a general $Z \subset X$ such that $\sharp(Z) = t$. Now assume that $\mathbb{K}$ is uncountable. Since $\text{Pic}^0(X)$ is countable, there are only countably many ample line bundles on X. Hence there is a non-empty set W_t of the Hilbert scheme $\text{Hilb}^t(X)$ of all zero-dimensional length t subschemes of Z such that $\text{Hilb}^t(X) \backslash W_t$ is a union of countably many proper algebraic subsets of $\text{Hilb}^t(X)$, each $Z \in W_t$ is locally a complete intersection and $h^1(X, \mathcal{I}_Z \otimes L) = 0$ for all $L \in \eta_+$ such that $L^2/2 + 2 \geq t$ and all $Z \in W_t$. Fix any $Z \in W_t$ and consider the general extension (1). Since $h^0(X, \omega_X) = 0$ and $t \geq 2$, the Cayley-Bacharach condition is satisfied ([1], Th. 1.4) and hence E_t is locally free. We have $\det(E_t) \cong \mathcal{O}_X$, $c_2(E_t) = t$ and E_t is slope properly semistable with respect to any polarization on X. Since $h^1(X, \mathcal{O}_X) = 0$, [1], Th. 1.4, gives that the set of all non-trivial extensions is parametrized by a $(t-1)$-dimensional projective space. Since $Z \neq \emptyset$, $h^0(X, E_t) = 1$. Thus E_t uniquely determines Z as the scheme-theoretic locus at which any non-zero section of E_t drops rank. Since

$\mathcal{O}_X$ is spanned, $h^0(X,\mathcal{O}_X) = 1$ and $h^1(X,\mathcal{O}_X) = 0$, we have $h^1(X,\mathcal{I}_Z) = t-1$. Hence (1) gives $h^1(X,E_1) = 0$ and $h^1(X,E_t) > 0$ if $t > 1$. Fix $L \in \eta_+$. We saw that $h^1(X,L) = 0$. Since $Z \in W_t$ and $t \le h^0(X,L)$, $h^1(X,\mathcal{I}_Z \otimes L) = 0$. Hence $h^1(X,E_t \otimes L) = 0$. Since $\det(E_t) \cong \mathcal{O}_X$ and $\operatorname{rank}(E_t) = 2$, $E_t^* \cong E_t$. Hence $h^1(X,E \otimes L^*) = h^1(X,E \otimes L)$. Thus E_t is WACM, but not ACM. E_t is properly semistable in the sense of Mumford-Takemoto with respect to any polarization of X. As in the case of an Enriques surface we see that E is not an extension of two line bundles. Conversely, take a zero-dimensional scheme $Z \subset X$, $Z \neq \emptyset$ and take any extension (1) with locally free middle term, F. set $t := \operatorname{length}(Z)$. Since F is locally free, the Cayley-Bacharach condition must be satisfied and hence $t \ge 2$. Now assume that F is WACM. Fix $L \in \eta_+$. Since $h^2(X,L) = 0$ and $h^1(X,F \otimes L) = 0$, we get $h^1(X,\mathcal{I}_Z \otimes L) = 0$. Hence $t \ge h^0(X,L)$. Taking L with minimal self-intersection, we get $t \le \delta/2 + 2$. Since $h^1(X,\mathcal{I}_Z \otimes L) = 0$ for all $L \in \eta_+$, we see that all WACM non-trivial vector bundles E with $\det(E) \cong \mathcal{O}_X$, $h^0(X,E) > 0$, $h^0(X,E(-D)) = 0$ for every divisor $D > 0$ are given by our construction for some integer $t := c_2(E)$ such that $2 \le t \le \delta/2 + 2$.

Proof of Theorem 2. Let E be a rank 2 ACM vector bundle on X. Fix $H \in \eta_+$ and let A be the rank 1 subsheaf of E such that $w := A \cdot H$ is maximal. The maximality of the integer w and the ampleness of H gives that A is saturated in E. Since $\det(E) \cong \mathcal{O}_X$, we get an exact sequence

$$0 \to A \to E \to \mathcal{I}_Z \otimes A^* \to 0 \tag{4}$$

with Z a zero-dimensional subscheme of X and $c_2(E) = \operatorname{length}(Z) - A^2$. Since $h^1(X,E) = 0$, we get $h^1(X,\mathcal{I}_Z \otimes A^*) \le h^2(X,A)$ and $h^1(X,A) \le h^0(X,\mathcal{I}_Z \otimes A^*)$. Serre duality gives $h^2(X,A) = h^0(X,A^*)$.

(a) Here we assume $w = 0$. Since H is ample, $h^0(X,A^*) > 0$ if and only if $A \cong \mathcal{O}_X$. Hence $h^1(X,\mathcal{I}_Z \otimes A^*) = 0$ if $A \neq \mathcal{O}_X$. For the same reason $h^0(X,A) + h^0(X,A^*) > 0$ if and only if $A \cong \mathcal{O}_X$. First assume $A \neq \mathcal{O}_X$. We get $h^1(X,\mathcal{I}_Z \otimes A^*) = 0$. Hence $h^1(X,A^*) = 0$ and $\operatorname{length}(Z) \le h^0(X,A^*) = 0$. Thus E is an extension of A^* by A if $A \neq \mathcal{O}_X$.

(a1) Here we assume $A \neq \mathcal{O}_X$ and $h^1(X,A^{\otimes 2}) > 0$. If

$$h^0(X,A^{\otimes 2}) = h^2(X,A^{\otimes 2}) = 0,$$

then Riemann-Roch gives $A^2 < 0$ and hence $A^2 \in \{-4,-2\}$. Now assume

$$h^0(X,A^{\otimes 2}) + h^2(X,A^{\otimes 2}) > 0$$

and that X has Property (+). Since X has no curve with negative self-intersection, every effective divisor is nef. Since $h^0(X,A^{\otimes 2}) + h^2(X,A^{\otimes 2}) > 0$ and $\omega_X \cong \mathcal{O}_X$, we get that $A^{\otimes 2}$ is nef. Hence $A^2 \ge 0$. Assume $A^2 > 0$. Riemann-Roch gives that either $h^0(X,A) > 0$ or $h^0(X,A^* \otimes \omega_X) > 0$. Hence either $h^0(X,A^{\otimes 2}) > 0$ or $h^0(X,A^{\otimes -2}) > 0$. Since $w = 0$ any of these inequalities implies $A^{\otimes 2} \cong \mathcal{O}_X$, contradicting the assumption on A and the fact that $\operatorname{Pic}(X)$ has no torsion.

(a2) Here we assume $h^1(X,A^{\otimes 2}) = 0$. Hence (4) splits. Hence both A and A^* are ACM.

(a3) Here we assume $A \cong \mathcal{O}_X$. Since $\operatorname{length}(Z) \le h^0(X,A^*) = 1$, Z is a point. Since $\omega_X \cong \mathcal{O}_X$ and Z is a point, we get the Cayley-Bacharach condition is not satisfied and hence the middle term of any extension (4) with $\mathcal{O}_X$ and Z a point is not locally free, contradiction. Hence $Z = \emptyset$ if $w = 0$.

(b) Here we assume $w > 0$. Hence $h^0(X, A^*) = 0$. Serre duality gives $h^2(X, A) = 0$. Hence $Z = \emptyset$ and $h^1(X, A) = h^1(X, A^*) = 0$. Thus Riemann-Roch gives $h^0(X, A) = A^2/2 + 2$ and $h^2(X, A^*) = A^2/2 + 2$. Since $h^0(X, A^*) = h^2(X, A) = 0$, (4) gives $h^0(X, E) = h^0(X, A)$ and $h^2(X, E) = h^2(X, A^*)$. Since $Z = \emptyset$, (4) gives $c_2(E) = -A^2$. Since $\det(E) \cong \mathcal{O}_X$, $\chi(E) = -c_2(E) + 4 = A^2 + 4$. Since $h^1(X, E) = 0$, $\chi(E) \geq 0$. Hence $A^2 \geq -4$. Riemann-Roch gives that A^2 is an even integer.

(b1) Here we assume $h^1(X, A^{\otimes 2}) > 0$. As in case (a1) we get $-4 \leq A^2 \leq -2$ if $h^0(X, A^{\otimes 2}) = h^2(X, A^{\otimes 2}) = 0$. Now assume $A^2 \geq 0$, that X has Property (+) and that X is not quasi-elliptic. Riemann-Roch gives $h^0(X, A^{\otimes 2}) + h^2(X, A^{\otimes 2}) > 0$. Hence either $h^0(X, A^{\otimes 2})) > 0$ or $h^0(X, A^{\otimes -2} \otimes \omega_X) > 0$. The latter inequality cannot occur, because $w > 0$. Hence$A^{\otimes 2}$ is effective. Since X has Property (+), $A^{\otimes 2}$ is nef. Hence the assumption $h^1(X, A^{\otimes 2}) > 0$ and (assuming X not quasi-elliptic) the vanishing theorem [8], Cor. 8, for nef and big line bundles gives $A^2 = 0$.

(b2) Here we assume $h^1(X, A^{\otimes 2}) = 0$. Hence (4) splits. Hence both A and A^* are ACM.

(c) Here we assume $w < 0$. Hence E is H-stable in the sense of Mumford and Takemoto. Since $c_1(E) \cdot H = 0$, this implies $h^0(X, E) = 0$. Since E is H-stable, E^* is H-stable. Hence $h^0(X, E) = 0$, i.e. $h^2(X, E) = 0$. Since E is ACM, Riemman-Roch gives $-c_2(E) + 4 = \chi(E) = 0$, i.e. $-A^2 + \text{length}(Z) = 4$. Riemann-Roch for A gives that A^2 is an even integer. Since $w < 0$, $h^2(X, A) = 0$. Hence $h^1(X, E) = 0$ implies $h^1(X, \mathcal{I}_Z \otimes A^*)$. Hence $h^1(X, A^*) = 0$ and $h^0(X, A^*) \geq \text{length}(Z)$. Thus $Z = \emptyset$ if $h^0(X, A^*) = 0$

(c1) Here we assume that X has Property (+). Assume $Z \neq \emptyset$. Hence $h^0(X, A^*) > 0$. Since X has Property (+), $A^2 \geq 0$. Hence if X has Property (+) and $Z \neq \emptyset$, then $\text{length}(Z) = 4$ and $A^2 = 0$. However, $h^1(X, A^*) = 0$, $h^2(X, A^*) = h^0(X, A) = 0$ and $A^2 = 0$ give $h^0(X, A^*) = 2 < 4 = \text{length}(Z)$, contradiction. Since $Z = \emptyset$, $c_2(E) = -A^2 = 4$. □

Remark 4. Let X be a $K3$-surface such that $\text{Pic}(X) \cong \mathbb{Z}$. Let δ be the self-intersection of a generator of $\text{Pic}(X)$. Every line bundle on X is ACM. Hence the proof of Theorem 2 shows that a rank 2 vector bundle on X such that $\det(E) \cong \mathcal{O}_X$ is ACM if and only if one of the following conditions is satisfied:

(i) $E \cong A \otimes A^*$ for some $A \in \text{Pic}(X)$;
(ii) there is an integer t such that $2 \leq t \leq \delta/2 + 2$ such that E is one of the vector bundles E_t described in Example 2.

Proposition 2. *Let X be a projective $K3$ surface. The following conditions are equivalent:*

(i) *$Pic(X) \cong \mathbb{Z}$;*
(ii) *every line bundle on X is ACM;*
(iii) *every line bundle on X is WACM;*
(iv) *every ample line bundle on X is ACM;*
(v) *every ample line bundle on X is WACM.*

Proof. The first part of Remark 4 gives that (i) implies (ii). Hence it is sufficient to show that if $\rho \geq 2$, then there is an ample line bundle on X which is not WACM. Since $\rho \geq 2$, the intersection form on $\text{Pic}(X)$ is not definite positive by Hodge Index theorem. Hence there is $A \in \text{Pic}(X)$ such that $A^2 < 0$. Set $B := A^{\otimes 2}$. Since A^2 is an even integer $B^2 \leq -4$. Hence $\chi(B) = B^2 + 2 < 0$. Hence $h^1(X, B) > 0$. Since

every Cartier divisor on a projective variety is the difference of two very ample divisors, there are ample R, L such that $B := R \otimes L^*$. Since $h^1(X, B) > 0$, R is not WACM. □

Proof of Theorem 3. Since X has Property (++), it is not quasi-elliptic and hence we may use Kodaira vanishing on X ([8], Cor. 8). Take E given by an extension (4). We saw in the proof of Theorem 2 that $Z = \emptyset$ and hence $c_2(E) = -A^2$. First assume $A^2 = 0$, i.e. $c_2(E) = 0$. Since $\chi(A) = 2$, either A or A^* must have a section. Since $A^2 = 0$ and X has Property (++), we get $A \cong \mathcal{O}_X$ and hence $E \cong \mathcal{O}_X^{\oplus 2}$. Now assume $A^2 > 0$, i.e. $c_2(E) < 0$. Hence either A is ample or A^* is ample. In both cases we have $h^1(X, A^{\otimes 2}) = 0$ by Kodaira vanishing and Serre duality. Hence $E \oplus A \oplus A^*$, i.e. we are in case (ii). □

References

[1] F. Catanese, Footnotes to a theorem of I. Reider, Algebraic Geometry Proceedings, L'Aquila 1988, 67–74, Lect. Notes in Math. 1417, Springer, Berlin, 1990.

[2] F. R. Cossec, Projective models of Enriques surfaces, Math. Ann. 265 (1983), 283–334.

[3] F. R. Cossec, On the Picard group of Enriques surfaces, Math. Ann. 271 (1985), 577–600.

[4] F. R. Cossec and I. V. Dolgacev, Enriques surfaces I, Birkhäuser, Boston, 1989.

[5] R. Hartshorne, Ample subvarieties of algebraic varieties, Lect. Notes in Math. 156, Springer, Berlin, 1970.

[6] M. Casanellas and R. Hartshorne, ACM bundles on cubic hypersurfaces, arXiv:math/0801.3600.

[7] T. Johsen and A. L. Knutsen, $K3$ projective models in scrolls, Lect. Notes in Math. 1842, Springer, Berlin, 2004.

[8] N. I. Sheperd-Barron, Unstable vector bundles and linear systems on surfaces in characteristic p, Invent. Math. 106 (1991), no. 2, 243–262.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 13–17
ISSN 1930-1235: (2009)

A COMMON FIXED POINT THEOREM FOR A FAMILY OF SELFMAPPINGS SATISFYING A GENERAL CONTRACTIVE CONDITION OF OPERATOR TYPE

Cihangir Alaca

Department of Mathematics,
Faculty of Science and Arts,
Sinop University, 57000 Sinop,
Turkey
cihangiralaca@yahoo.com.tr

Abstract. In this paper, we prove a common fixed point theorem for a family of selfmappings satisfying a general contractive condition of operator type.

1. Introduction

The class of generalized contraction mappings, introduced and studied by Ćirić in [6], is very significant in a fixed point theory. As noted by Gornićki and Rhoades [8], a contractive condition (2.1) on a pair of generalized contractions. Jungck [9] proved a fixed point theorem for commuting maps generalizing the Banach's fixed point and further he [10] introduced more generalizing commutativity, so called compatibility, which is more general than that of weak commutativity defined by Sessa [12]. Lately, Branciari [4] obtained a fixed point results for a single mapping satisfying an analogue of Banach's contraction principle (see [3] and [5]) for an integral type inequality. Rhoades [11] proved two fixed point theorems involving more general contractive conditions. Vijayaraju et al. [13] established a general principle, which maked it possible to proved many fixed point theorems for a pair of maps of integral type. Aliouche [1] gave a common fixed point theorem for selfmappings of a symmetric space under a contractive condition of integral type. Altun and Turkoglu [2] proved a fixed point theorem for mappings satisfying a general contractive of operator type.

The main purpose of this paper is to give a common fixed point theorem for a family of selfmappings satisfying a general contractive condition of operator type.

2. Preliminaries

Let X be a nonempty set and let $\{T_\alpha\}_{\alpha\in J}$ be a family of selfmappings on X and J indexing set. A point $u \in X$ is called a common fixed point for a family

2000 *Mathematics Subject Classification.* 47H10, 54E50, 58J20.
Key words and phrases. Common fixed point, contractive condition of operator type.

$\{T_\alpha\}_{\alpha\in J}$ iff for each T_α. The following theorem was given by Ćirić [7] for a family of generalized contraction.

Theorem 1. *Let (X,d) be a complete metric space and let $\{T_\alpha\}_{\alpha\in J}$ be a family of selfmappings of X. If there exists fixed $\beta\in J$ such that for each $\alpha\in J$:*

$$d(T_\alpha x,T_\beta y)\leq \lambda\max\left\{\begin{array}{c} d(x,y),d(x,T_\alpha x),d(y,T_\beta y),\\ \frac{1}{2}\left[d(x,T_\beta y)+d(y,T_\alpha x)\right]\end{array}\right\} \tag{2.1}$$

for some $\lambda=\lambda(\alpha)\in(0,1)$ and all $x,\ y\in X$, then all T_α have a unique common fixed point, which is a unique fixed point of each T_α, $\alpha\in J$.

The following theorem was given by Branciari [4] was to analyze the existence of fixed points for mappings of f defined on a complete metric space (X,d) satisfing a contractive condition of integral type.

Theorem 2. *Let (X,d) be a complete metric space, $c\in(0,1)$ and $f:X\to X$ be a mapping such that for each $x,\ y\in X$ one has*

$$\int_0^{d(fx,fy)}\varphi(t)dt\leq c\int_0^{d(x,y)}\varphi(t)dt$$

where $\varphi:[0,+\infty)\to[0,+\infty)$ is a Lebesgue-integrable mapping which is summable (i.e. with finite integral) on each compact subset of $[0,+\infty)$, non-negative and such that for each $\varepsilon>0$, $\int_0^{\varepsilon}\varphi(t)dt>0$; then f has a unique fixed point $a\in X$ such that for each $x\in X$, $\lim_{n\to\infty}f^nx=a$.

The following concept of $O\left(f\ ;.\right)$ and its examples was given by Altun and Turkoglu [2].

Let $F([0,\infty))$ be class of all function $f:[0,\infty)\to[0,\infty]$ and let Θ be class of all operators

$$O\left(\bullet;.\right):F([0,\infty))\to F([0,\infty)),\ \ f\to O\left(f\ ;.\right)$$

satisfying the following conditions:

(i) $O\left(f\ ;t\right)>0$ for $t>0$ and $O\left(f\ ;0\right)=0$,

(ii) $O\left(f\ ;t\right)\leq O\left(f\ ;s\right)$ for $t\leq s$,

(iii) $\lim_{n\to\infty}O\left(f\ ;t_n\right)=O\left(f\ ;\ \lim_{n\to\infty}t_n\right)$,

(iv) $O\left(f\ ;\max\{t,s\}\right)=\max\{O\left(f\ ;t\right),O\left(f\ ;s\right)\}$ for some $f\in F([0,\infty))$.

Example 1. *If $f:[0,\infty)\to[0,\infty)$ is a Lebesque integrable mapping which is finite integral on each compact subset of $[0,\infty)$, non-negative and such that for each $t>0$, $\int_0^t f(s)ds>0$, then the operator defined by*

$$O\left(f\ ;t\right)=\int_0^t f(s)ds$$

satisfies the conditions (i)-(iv).

Example 2. *If $f:[0,\infty)\to[0,\infty)$ non-decreasing, continuous function such that $f(0)=0$ and $f(t)>0$ for $t>0$, then the operator defined by*

$$O\left(f\ ;t\right)=\frac{f(t)}{1+f(t)}$$

satisfies the conditions (i)-(iv).

Example 3. *If $f:[0,\infty)\to[0,\infty)$ non-decreasing, continuous function such that $f(0)=0$ and $f(t)>0$ for $t>0$, then the operator defined by*

$$O\left(f\ ;t\right)=\frac{f(t)}{1+\ln\left(1+f(t)\right)}$$

satisfies the conditions (i)-(iv).

3. A common fixed point theorem and it's results

Now, we prove a common fixed point theorem for a family of selfmappings satisfying a general contractive condition of operator type in complete metric spaces.

Theorem 3. *Let (X,d) be a complete metric space and $\{T_\alpha\}_{\alpha\in J}$ be a family of selfmappings of X. If there exists a fixed $\beta\in J$ such that for each $\alpha\in J$:*

$$O\left(f;d\left(T_\alpha x,T_\beta y\right)\right)\leq\lambda O\left(f;m(x,y)\right) \tag{3.1}$$

where $O\left(\bullet;.\right)\in\Theta$ and

$$m(x,y)=\max\left\{d(x,y),d(x,T_\alpha x),d(y,T_\beta y),\frac{1}{2}\left[d(x,T_\beta y)+d(y,T_\alpha x)\right]\right\} \tag{3.2}$$

for some $\lambda=\lambda(\alpha)\in(0,1)$ and all $x,\ y\in X$, then all T_α have a unique common fixed point, which is a unique fixed point of each T_α, $\alpha\in J$.

Proof. Let $\alpha\in J$ and $x\in X$ be arbitrary. Consider a sequence, defined inductively by

$$x_0=x,\ x_{2n+1}=T_\alpha x_{2n},\ x_{2n+2}=T_\beta x_{2n+1},\quad(n\geq0)\,.$$

For each integer $n\geq0$, from (3.1),

$$\begin{aligned} O\left(f;d\left(x_{2n+1},x_{2n+2}\right)\right) &= O\left(f;d\left(T_\alpha x_{2n},T_\beta x_{2n+1}\right)\right) \\ &\leq \lambda O\left(f;m(x_{2n},x_{2n+1})\right). \end{aligned} \tag{3.3}$$

Using (3.2), we have

$$m(x_{2n},x_{2n+1})=\max\left\{d\left(x_{2n},x_{2n+1}\right),d\left(x_{2n+1},x_{2n+2}\right)\right\}.$$

Substituting into (3.3) and (iv), one obtains

$$\begin{aligned} & O\left(f;d\left(x_{2n+1},x_{2n+2}\right)\right) \\ \leq\ & \lambda O\left(f;\max\left\{d\left(x_{2n},x_{2n+1}\right),d(x_{2n+1},x_{2n+2})\right\}\right) \\ =\ & \lambda\max\left\{O\left(f;d\left(x_{2n},x_{2n+1}\right)\right),O\left(f;d\left(x_{2n+1},x_{2n+2}\right)\right)\right\}. \end{aligned} \tag{3.4}$$

If $O\left(f;d\left(x_{2n+1},x_{2n+2}\right)\right)\geq O\left(f;d\left(x_{2n},x_{2n+1}\right)\right)$, then from (3.4) we have

$$O\left(f;d\left(x_{2n+1},x_{2n+2}\right)\right)\leq\lambda O\left(f;d\left(x_{2n+1},x_{2n+2}\right)\right)$$

which is a contradiction ($\lambda<1$). Thus $O\left(f;d\left(x_{2n+1},x_{2n+2}\right)\right)<O\left(f;d\left(x_{2n},x_{2n+1}\right)\right)$ and so from (3.4) one obtains

$$O\left(f;d\left(x_{2n+1},x_{2n+2}\right)\right)\leq\lambda O\left(f;d\left(x_{2n},x_{2n+1}\right)\right).$$

Similarly, we get that

$$O\left(f;d\left(x_{2n},x_{2n+1}\right)\right)\leq\lambda O\left(f;d\left(x_{2n-1},x_{2n}\right)\right).$$

Thus, for any $n \geq 1$ we have

$$\begin{aligned} O\left(f; d\left(x_n, x_{n+1}\right)\right) &\leq \lambda O\left(f; d\left(x_{n-1}, x_n\right)\right) \\ &\leq \lambda^2 O\left(f; d\left(x_{n-2}, x_{n-1}\right)\right) \\ &\vdots \\ &\leq \lambda^n O\left(f; d\left(x_0, x_1\right)\right). \end{aligned} \tag{3.5}$$

Taking the limit of (3.5), as $n \to \infty$, we have

$$\lim_{n\to\infty} O\left(f; d\left(x_n, x_{n+1}\right)\right) = 0,$$

which, from (i), implies that

$$\lim_{n\to\infty} d\left(x_n, x_{n+1}\right) = 0.$$

Therefore, $\{x_n\}$ is Cauchy sequence. (Similarly, see [2]).

Since X is complete, there is a $p \in X$ such that

$$\lim_{n\to\infty} x_n = p.$$

From (3.1) we have,

$$\begin{aligned} O\left(f; d\left(x_{2n+1}, T_\beta p\right)\right) &= O\left(f; d\left(T_\alpha x_{2n}, T_\beta p\right)\right) \\ &\leq \lambda \max \left\{ \begin{array}{c} d(x_{2n}, p), d(x_{2n}, T_\alpha x_{2n}), d(p, T_\beta p), \\ \frac{1}{2}\left[d(x_{2n}, T_\beta p) + d(p, T_\alpha x_{2n})\right] \end{array} \right\}. \end{aligned}$$

Taking the limit as $n \to \infty$ we get

$$O\left(f; d\left(p, T_\beta p\right)\right) \leq \lambda O\left(f; d\left(p, T_\beta p\right)\right),$$

which implies that

$$O\left(f; d\left(p, T_\beta p\right)\right) = 0,$$

which from (i), implies that $d\left(p, T_\beta p\right) = 0$; hence $T_\beta p = p$.

Now we show that p is a fixed point of all $\{T_\alpha\}_{\alpha\in J}$. Let $\alpha \in J$ be arbitrary. Then from (3.1) with $x = y = p = T_\beta p$ we have

$$\begin{aligned} O\left(f; d\left(T_\alpha p, p\right)\right) &= O\left(f; d\left(T_\alpha p, T_\beta p\right)\right) \leq \lambda(\alpha) O\left(f; m(p, p)\right) \\ &\leq \lambda(\alpha) \max \left\{ \begin{array}{c} O\left(f; d(p, p)\right), O\left(f; d(p, T_\alpha p)\right), O\left(f; d(p, T_\beta p)\right), \\ \frac{1}{2}\left[O\left(f; d(p, T_\beta p)\right) + O\left(f; d(p, T_\alpha p)\right)\right] \end{array} \right\} \\ &= \lambda(\alpha) \max \left\{ O\left(f; d(p, T_\alpha p)\right), \frac{1}{2} O\left(f; d(p, T_\alpha p)\right) \right\}. \end{aligned}$$

Therefore, we get

$$O\left(f; d\left(T_\alpha p, p\right)\right) \leq \lambda(\alpha) O\left(f; d(p, T_\alpha p)\right)$$

which implies that

$$O\left(f; d\left(T_\alpha p, p\right)\right) = 0,$$

which, from (i), implies that $d\left(T_\alpha p, p\right) = 0$ or $T_\alpha p = p$. Thus, all T_α have a common fixed point.

Now we prove the uniqueness of the fixed point p. Suppose that q is another a fixed point of T_β. Then it follows, as above, that q is a common fixed point of all $\{T_\alpha\}_{\alpha\in J}$. Thus, from (3.1) we have

$$\begin{aligned} O(f;d(p,q)) &= O(f;d(T_\alpha p,T_\beta q)) \\ &\leq \lambda O(f;m(p,q)) \\ &= \lambda O(f;d(p,q)), \end{aligned}$$

which implies that

$$O(f;d(p,q))=0,$$

which, from (i), implies that $d(p,q)=0$. Hence $p=q$. Thus, p is a unique common fixed point of all $\{T_\alpha\}_{\alpha\in J}$. □

Remark 1. *It is clear that Theorem 3 is a generalization of Theorem 1 in [2].*

Remark 2. *We can have new result, if we combine Theorem 3 and some examples for $O(f;.)$.*

Remark 3. *Theorem 3 is a generalization of Theorem 1, in fact letting $f=I$ (identity map) and $O(f;t)=t$ in (3.1) (it is obvious that $O(f\ ;.)\in\Theta$) one has*

$$d(T_\alpha x,T_\beta y)=O(f;d(T_\alpha x,T_\beta y))\leq\lambda O(f;m(x,y))=\lambda m(x,y),$$

thus Ćirić's [6,7] generalized contraction also satisfies.

References

[1] A. Aliouche, A common fixed point theorem for weakly compatible mappings in symmetric spaces satisfying a contractive condition of integral type, J. Math. Anal. Appl., 322 (2) (2006) 796 − 802.

[2] I. Altun and D. Turkoglu, A fixed point theorem for mappings satisfying a general contractive condition of operator type, J. Comput. Anal. Appl., 9 (1) (2007) 9 − 14.

[3] S. Banach, Sur les opérations dans les ensembles abstraits et leur application aux équations intégrales, Fund. Math., 3 (1922) 133 − 181.

[4] A. Branciari, A fixed point theorem for mappings satisfying a general contractive condition of integral type, Internat. J. Math.&Math. Sci. 29 (9) (2002) 531 − 536.

[5] R. Caccioppoli, Un teorema generale sull'esistenza di elementi uniti in una trasformazione funzionale, Rend. Accad. dei Lincei, 11 (1930) 794 − 799.

[6] Lj. B. Ćirić, Generalized contractions and fixed point theorems, Publ. Inst. Math., 12 (26) (1971) 19 − 26.

[7] Lj. B. Ćirić, On a family of contractive maps and fixed points, Publ. Inst. Math., 17 (31) (1974) 45 − 51.

[8] J. Gornicki, B. E. Rhoades, A general fixed point theorem for involutions, Indian J. Pure Appl. Math. 27 (31) (1996) 45 − 51.

[9] G. Jungck, Commuting maps and fixed points,Amer. Math. Monthly, 83 (1976) 261 − 263.

[10] G. Jungck, Compatible mappings and common fixed points, Internat. J. Math. Math. Sci., 9 (1986) 771 − 779.

[11] B. E. Rhoades, Two fixed point theorems for mappings satisfying a general contractive condition of integral type, Internat. J. Math. Math. Sci., 63 (2003) 4007 − 4013.

[12] S. Sessa , On Weak Commutativity Condition of Mappings in Fixed Point Considerations, Publ. Inst. Math., 32 (46) (1982) 149 − 153.

[13] P. Vijayaraju, B. E. Rhoades and R. Mohanraj, A fixed point theorem for a pair of maps satisfying a general contractive condition of integral type, Internat. J. Math. Math. Sci., 15 (2005) 2359 − 2364.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 25–33
ISSN 1930-1235: (2009)

ALGEBRAIC GROUPS AND SMALL WORLD GRAPHS OF HIGH GIRTH

V. A. Ustimenko

University of Maria Curie-Sklodowska,
vasyl@golem.umcs.lublin.pl

Abstract. We apply term algebraic graphs for an infinite family of graphs for which the vertex set and the neighbourhood of each vertex are quasiprojective varieties over the commutative ring K. For each integral domain K with unity of characteristic $\neq 2$ and integral $m \geq 2$ we construct an edge transitive graph $\Gamma_m(K)$ of girth $\geq m$ and diameter bounded by the constant independent on K. In particular, for each m we have a family of algebraic small world graphs $\Gamma(m, F_{p^s})$, $s = 1, 2, \dots$ over F_p, where p is prime, of girth $\geq m$.

1. Introduction

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [4]. All graphs (finite or infinite) we consider are simple, i.e. indirected without loops and multiple edges. Let $V(\Gamma)$ denotes the set of vertices of the graph Γ. A pass in Γ is called *simple* if all its vertices are distinct. When it is convenient, we shall identify Γ with the corresponding antireflexive symmetric binary relation on $V(\Gamma)$. The *length* of a pass is the number of its edges. The diameter of the graph is the maximal length of the shortest pass between two vertices. The *girth* of a graph Γ is the length of the shortest cycle in Γ.

We shall use term *the family of algebraic graphs* for the family of graphs $\Gamma(K)$, where K belongs to some infinite class F of commutative rings, such that the neighbourhood of each vertex of $\Gamma(K)$ and the vertex set itself are quasiprojective varieties over K of dimension ≥ 1 (see [1]).

Such a family can be treated as special Turing machine with the internal and external alphabet K.

Double cosets graphs corresponding to PwP', where P and P' are maximal parabolic subgroups of simple group $G(K)$ of Lie type defined over the field K are examples of algebraic edge-transitive graphs of finite diameter (see [1] or [6]). But the girth of them is bounded by 16 (case of generalised octagon defined over the field).

Theorem 1. *For each integer d, $d > 2$ there is an infinite family of edge-transitive algebraic graphs $\Gamma_d(K)$, where K is an integrity ring with unity of characteristic $\neq$*

Key words and phrases. infinite groups acting on graphs, algebraic graphs, graphs of large girth, small world graphs.

2, *such that* $g(\Gamma(K)) \geq d$ *and diameter* $\mathrm{diam}(\Gamma_d(K))$ *is bounded by some constant, independent from* K.

The statement proven by explicit construction of bipartite graphs $\Gamma_n(K)$ with point set and line set of kind K^n such that neighbourhood of each vertex is isomorphic to K.

The diameter of a k-regular graph (or graph with the average degree k) of order v is at least $\log_{k-1}(v)$ and it is known that the random k-regular graph has diameter close to this lower bound. In the case of family of small world graphs the diameter is $O(\log_{k-1}(v))$. The girth of the graph is the smallest length of it is cycle. Most known explicit constructions of infinite families of regular small world graphs are of girth 4 (see, for instance, [5]).

Corollary 2. *For each pair* $(k \geq 3, g \geq 3)$ *there is a regular small world graph of degree* $\geq k$ *and girth* $\geq g$ *with bounded diameter.*

The explicit construction construction of graph $\Gamma_d(K)$ are connected with studies of infinite families of graphs of large girth in the sense of N. Biggs [2] i.e. graphs G_i of degree l_i and unbounded girth g_i such that

$$g_i \geq \gamma \log_{l_i-1}(v_i) \tag{1.1}$$

As it follows from Even Circuit Theorem by Erdø s' $\gamma \leq 2$, but no family has been found for which $\gamma = 2$. Bigger γ's correspond to the larger girth.

The first explicit examples of families with large girth were given by Margulis [13], [14], [15] with for some infinite families with arbitrary large valency. The constructions were Cayley graphs $X^{p,q}$ of group $SL_2(Z_q)$ with respect to special sets of $q+1$ generators, p and q are primes congruent to 1 mod4. Then independently Margulis and Lubotsky, Phillips, and Sarnak [12] proved that for each p the constant γ for graphs $X^{p,q}$ with fixed p is $\geq 4/3$. In [3] Biggs and Boshier showed that this γ is asymptotically $4/3$.

The family of $X^{p,q}$ is not a family of algebraic graphs because the neighbourhood of each vertex is not an algebraic variety over F_q. For each p, graphs $X^{p,q}$, where q is running via appropriate primes, form a family of small world graph of unbounded diameter.

The fist family of connected algebraic graphs with over F_q of large girth and arbitrarily large degree had been constructed in [9]. These graphs $CD(k,q)$, k is an integer ≥ 2 and q is od prime power had been constructed as connected component of graphs $D(k,q)$ defined earlier (see [7], [8]). For each q graphs $CD(k,q)$, $k \geq 2$ form a family of large girth with $\gamma = 4/3\log_{q-1}q$.

Some new examples of algebraic graphs of large girth and arbitrary large degree the reader can find in [22].

Graphs $D(n,q)$ had been defined by diophantine equations, they have natural generalisations $D(n,K)$ defined over general commutative ring (see section 2 of the paper). In [22] the following statement had been proven.

Proposition 3. *For each integral domain* K *the girth of the graph* $D(n,k)$ *is* $\geq n+5$.

We prove that for each commutative ring with unity of characteristic $\neq 2$ the connected components of $D(n,K)$ are isomorphic algebraic graphs over K. So the girth of the connected component is $g(D(n,K))$ We establish the upper bound for

the diameter of the connected components of $D(n, K)$ independent on the ring K. It means that for each d we can chose the graph $\Gamma_d(K)$ among connected components of graphs $D(n, K)$, $n = 2, 3, \ldots$.

The description of the connected components $D(n, F_q)$, q is odd number had been obtained in [10], but the question on the evaluation of diameter was open.

The technique of studies the connected components of $CD(n, K)$ is group theoretical. In section 2 we define the automorphism group $U(n, K)$ acting edge transitive on the vertex set of graphs $D(n, K)$. We introduce imprimitivity blocks $CD(k, K) = C_t(K)$ of transformation group $(U(n, K), D(n, K))$ such that induced subgraph is an bipartite algebraic graph with partition sets isomorphic to K^t, where $t = [4/3n] + 1$ for $n = 0, 2, 3 \bmod 4$ and $t = [3/4n] + 2$ for $n = 1 \bmod 4$. We show that the graph $C_t(K)$ for the ring K with unity of odd characteristic is the connected component of $D(n, K)$. Let $D(K)$, $CD(K)$ and $U(K)$ are natural projective limits of graphs $D(n, K)$, $CD(n, K)$ and groups $U(n, K)$ when $n \to \infty$. As it was established in [22] for the case of integral domain K the girth of $D(n, K) \geq n+5$. It means that if K is an integral domain with unity of odd characteristic then CD(K) is a tree and $U(K)$ is isomorphic to the free product of two copies of additive group K^+ for the ring K.

In section 3 we establish the upper bound for the diameter of the graph $C_t(K)$, where K is the ring with unity of odd characteristic. As a corollary we get that the following statement

Proposition 4. *The family $C_t(K)$, where t is fixed and K belongs to the class of finite rings with unity of odd characteristic is the family of algebraic small world graphs of bounded diameter.*

The combination of small diameter and large girth makes graphs $C_t(K)$ useful in cryptographical applications (see [19], [20], [21], [22]).

2. Transformation groups of incidence structures defined over commutative rings

The *incidence structure* (P, L, I) (or *bipartite graph*) is a triple where P and L are two disjoint sets (set of *points* and set of lines, respectively) and I is symmetric binary relation on$P \cup L$ (*incidence relation*). As is usually done, we impose the following restrictions on I: two points (lines) are incident if and only if they coincide.

We need the following well known results on groups acting on graphs.

Let G be a group with proper distinct subgroups G_1 and G_2. Let us consider the incidence structure with the point set $P = (G : G_1)$ and the line set $(G : G_2)$ and incidence relation $I : \alpha I \beta$ if and only if the set theoretical intersection of cosets α and β is nonempty set. We shall not distinguish the incidence relation and corresponding graph $\Gamma(G)_{G_1,G_2}$. Let $l(g)$ be the minimal length of representation of g in the form of products of elements from G_1 and G_2 The following statement had been formulated first by G. Glauberman.

Lemma 5. *Graph I is connected if and only if $< G_1, G_2 >= G$. The diameter of I is* $\max l(g)$, $g \in G$.

Let $A =< a_1, \ldots, a_n | R_1(a_1, \ldots, a_n), \ldots, R_d(a_1, \ldots, a_n) >$ and

$B =< b_1, \ldots b_m | S_1(b_1, \ldots b_m), \ldots, S_t(b_1, \ldots, b_m) >$ are subgroups with generators a_i, $i = 1, \ldots, n$ and b_j, $j = 1, \ldots, m$ and generic relations R_i, $i = 1, \ldots, d$ and

S_j, $j = 1, \ldots, t$, respectively. Free product $F = A * B$ of A and B be the subgroup $< a_1, \ldots, a_n, b_1, \ldots, b_m | R_1, \ldots R_d, S_1, \ldots, S_t >$ (see [12]).

The definition of an operation of free product F_H of groups A and B amalgamated at common subgroup H can be found in [20]. If $H =< e >$, then $F_H = A * B$.

Theorem 6. *(see, for instance [12]) Let G acts edge transitively but not vertex transitively on a tree T. Then G is the free product of the stabilizers G_a and G_b of adjacent vertices a and b amalgamated at their intersection.*

Corollary 7. *Let G acts edge regularly on the tree T, i. e. $|G_a \cap G_b| = 1$. Then G is the free product $G_a * G_b$ of groups G_a and G_b.*

We define the family of graphs $D(k, K)$, where $k > 2$ is positive integer and K is a commutative ring, such graphs have been considered in [8] for the case $K = F_q$ (some examples are in [7]).

let P and L be two copies of Cartesian power K^N, where K is the commutative ring and N is the set of positive integer numbers. Elements of P will be called *points* and those of L *lines*.

To distinguish points from lines we use parentheses and brackets: If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to adopt the notation for co-ordinates of points and lines introduced in [15] for the case of general commutative ring K:

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots),$$

$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots].$$

The elements of P and L can be thought as infinite ordered tuples of elements from K, such that only finite number of components are different from zero.

We now define an incidence structure (P, L, I) as follows. We say the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their co-ordinates hold:

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0} p_{i-1,i} \\ l'_{i,i} - p'_{i,i} &= l_{i,i-1} p_{0,1} \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i} p_{0,1} \\ l_{i+1,i} - p_{i+1,i} &= l_{1,0} p'_{i,i} \end{aligned} \tag{2.1}$$

(This four relations are defined for $i \geq 1$, $p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$). This incidence structure (P, L, I) we denote as $D(K)$. We identify it with the bipartite *incidence graph* of (P, L, I), which has the vertex set $P \cup L$ and edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

For each positive integer $k \geq 2$ we obtain an incidence structure (P_k, L_k, I_k) as follows. First, P_k and L_k are obtained from P and L, respectively, by simply projecting each vector onto its k initial coordinates with respect to the above order. The incidence I_k is then defined by imposing the first $k-1$ incidence equations and ignoring all others. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k, K)$.

To facilitate notation in future results, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = -1$, and to assume that (6) are defined for $i \geq 0$.

Notice that for $i = 0$, the four conditions (2.1) are satisfied by every point and line, and, for $i = 1$, the first two equations coincide and give $l_{1,1} - p_{1,1} = l_{1,0}p_{0,1}$.

The incidence relation motivated by the linear interpretation of Lie geometries in terms their Lie algebras [16] (see [18]). Let us define the "root subgroups" U_α, where the "root" α belongs to the root system

$$\mathrm{Root} = \{(1,0),(0,1),(1,1),(1,2),(2,1),(2,2),(2,2)'\dots,(i,i),(i,i)',(i,i+1),(i+1,i)\dots\}.$$

The "root system above" contains all real and imaginary roots of the Kac-Moody Lie Algebra $\tilde{A}_1$ with the symmetric Cartan matrix. We just doubling imaginary roots (i,i) by introducing $(i,i)'$.

Group U_α generated by the following "root transformations" $t_\alpha(x)$, $x \in K$ of the $\mathrm{P} \cup \mathrm{L}$ given by rules $p_\beta = p_\beta + r_\beta(x)$, $l_\beta = l_\beta + s_\beta(x)$, where $\beta \in \mathrm{Root}$ and the functions $r_\beta(x)$, $s_\beta(x)$ are consist of summands defined by the following tables ($i \geq 0$, $m \geq 1$).

	$s_{0,1}(x)$	$s_{1,0}(x)$	$s_{m,m+1}(x)$	$s_{m+1,m}(x)$	$s_{m,m}(x)$	$s'_{m,m}(x)$
$l_{i,i}$		$-l_{i,i-1}x$	$+l_{r,r-1}x$, $r-m\geq 1$		$-l_{r,r}x$, $r-m\geq 0$	
$l_{i,i+1}$		$(l_{i,i}+l'_{i,i})x$ $+l_{i,i-1}x^2$	$+l'_{r,r}x$, $r=i-m\geq 0$		$-l_{r,r+1}x$, $r=i-m\geq 0$	
$l_{i+1,i}$	$+l_{i,i}x$			$-l_{r,r}x$, $r=i-m\geq 0$		$+l_{r+1,r}x$, $r=i-m\geq 0$
$l'_{i,i}$	$l_{i-1,i}x$	$l_{i,i-1}x$		$-l_{r-1,r-1}x$, $r=i-m\geq 1$		$+l'_{r,r}$, $r=i-m\geq 0$

TABLE 1

	$r_{0,1}(x)$	$r_{1,0}(x)$	$r_{m,m+1}(x)$	$r_{m+1,m}(x)$	$r_{m,m}(x)$	$r'_{m,m}(x)$
$p_{i,i}$	$+p_{i-1,i}x$	$p_{i,i-1}x$	$+p_{r,r-1}x$ $r=i-m\geq 1$		$-p_{r,r}x$ $r=i-m\geq 0$	
$p_{i,i+1}$		$+p'_{i,i}x$	$+p'_{r,r}x$ $r=i-m\geq 0$		$-p_{r,r+1}x$ $r=i-m\geq 0$	
$p_{i+1,i}$	$(p_{i,i}+p'_{i,i})x$ $+p_{i-1,i}x^2$			$-p_{r,r}x$, $r=i-m\geq 0$		$+p_{r+1,r}x$, $r=i-m\geq 0$
$p'_{i,i}$	$p_{i-1,i}x$			$-p_{r-1,r}x$, $r=i-m\geq 1$		$+p'_{r,r}$, $r=i-m\geq 0$

TABLE 2

Proposition 8. (i)*For each pair* (α,x), $\alpha \in \mathrm{Root}$, $x \in K$ *the transformation* $t_\alpha(x)$ *are automorphisms of* $D(K)$. *The projections of these maps onto the graph* $D(n,K)$, $n \geq 2$ *are elements of* $\mathrm{Aut}(D(n,K))$.

(ii) *Group* $\mathrm{U}(K)$ *acts edge regularly on the vertices of* $\mathrm{D}(K)$.

(iii) *Group* $\mathrm{U}(n,K)$ *generated by projections of* $t_\alpha(x)$ *onto the set of vertices* V *of* $\mathrm{D}(n,K)$ *acts edge regularly on* V.

Proof. Statement (i) follows directly from the definitions of incidence and closed formulas of root transformations $t_\alpha(x)$. Let $<$ be the natural lexicographical linear order on roots of kind (i,j), where $|i-j| \leq 1$. Let us assume additionally that $(i,i) < (i,i)' < (i,i+1)$. Then by application of transformations $t_\alpha(x_\alpha)$, $\alpha \neq (0,1)$ to a point (p) consecutively with respect to the above order, where parameter x_α is chosen to make α component of the image equals zero, we are moving point (p) to zero point (0). A neighbour $[a,0,\dots,0]$ of the zero point can be shifted to the line $[0]$ by the transformation $t_{(1,0)}(-a)$. Thus each pair of incident elements can be shifted to $((0),[0])$ and group U acts edge regularly on vertices of $D(K)$. This

action is regular ((*ii*)) because the stabilizer of the edge $(0), [0]$ is trivial. Same arguments about the action of $U(n, K)$ justify (*iii*).

□

Remark For $K = F_q$ this statement had been formulated in [8].

Let $k \geq 6$, $t = [(k+2)/4]$, and let $u = (u_\alpha, u_{11}, \cdots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \cdots)$ be a vertex of $\mathrm{D}(k, K)$ ($\alpha \in \{(1,0),(0,1)\}$, it does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, let

$a_r = a_r(u) = \sum_{i=0,r} (u_{ii} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1})$,

and $a = a(u) = (a_2, a_3, \cdots, a_t)$.

Proposition 9. *(i) The classes of equivalence relation $\tau = \{(u,v) | a(u) = a(v)\}$ form the imprimitivity system of permutation groups $\mathrm{U}(K)$ and $\mathrm{U}(n, K)$*

(ii) For any $t-1$ ring elements $x_i \in K$), $2 \leq t \geq [(k+2)/4]$, there exists a vertex v of $\mathrm{D}(k, K)$ for which

$a(v) = (x_2, \ldots, x_t) = (x)$.

(3i) The equivalence class C for the equivalence relation τ on the set $K^n \cup K^n$ is isomorphic to the affine variety $K^t \cup K^t$, $t = [4/3n] + 1$ for $n = 0, 2, 3 \bmod 4$, $t = [4/3n] + 2$ for $n = 1 \bmod 4$.

Proof. Let C be the equivalence class on τ on the vertex set $\mathrm{D}(K)$ ($\mathrm{D}(n, K)$ then the induced subgraph, with the vertex set C is the union of several connected components of $\mathrm{D}(K)$ ($\mathrm{D}(n, K)$).

Without loss of generality we may assume that for the vertex v of $C(n, K)$ satisfying $a_2(v) = 0, \ldots a_t(v) = 0$. We can find the values of components $v'_{i,i)}$ from this system of equations and eliminate them. Thus we can identify P and L with elements of K^t, where $t = [3/4n] + 1$ for $n = 0, 2, 3 \bmod 4$, and $t = [3/4n] + 2$ for $n = 1 \bmod 4$.

□

We shall use notation $C(t, K)$ ($C(K)$) for the induced subgraph of $D(n, K)$ with the vertex set C.

Remark.

If $K = F_q$, q is odd, then the graph $C(t, k)$ coincides with the connected component $CD(n, q)$ of the graph $D(n, q)$ (see [10]), graph $C(F_q)$ is a q-regular tree. In other cases the question on the connectedness of $C(t, K)$ is open. It is clear that $g(C(t, F_q))$ is $\geq 2[2t/3] + 4$.

Let $U_\alpha =< t_\alpha(x) | x \in K >$ be a subgroup of $U(K)$. It is isomorphic to the additive group K^+ of the ring K. Let U^C be subgroup generated by $t_\alpha(x)$, $x \in K$, $\alpha \in \{(0,1,(1,0),\ldots,(i,i),(i,i+1),\ldots\}$. Let ${U_n}^C$ be the subgroup generated by transformations $t_\alpha(x)$ from U^C onto the graph $D(n, K)$ (or $C(n, K)$).

Proposition 10. (i) *The connected component $CD(n, K)$ of the graph $D(n, K)$ (or its induced subgraph $C(t, K)$) is isomorphic to $\Gamma({U_n}^C)_{U_{(0,1)}, U_{(1,0)}}$.*

(ii) Projective limit of graphs $D(n, K)$ (graphs $C(t, K)$, $CD(n, K)$) with respect to standard morphisms of $D(n+1, K)$ onto $D(n, K)$ (their restrictions on induced subgraphs) equals to $D(K)$ ($C(K)$, $CD(K) = {U^C}_{U_{(0,1)}, U_{(1,0)}}$, respectively).

If K is an integrity domain, then $D(K)$ and $CD(K)$ are forests. Let C be the connected component, i.e tree.

Group U^C acts regularly on $CD(K)$. So we can apply theorem on group acting regular on the tree and get the following statement.

Proposition 11. *If K is integrity domain then group $U^C(K)$ is isomorphic to the free product of two copies of K^+.*

3. Main statement

Theorem 12. *The diameter of the graph $C_m(K)$, $m \geq 2$, K is a commutative ring with unity of odd characteristic is bounded by function $f(m)$, defined by the following equations:*

$$f(m) = \begin{cases} (32/3)(4^{(m+1)/3} - 1) - m + 7, & \text{for } m = 2 \text{ (mod3)} \\ (32/3)(4^{(m-1)/3} - 1) + 4^{(m+5)/3} - m + 7 & \text{for } m = 1 \text{ (mod3)} \\ (32/3)(4^{m/3} - 1) + 32 \times 4^{(m-3)/3} - m + 7, & \text{for } m = 0 \text{ (mod3)} \end{cases}$$

Proof. Let $C = C_t(K)$ be the block of equivalence relation τ, containing zero point and zero line. Let us consider the stabiliser of this block. It is clear that group G generated by elements $t_{i,i+1}(x)$, $t_{i+1,i}(x)$, $i \geq 0$, $t_{1,1}(x)$ and $t_i(x) = t_{i,i}(x)t'_{i,i}(x)$, $i \geq 2$, $x \in K$ stabilises C and acts regularly on this set.

Let $l(g)$ be the minimal length of irreducible representation of $g \in G$ in the form

$$T_1(x_1)T_2(x_2)\dots T_d(x_d), x_i \in K, \tag{3.1}$$

where consecutive elements $T_i(x_i)$ and $T_{i+1}(x_{i+1})$ belong to different subgroups U_1 and U_2.

As it follows from the group theoretical interpretation of lemma 3 the diameter of group G is equal to the maximal length $l(g)$.

Let $G_{1,1}$ be the totality of all commutator elements $[t_{0,1}(x), t_{1,0}(y)] = t(x, y)$. Then applications of $T_{1,1}(y) = t(1, y)$ to zero point (0) (or line) do not change its first component. For the second component $u_{1,1}$ of (u) $= (0)^{T_{1,1}(y)}$ we have $u_{1,1} = y$. In fact, $(O)^{T_{1,1}(y)} = (O)^{t_{1,1}}(y)$ and $l(\mathrm{u}) \leq 4$.

Let us consider the totality $G_{1,2}$ of the commutators $t(x, y) = [t_{0,1}(x), T_{1,1}(y)]$. Then its action of on zero line (point) does not change its first, second components. The third component will be $2xy$. Let us consider $T_{1,2}(y) = t(x/2, y)$. Let $u = [O]^{T_{1,2}(y)}$, then $u_{1,2} = y$. Similarly, we construct the totality $G_{2,1}$ of commutators $t(x, y)[t_{1,0}(x)T_{1,1}(y)]$ containing element $T = T_{2,1}(y)$, such that $O^T = O^{T_{2,1}(y)} = [0, 0, 0, y, \dots]$. We can write the irreducible presentation of $g \in G$ in the form (3.1) starting either with element from U_1 or U_2. It means that $l(g) \leq 8$ for $g \in G_{1,2} \cup G_{2,1}$

Let us define $G_{2,2}$ as totality of commutators $[t_{1,0}(x), T_{1,2}(y)]$ (or equivalently as set of elements of kind $[t_{0,1}(x), T_{2,1}(y)]$. Then for element $t \in G_{2,2}$ we have $O^t = O^{t_2(xy)} = (0, 0, 0, 0, xy, xy, \dots)$. We have $l(g) \leq 16$ for $g \in G_{2,2}$.

We can define recurrently $Gi, i + 1$, $Gi + 1, i$ and $G_{i+1,i+1}$, $i \geq 2$ as totalities of elements of kind $[t_{0,1}(x), T_{i,i}(y)]$, $[t_{1,0}(x), T_{i,i}(y)]$ and $[t_{0,1}(x), T_{i,i+1}(y)]$, respectively. The length of elements from $G_{i,i+1}$ and $G_{i+1,i}$ are bounded by 2^{2i+1} and $l(g) \leq 2^{2i+2}$ for $g \in G_{i+1,i+1)}$. Notice, that the element $g \in G_\alpha$ acting on element v (point or line) changing only components v_β , $\beta > \alpha$. We can find an element $g \in G_\alpha$, such that for $u = v^g$ the component u_α equals zero.

Let $u \in G$ be element such that $O^u = v$. Then by consecutive applications of appropriate transformations $g \in G_\alpha$ with respect to natural order on roots we

can move v to O It means that each element $g \in G$ can be presented as product $g_{0,1}g_{1,0}g_{1,1}\dots g_\alpha\dots$, where $g_\alpha \in G_\alpha$. Let $d(\alpha)$ be the length of g_α. We can bound the length of g by the sum S of d_α. In case when α is not simple root we have a choice to write irreducible representation of g_α, is with the first character from U_1 or the one from U_2. It allows slightly improve the bound foe the diameter - get $S-m+1$ instead of S.

Let us count S for the case $m = 2\mathrm{mod}\ 3$. If $m = 2$ then $S = 6$. In case of $m \geq 5$ each triple of roots $(i, i+1)$, $(i+1, i)$, $(i+1, i+1)$, $i \geq 1$ contributes summands 2^{2i+1}, 2^{2i+1} and 2^{2i+2}. So we can count S via the sum of the geometrical progression.

Let $m = 2\mathrm{mod}\ 3$ then each triple as above contribute summand 2^{2i+3}. So we have the geometrical progression $2^{(2i+3)}$, $i = 1, \dots (m-2)/3$. The roots $(0, 1)$, $(1, 0)$ and $(1, 1)$ contribute 6.

In case $m = 0\mathrm{mod}\ 3$ we have a geometrical progression 2^{2i+3}, $i = 1, \dots, m/3-1$ and last root contributes $32 \times 4^{m/3-1}$.

In case $m = 1\mathrm{mod}3$) we have a geometrical progression 2^{2i+3}, $i = 1, \dots, (m-4)/3$ and two last roots contributes $64 \times 4^{(m-4)/3}$

This way we are getting the formulae for the bound.

□

Remark. Theorem 1 follows directly from theorem 12 and Proposition 3.

References

[1] N. Biggs, *Algebraic Graph Theory* (2nd ed), Cambridge, University Press, 1993.

[2] N.L. Biggs, *Graphs with large girth*, Ars Combinatoria, 25C (1988), 73–80.

[3] N.L. Biggs and A.G. Boshier, *Note on the Girth of Ramanujan Graphs*, Journal of Combinatorial Theory, Series **B 49**, pp. 190–194 (1990).

[4] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[5] B. Bollobás, *Random Graphs*, Academic Press, London, 1985.

[6] A. Brouwer, A. Cohen and A. Niemaier *Distance Regular Graphs*, Springer Verlag (1987), 380 p.

[7] F. Lazebnik, V. A. Ustimenko, *New Examples of graphs without small cycles and of large size*, Europ. J. of Combinatorics, 14 (1993) 445-460.

[8] F. Lazebnik F. and V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. , 60, (1995), 275 - 284.

[9] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.

[10] Lazebnik, F., Ustimenko, V.A. and A.J. Woldar, *A characterisation of the components of the graph $D(k, q)$*, Discrete Mathematics, 157 (1996), 271-283.

[11] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.

[12] W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory*, Interscience publ., 1966.

[13] G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.

[14] G. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii., 24, N1, 51-60. English translation publ. Journal of Problems of Information transmission (1988), 39-46.

[15] M. Margulis, *Arithmetic groups and graphs without short cycles*, 6th Intern. Symp. on Information Theory, Tashkent, abstracts, vol. 1, 1984, pp. 123-125 (in Russion).

[16] V. A. Ustimenko, *Linear interpretation of Chevalley group flag geometries*, Ukrainian Math. J. 43, Nos. 7,8 (1991), pp. 1055–1060 (in Russian).

[17] V. A. Ustimenko, *Coordinatisation of regular tree and its quotients*, in "Voronoi's impact on modern science, eds P. Engel and H. Syta, book 2, National Acad. of Sci, Institute of Matematics, 1998, 228p.

[18] V. A. Ustimenko, *On the varieties of parabolic subgroups, their generalizations and combinatorial applications*, Acta Applicandae Mathematicae, 52 (1998), 223-238.
[19] V. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, 2002, vol. 74, N2, 117-153.
[20] V. Ustimenko, *CRYPTIM: Graphs as tools for symmetric encryption*, In Lecture Notes in Comput. Sci., 2227, Springer, New York, 2001.
[21] V. Ustimenko, *Maximality of affine group and hidden graph cryptsystems*, Journal of Algebra and Discrete Mathematics, October, 2004, v.10, pp 51-65.
[22] V. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Zapiski Nauchnyh Seminarov POMI, vol. 326, "Representation Theory, Dynamical Systems. Combinatorial and Algorithmic Methods, 2005, 214-235.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 35–42
ISSN 1930-1235: (2009)

GENERALIZED COMPLEMENTARITY PROBLEMS IN BANACH SPACES

A. P. Farajzadeh[1,*]

[1] *Department of Mathematics,*
Razi University
Kermanshah, 67149, Iran.
email: ali-ff@sci.razi.ac.ir.

[*] *School of Mathematics,*
Institute for research in Fundamental Sciences (IPM)
P.O. Box 19395-5746.

A. Amini-Harandi

Department of Mathematics
University of Shahrekord,
Shahrekord, 88186-34141, Iran.
email: amini-h@yahoo.com

Abstract. In this paper, a class of complementarity problem and three classes of variational inequalities in real Banach spaces are introduced, and the equivalence among them are established under certain conditions. Several coercivity conditions are introduced for the existence of solutions of the generalized complementarity problem. Our results can be viewed as extension and generalization of the recent paper [N. J. Huang, J. Li, D. O'Regan, Generalized f-complementarity problems in Banach spaces, vol. **142,** pg. 3828-3840, 2008].

1. Introduction and Preliminaries

The complementarity problem (for short, CP) was introduced first by Cottle and Dantzig [6] in 1968. It is well known that (CP) is closely related to optimization problems, variational inequalities, equilibrium problems, fixed point theory, operations research, game theory, economics and finance, as well as applied sciences. Since 1960s, (CP) has been studied extensively by many authors (see, for instance, [1]-[6], [8]-[16] and the references therein).

In this paper let X be a real Banach space with dual X^*, and K a nonempty, closed and convex cone of X. Denote $\langle t, x\rangle$ value of the linear continuous function $t \in X^*$ at x. In 2001, Yin, Xu and Zhang [19] introduced and studied a class of

2000 *Mathematics Subject Classification.* Primary 49J40; Secondary 47J20, 54C60, 91B50.
Key words and phrases. Generalized complementarity problem; generalized variational inequality problems; positively homogeneous mapping; KKM mapping.
The first author was in part supported by a grant from IPM (No. 87490015).

f-complementarity problems (for short, f-CP), which consists of finding $\overline{x} \in K$ such that

$$\langle T\overline{x}, \overline{x}\rangle + f(\overline{x}) = 0 \text{ and } \langle T\overline{x}, y\rangle + f(y) \geq 0, \ \forall y \in K.$$

The (f-CP) has been extended to the vector f-complementarity problem by Fang and Huang [9], the vector f-implicit complementarity problem by Li and Huang [15] and (the latest extension) the generalized f-complementarity problem (for short, Gf-CP) by Huang, Li and O'Regan [12] which consists of finding $\overline{x} \in K$ and $\overline{t} \in F(\overline{x})$ such that

$$\langle \overline{t}, \overline{x}\rangle + f(\overline{x}) = 0 \text{ and } \langle \overline{t}, y\rangle + f(y) \geq 0, \ \forall y \in K,$$

where $F : K \to 2^{X^*} \setminus \{\emptyset\}$.

In this paper we consider the following problem which consists of finding $\overline{x} \in K$ and $\overline{t} \in F(\overline{x})$ such that

$$\text{(GCP)} \qquad G(\overline{t}, \overline{x}) = 0 \text{ and } G(\overline{t}, y) \geq 0, \ \forall y \in K,$$

where $G : X^* \times K \to \mathbb{R}$. We call this problem generalized complementarity problem (GCP) and denote it by S_c the solution set of (GCP).

Remark that if we define $G(t, x) = \langle t, x\rangle + f(x)$, where $f : K \to (-\infty, \infty)$, then (GCP) reduces to the (Gf-CP).

We also study the following three classes of variational inequalities:

$(GVI)_1$ Find $\overline{x} \in K$ such that

$$\exists\ \overline{t} \in F(\overline{x}) : \ G(\overline{t}, y) \geq G(\overline{t}, \overline{x}), \ \forall\ y \in K;$$

$(GVI)_2$ Find $\overline{x} \in K$ such that

$$\forall\ y \in K, \ \exists\ \overline{t} \in F(\overline{x}) \ : \ G(\overline{t}, y) \geq G(\overline{t}, \overline{x});$$

$(GVI)_3$ Find $\overline{x} \in K$ such that

$$\forall\ y \in K, \ \forall\ t \in F(y) \ : \ G(t, y) \geq G(t, \overline{x}).$$

We denote the solution set of $(GVI)_1$, $(GVI)_2$ and $(GVI)_3$ by S_1, S_2 and S_3, respectively.

2. EQUIVALENCE among (G-CP) $(GVI)_1$, $(GVI)_2$ and $(GVI)_3$

In this section, we investigate the equivalence among (G-CP) $(GVI)_1$, $(GVI)_2$ and $(GVI)_3$. First we recall some definitions. Let $G : X^* \times K \to \mathbb{R}$ and $t \in X^*$. The mapping $x \to G(t, x)$ is said to be

- positively homogeneous, if for all $\alpha > 0$ and $x \in K$,
$$G(t, \alpha x) = \alpha G(t, x);$$
- convex, if for all pairs $(x, y) \in K \times K$ and all $\lambda \in [0, 1]$,
$$G(t, \lambda x + (1 - \lambda)y) \leq \lambda G(t, x) + (1 - \lambda)G(t, y);$$
- sublinear, if it is convex and homogeneous;
- subadditive, if for all pairs $(x, y) \in K \times K$,
$$G(t, x + y) \leq G(t, x) + G(t, y);$$

• lower semicontinuous (l.s.c.), if for every $x \in K$,

$$\liminf_{y \to x} G(t, y) \geq G(t, x).$$

Theorem 2.1. *Let $F : K \to 2^{X^*} \backslash \{\emptyset\}$ and $G : X^* \times K \to \mathbb{R}$. Then the following statements are valid:*

(i) $S_c \subseteq S_1$.
(ii) *If $G(x, .)$ is positively homogeneous, then $S_1 \subseteq S_c$.*

Proof. (i) is trivial.

(ii) Let $\overline{x} \in S_1$. Then $\overline{x} \in K$ and

$$\exists \overline{t} \in F(\overline{x}) : \ G(\overline{t}, y) \geq G(\overline{t}, \overline{x}), \ \forall y \in K. \tag{2.1}$$

By letting $y = 2\overline{x}$ and $y = \frac{\overline{x}}{2}$,respectively, in 2.1 (note that K is convex cone and the mapping $x \to G(t, x)$ is positively homogeneous) we get

$$G(\overline{t}, \overline{x}) \geq 0 \ \text{ and } G(\overline{t}, \overline{x}) \leq 0,$$

and hence

$$G(\overline{t}, \overline{x}) = 0. \tag{2.2}$$

Now (2.1) and (2.2) imply that

$$G(\overline{t}, \overline{x}) = 0 \ \text{ and } G(\overline{t}, y) \geq 0.$$

Hence $\overline{x} \in S_c$. The proof is complete.

□

Definition 2.2. Let $F : K \to 2^{X^*} \backslash \{\emptyset\}$ and $G : X^* \times K \to \mathbb{R}$. The F is said to be

• upper semi-continuous (u.s.c) at $x \in K$ if, for every open set V containing $F(x)$, there exists an open set U containing x such that $F(U) \subseteq V$, where X^* is equipped with the w^* -topology;
• upper hemi-continuous (u.h.c) if the restriction of F on straight lines is upper semi-continuous;
• G-monotone if, for every $x, y \in K$

$$G(t_x, x) + G(t_y, y) \geq G(t_x, y) + G(t_y, x) \ \forall t_x \in F(x), \forall t_y \in F(y);$$

• strictly G-monotone if, for every $x, y \in K$

$$G(t_x, x) + G(t_y, y) > G(t_x, y) + G(t_y, x) \ \forall t_x \in F(x), \forall t_y \in F(y);$$

Lemma 2.3. *([18]) Let A be a nonempty convex set in a vector space and let B be a nonempty compact convex set in a Hausdorff topological vector space. Suppose that g is a real valued function on $A \times B$ such that for each $a \in A$, $g(a, .)$ is l.s.c and convex on B, and for each fixed $b \in B$, $g(., b)$ is concave on A. Then*

$$\min_{b \in B} \sup_{a \in A} g(a, b) = \sup_{a \in A} \min_{b \in B} g(a, b).$$

Theorem 2.4. *Let $F : K \to 2^{X^*} \backslash \{\emptyset\}$ and $G : X^* \times K \to \mathbb{R}$. Then the following hold:*

(i) $S_1 \subseteq S_2$.
(ii) *If F is G-monotone, then $S_2 \subseteq S_3$.*
(iii) *If F is u.h.c, for each fixed $t \in X^*$, $x \to G(t, x)$ is convex, and for each fixed $x \in K$, $t \to G(t, x)$ is u.s.c, then $S_3 \subseteq S_2$.*

(iv) *If F has w^*-compact and convex values, for each fixed $x \in K,\ t \to G(t,x)$ is concave, l.s.c, and for each fixed $t \in X^*,\ x \to G(t,x)$ is convex, then $S_1 = S_2$.*

Proof. (i) It is trivial.
(ii) Let $\overline{x} \in S_2$. Then

$$\forall y \in K,\ \exists \overline{t} \in F(\overline{x})\ :\ G(\overline{t}, y) \geq G(\overline{t}, \overline{x}). \quad (2.3)$$

Since F is G-monotone, for every $y \in K$ and $t \in F(y)$, we have

$$G(t,y) + G(\overline{t}, \overline{x}) \geq G(t, \overline{x}) + G(\overline{t}, y). \quad (2.4)$$

It follows from (2.3) and (2.4) that

$$G(t,y) - G(t,\overline{x}) \geq G(\overline{t}, y) - G(\overline{t}, \overline{x}) \geq 0\ \forall y \in K, \forall t \in F(y),$$

and so $\overline{x} \in S_3$.
(iii) Suppose that the conclusion is not true. Then there exists $\overline{x} \in K$ such that $\overline{x} \in S_3$ and $\overline{x} \notin S_2$. It follows from $\overline{x} \notin S_2$, that there exists $y \in K$ for which,

$$G(t,y) < G(\overline{t}, \overline{x}),\ \forall t \in F(\overline{x}).$$

Hence, setting $x_\lambda = \lambda y + (1-\lambda)\overline{x}$ and taking λ close to 0, we have

$$G(t_\lambda, y) < G(\overline{t}, \overline{x}) \qquad \forall t_\lambda \in F(x_\lambda), \quad (2.5)$$

(note $\{t \in X^* : G(t,y) < G(\overline{t}, \overline{x})\}$ is a w^*-open neighborhood of $F(\overline{x})$ and F is u.h.c). From the convexity, for each fixed $t \in X^*$, the mapping $x \to G(t,x)$ gives

$$G(t_\lambda, x_\lambda) \leq \lambda G(t_\lambda, y) + (1-\lambda) G(t_\lambda, \overline{x}). \quad (2.6)$$

Now (2.5) and (2.6) imply that

$$G(t_\lambda, \overline{x}) < G(\overline{t}, \overline{x}),\ \forall t_\lambda \in F(x_\lambda),$$

which contradicts $\overline{x} \in S_3$. Thus, $\overline{x} \in S_2$ and (iii) is true.
(iv) From conclusion (i), it suffices to show that $S_2 \subseteq S_1$. Let $\overline{x} \in S_2$. Then

$$\forall y \in K,\ \exists \overline{t} \in F(\overline{x})\ :\ G(\overline{t}, y) \geq G(\overline{t}, \overline{x}). \quad (2.7)$$

Define $g : K \times F(\overline{x}) \to \mathbb{R}$ by

$$g(a,b) = G(b, \overline{x}) - G(b,a)$$

One can easily see that g satisfies all assumptions of Lemma 2.3. Hence it follows from Lemma 2.3 that

$$\min_{b \in F(\overline{x})} \sup_{a \in K} (g(a,b) = G(b,\overline{x}) - G(b,a)) = \sup_{a \in K} \min_{b \in F(\overline{x})} g(a,b) \leq 0, \quad (2.8)$$

(note (2.7) guarantees the inequality in (2.8)). Thus,

$$\exists \overline{t} \in F(\overline{x}) :\ \sup_{a \in K}\ g(a, \overline{t}) \leq 0,$$

and so

$$G(\overline{t}, \overline{x}) \leq G(\overline{t}, y),\ \forall y \in K.$$

Therefore $\overline{x} \in S_1$. This completes the proof. □

Theorem 2.5. *Let $G : X^* \times K \to \mathbb{R}$ such that $G(a,.)$ is sublinear. Assume that $F : K \to 2^{X^*} \setminus \{\emptyset\}$ is G-monotone, u.h.c., and has w^*-compact convex values. Then*

(i) $S_c = S_1 = S_2 = S_3$.

(ii) *If F is strictly G-monotone and $S_i \neq \emptyset (i = 1, 2, 3)$, then S_c consists of one point.*

Proof. Conclusion (i) follows directly from Theorem 2.4.
(ii) It is sufficient, by (i), to show that S_2 consists of one point. Assume that F is strictly G-monotone and $S_2 \neq \emptyset$. Let $\overline{x_1}$ and $\overline{x_2}$ solve $(GVI)_2$. Then, by (i), $\overline{x_1}, \overline{x_2} \in S_1$ and so

$$\exists\ \bar{t}_1 \in F(\overline{x}_1)\ :\ G(\bar{t}_1, \overline{x}_2) \geq G(\bar{t}_1, \overline{x}_1), \tag{2.9}$$

and

$$\exists\ \bar{t}_2 \in F(\overline{x}_2)\ :\ G(\bar{t}_2, \overline{x}_1) \geq G(\bar{t}_2, \overline{x}_2). \tag{2.10}$$

If $\overline{x}_1 \neq \overline{x}_2$, then the strict G-monotonicity of F implies that

$$G(\overline{t_1}, \overline{x_1}) + G(\overline{t_2}, \overline{x_2}) > G(\overline{t_1}, \overline{x_2}) + G(\overline{t_2}, \overline{x_1}). \tag{2.11}$$

Now from (2.9) and (2.11) we get

$$G(\bar{t}_2, \overline{x}_2) > G(\bar{t}_2, \overline{x}_1),$$

which contradicts (2.10). Hence $\overline{x}_1 = \overline{x}_2$, and so S_2 consists of one point. This completes the proof. □

3. Coercivity Conditions for (GCP)

Denote by $\mathcal{K}$ the set of all weakly compact convex subset of K. We consider the following three classes of coercivity conditions:

(C_1) $\exists E \in \mathcal{K}, \forall x \in K\backslash E, \forall t \in F(x), \exists y \in E :\ G(t, y) < G(t, x)$;

(C_2) $\exists E \in \mathcal{K}, \forall x \in K\backslash E, \exists y \in E, \forall t \in F(x) :\ G(t, y) < G(t, x)$;

(C_3) $\exists E \in \mathcal{K}, \forall x \in K\backslash E, \exists y \in E, \exists t \in F(y) :\ G(t, y) < G(t, x)$.

Theorem 3.1. *Let $F : K \to 2^{X^*}\backslash\{\emptyset\}$ and $G : X^* \times K \to \mathbb{R}$. Then the following statements hold:*

(i) *Condition (C_1) (resp., (C_2) and (C_3)) implies that S_1 (resp., S_2 and S_3) is contained in the weakly compact set E.*
(ii) *Condition (C_2) implies (C_1).*
(iii) *If F has convex values, for each fixed $t \in X^*$, $x \to G(t, x)$ is convex l.s.c. and for each fixed $x \in K$ $t \to G(t, x)$ is concave, then condition (C_1) implies (C_2).*
(iv) *If F is G-monotone, then condition (C_3) implies (C_2).*

Proof. Statements (i), (ii) and (iv) are obvious. It suffices to show that conclusion *(iii)* holds. Assume that condition (C_1) holds. Then

$$\exists E \in \mathcal{K}, \forall x \in K\backslash E, \forall t \in F(x), \exists y \in E :\ G(t, y) < G(t, x).$$

Assume F has convex values and $G(t, .)$ is convex and l.s.c. (w.l.s.c). As the proof in (iv) of Theorem 2.4, for any given $x \in K\backslash E$, define $h : F(x) \times E \to \mathbb{R}$ by

$$h(a, b) = G(a, b) - G(a, x).$$

It is easy to see that h satisfies all the assumptions of Lemma 2.3. Hence Lemma 2.3 implies that

$$\min_{b\in E} \sup_{a\in F(x)} h(a, b) = \sup_{a\in F(x)} \min_{b\in E} h(a, b) < 0$$

and so

$$\exists y \in E: \sup_{a \in F(x)} h(a,y) < 0.$$

Therefore

$$G(t,y) < G(t,x),\ \forall t \in F(x),$$

which implies that condition (C_2) holds. This completes the proof. □

Let P be a nonempty subset of a topological vector space Y. A set-valued mapping $G: P \to 2^Y$ is called a KKM-mapping if, for every finite subset $\{y_1, y_2, ..., y_k\}$ of P,

$$co\{y_1, y_2, ..., y_k\} \subseteq \bigcup_{i=1}^{k} G(y_i).$$

Lemma 3.2. *([8]) Let P a nonempty subset of a Hausdorff topological vector space Y. Let $G: P \to 2^Y$ be a KKM-mapping such that, for any $y \in Y$, $G(y)$ is closed and, for some $y^* \in P$, $G(y^*)$ is compact . Then*

$$\bigcap_{y \in P} G(y) \neq \emptyset.$$

Theorem 3.3. *Let $G: X^* \times K \to \mathbb{R}$ and $F: K \to 2^{X^*} \backslash \{\emptyset\}$ be u.h.c., and G-monotone. Let, for each fixed $t \in X^*$, the mapping $x \to G(t,x)$ be a convex and l.s.c. If condition C_2 holds, then S_2 is nonempty.*

Proof. Suppose that condition C_2 holds, i.e.,

$$\exists E \in \mathcal{K}, \forall x \in K \backslash E, \exists y \in E, \forall t \in F(x):\ G(t,y) < G(t,x).$$

Define $H_0: K \to 2^E$ by

$$H_0(y) = \{x \in E: G(t,y) \geq G(t,x), \forall t \in F(y)\} \qquad \forall y \in K.$$

It is clear that $\bigcap_{y \in K} H_0(y) \subseteq S_3$, and from Theorem 2.5 one has $\bigcap_{y \in K} H_0(y) \subseteq S_3 = S_2$. We now show that $\bigcap_{y \in K} H_0(y) \neq \emptyset$. Since the mapping $x \to G(t,x)$ is convex and l.s.c, it is easy to show that $H_0(y)$ is weakly closed, for each $y \in K$, and so $\bigcap_{y \in K} H_0(y)$ is weakly closed. Hence, since E is w-compact, $H_0(y)$ and $\bigcap_{y \in K} H_0(y)$ are compact. Thus, it suffices to prove that the family $\{H_0(y)\}_{y \in K}$ has the finite intersection property. Let $\{y_1, y_2, ..., y_k\}$ be any finite subset of K, and set $M = \overline{co}(E \cup \{y_1, y_2, ..., y_k\})$, where $\overline{co}$ denotes the closed convex hull. Then M is nonempty, w-compact and convex. Define $H: M \to 2^M$ by

$$H(y) = \{x \in M: G(t,y) \geq G(t,x), \forall t \in F(y)\}, \qquad \forall y \in M.$$

Clearly $y \in H(y)$, and the convexity of the mapping $x \to G(t,x)$ and l.s.c, respectively, imply that $H(y)$ is convex and closed, respectively. Since M is weakly compact, so is $H(y)$. Next, we prove that H is a KKM-mapping. Suppose to the contrary that there exist a finite subset $\{u_1, ..., u_n\}$ of M and $\lambda_i \geq 0, i = 1, 2, ..., n$ with $\sum_{i=1}^{n} \lambda_i = 1$, such that

$$u = \sum_{i=1}^{n} \lambda_i u_i \notin \bigcup_{j=1}^{n} H(u_j).$$

Then, for each $i = 1, 2, ..., n$, there exists $t_i \in F(u_i)$ such that

$$G(t_i, u_i) < G(t_i, u).$$

Since F is G-monotone, we have

$$G(t_i, u) + G(t, u_i) \leq G(t_i, u_i) + G(t, u),$$

and so

$$G(t, u_i) \leq G(t, u).$$

From the convexity of the mapping $x \to G(t, x)$, we have

$$0 = G(t, u) - G(t, u) = G(t, \sum_{i=1}^{n} \lambda_i u_i) - G(t, u) \leq$$

$$\sum_{i=1}^{n} \lambda_i (G(t, u_i) - G(t, u)) < 0,$$

which is a contradiction. Hence H is a KKM-mapping. Therefore H satisfies all the assumptions of Lemma 3.2 and hence $\bigcap_{y \in M} H(y) \neq \emptyset$. So

$$\exists\, \overline{x} \in M\ \forall\, y \in M,\ \forall\, t \in F(y)\ :\ G(t, y) \geq G(t, \overline{x}).$$

Hence $\overline{x}$ is a solution of $(GVI)_3$ in M. From Theorem 2.5 (i), we get that $\overline{x}$ is a solution of $(GVI)_2$ in M and so

$$\forall\, y \in M,\ \exists\, \overline{t} \in F(\overline{x})\ :\ G(\overline{t}, y) \geq G(\overline{t}, \overline{x}).$$

Since condition C_2 holds, one has $\overline{x} \in E$. Moreover, $\overline{x} \in H_0(y_j)$, for $j = 1, 2, ..., k$, which implies that $\{H_0(y)\}_{y \in K}$ has the finite intersection property. This completes the proof. □

Theorem 3.4. *Let $G : X^* \times K \to \mathbb{R}$ and $F : K \to 2^{X^*} \setminus \{\emptyset\}$ is G-monotone, u.h.c., and has w^* compact convex values. Let $G(t, .)$ be sublinear and l.s.c. If each of conditions (C_1), (C_2) and (C_3) holds, then S_c is nonempty and bounded.*

Proof. The conclusion follows directly from Theorem 2.5 and Theorem 3.3. □

Acknowledgments

The authors would like to thank referees for valuable suggestions and remarks.

References

[1] C. Baiochhi and A. Capelo, Variational and Quasivariational Inequalities, *J. Wiley and Sons, New York.* 1984.

[2] E. Blum and W. Oettli, From optimization and From optimization and variational inequalities to equilibrium problems, *Mathematics Student.,* vol. **63**, pg. 123-145, 1994.

[3] A. Bnouhachem and M. Aslam Noor, A new predictor-corrector method for pseudomonotone nonlinear complementarity problem, *Inter. J. Comput. Math.,* vol. **85**, pg. 1023-1038, 2008.

[4] Y. J. Cho, J. Li and N. J. Huang, Solvability of implicit complementarity problems, *Math. Comput. Modelling.*,vol. **45**, pg. 1001-1009, 2007.

[5] R. W. Cottle, Complementarity and variational problems, *Sympos. Math.,* vol. **19,** pg. 177-208, 1976.

[6] R. W. Cottle and G. B. Dantzig, Complementarity pivot theory of mathematical programming, *Linear Algeb. Appl.,* vol. **1,** pg. 163-185, 1968.

[7] M. Fakhar and J. Zafarani, Generalized vector equilibrium problems for pseudomonotone multivalued bifunctions, *J. Optim. Theory Appl.,* vol. **126,** pg. 109-124, 2005.

[8] K. Fan, A generalization of Tychonoff's fixed point theorem, *Math. Ann.,* vol. **142,** pg. 305-310, 1961.

[9] Y.P. Fang and N.J. Huang, The Vector F-Complementarity Problems with Demipseudomonotone Mappings in Banach Spaces, *App. Math. Lett.,* Vol. **16,** pg. 1019–1024, 2003.

[10] A. P. Farajzadeh, A. Amini-Harandi and M. Aslam Noor, On the generalized vector F-implicit complementarity problems and vector F-implicit variational inequality problems, *Math. Comm.,* vol. **12,** pg. 203-211, 2007.

[11] R. Glowinski, J. L. Lions and R. Tremolieres, Numerical Analysis of Variational Inequalities, *North-Holland, Amsterdam, Holland.,* 1981.

[12] N. J. Huang, J. Li, D. O'Regan, Generalized f-complementarity problems in Banach spaces, *J. Non. Anal.,* vol. **142**, pg. 3828-3840, 2008.

[13] S. Itoh, W. Takahashi and K. Yanagi, Variational inequalities and complementarity problems, *J. Math. Soc. Japan,* vol. *30*, pg. 23-28, 1978.

[14] S. Karamardian, Generalized complementarity problems, *J. Optim. Theory Appl.,* vol. **8**, pg. 223-239, 1971

[15] J. Li, N. J. Huang, Vector F-implicit complementarity problems in Banach spaces, *J. Math. Appl. Let.,* vol. *19,* pg. 464-471, 2006.

[16] M. A. Noor, Some developments in general variational inequalities, *Appl. Math. Computation,,* vol. **152** pg. 199-277, 2004.

[17] M. A. Noor, W. Oettli, On generalized nonlinear complementarity problems and quasiequilibria, *Le Math.,* vol. **49** pg. 313-331, 1994.

[18] M. Sion, On general minimax theorems, *Pac. J. Math.,* vol. **8** pg. 171-176, 1958.

[19] H.Y. Yin, C.X. Xu, Vector variational inequality and implicit vector complementarity problems, in " Vector Variational Inequalities and Vector Equilibria" (F. Giannessi, Eds.), Kluwer *Academic Publishers, Dordrechet, Holland.,* pg. 491-505, 2000.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 43–48
ISSN 1930-1235: (2009)

CONVEXITY OF FINITE SUMS

Anthony Sofo

Research Group in Mathematical Inequalities and Applications
School of Engineering and Science
Victoria University, PO Box 14428 Melbourne
VIC 8001, Australia.
anthony.sofo@vu.edu.au

Abstract. Convexity and log convexity results are established for sums involving ratios of binomial coefficients. We utilise recent results in which integral identities have been given to represent sums involving ratios of binomial coefficients.

1. Introduction

The integral representation of series of ratios of binomial coefficients have recently been investigated by a number of authors, see in particular Amghibech [1], Batir [2], and Sofo [5, 6, 7]. Recently Purkait and Sury [4], using mainly combinatorial methods, obtained expressions for

$$S=\sum_{n=0}^{p}\frac{(-1)^n n^r\binom{p}{n}}{\binom{n+j}{n}}$$

and deduced that for even integer $r\geq 0$ and $p=j>\frac{r}{2}$, S is identically zero or $\frac{1}{2}$ according as to whether $r>0$ or not. In this paper we supplement the results of Purkait and Sury by considering convexity properties of slightly more general forms of S.

In particular, the following theorem was given in [5].

Theorem 1. *for $a>0$, $p\geq 1, t\in\mathbb{R}$ and $j>0$*

$$S(a,j,p,t)=\frac{1}{j}\sum_{n=0}^{p}\frac{t^n\binom{p}{n}}{\binom{an+j}{j}}=\int_0^1(1-x)^{j-1}\left(1+tx^a\right)^p dx. \tag{1.1}$$

For an integer a we can write

$$\sum_{n=0}^{p}\frac{t^n\binom{p}{n}}{\binom{an+j}{j}}={}_{a+1}F_a\left[\begin{matrix}\frac{1}{a},\frac{2}{a},\frac{3}{a},\ldots,\frac{a}{a},-p\\ \frac{1+j}{a},\frac{2+j}{a},\frac{3+j}{a},\ldots,\frac{a+j}{a}\end{matrix}\middle|-t\right],$$

2000 *Mathematics Subject Classification.* Primary 35E10. Secondary 26A09, 26B20.
Key words and phrases. Convexity, Log convexity, Integral identities.

where the generalised hypergeometric representation ${}_pF_q\left[\cdot,\cdot\right]$, *is defined as*

$$ {}_pF_q\left[\begin{array}{c} a_1,a_2,...,a_p \\ b_1,b_2,...,b_q \end{array}\middle| t\right]=\sum_{n=0}^{\infty}\frac{(a_1)_n\ (a_2)_n\ ...\,(a_p)_n\ t^n}{(b_1)_n\ (b_2)_n\ ...\,(b_q)_n\ n!} $$

and $(w)_\alpha = w\,(w+1)\,(w+2)\,...\,(w+\alpha-1)=\frac{\Gamma(w+\alpha)}{\Gamma(w)}$ *is Pochhammer's symbol.*

The following analysis establishes the monotonicity and convexity properties of $S\left(a,j,p,t\right)$, by the use of its integral representation (1.1).

2. Convexity Properties

The following theorem is proved.

Theorem 2. *For* $p\geq 1$, $a\geq 1, t>0$ *and* $j>0$ *the function* $a\mapsto S\left(a,j,p,t\right)$, *as given in Theorem 1 is strictly decreasing and convex with respect to the parameter* $a\in[1,\infty)$ *for every* $x\in[0,1]$.

Proof. Let

$$ g\left(x,a\right)=\left(1-x\right)^{j-1}\left(1+tx^a\right)^p \tag{2.1} $$

be an integrable function for $x\in[0,1]$ and put

$$ f\left(a\right)=\int_0^1 g\left(x,a\right)dx, $$

so that $f\left(1\right)=\frac{1}{j}\ {}_2F_1\left[\begin{array}{c} 1,-p \\ 1+j \end{array}\middle| -t\right]$.

Applying the Leibniz rule for differentiation under the integral sign, we have that

$$ \begin{aligned} f'\left(a\right)&=\int_0^1\frac{\partial}{\partial a}g\left(x,a\right)dx \\ &=pt\int_0^1 x^a\left(1-x\right)^{j-1}\left(1+tx^a\right)^{p-1}\ln x dx \end{aligned} \tag{2.2} $$

Since

$$ x^a\left(1-x\right)^{j-1}\left(1+tx^a\right)^{p-1}\ln x<0\quad\text{for}\quad x\in(0,1), $$

then $f'\left(a\right)<0$, so that the sum of the ratio of binomial coefficients (1.1), is a strictly decreasing sum with respect to the parameter a for $x\in[0,1]$. Now

$$ \begin{aligned} f''\left(a\right)&=\int_0^1\frac{\partial^2}{\partial^2 a}g\left(x,a\right)dx \\ &=pt\int_0^1\left(1-x\right)^{j-1}\left(1+tx^a\right)^{p-2}x^a\left(ptx^a+1\right)\left(\ln x\right)^2dx, \end{aligned} \tag{2.3} $$

and since

$$ \left(1-x\right)^{j-1}\left(1+tx^a\right)^{p-2}x^a\left(ptx^a+1\right)\left(\ln x\right)^2>0, $$

then $f''\left(a\right)>0$ so that (1.1) is a convex function for $x\in[0,1]$. □

In the following we establish the log convexity of the function $a\mapsto S\left(a,j,p,t\right)$ with respect to the positive parameter a. Firstly, we state the Cauchy-Buniakowsky-Schwarz inequality.

Cauchy-Buniakowsky-Schwarz inequality: *Let $p(x)$, $q(x)$ and $r(x)$ be integrable functions for $x \in [\alpha, \beta]$, then*

$$\left(\int_\alpha^\beta p(x)\, q^2(x)\, dx\right)\left(\int_\alpha^\beta p(x)\, r^2(x)\, dx\right) \geq \left(\int_\alpha^\beta p(x)\, q(x)\, r(x)\, dx\right)^2.$$

A proof of this theorem can be found in [3].

Theorem 3. *For $p \geq 1$, $a \geq 1, t > 0$ and $j > 0$, the function $a \mapsto S(a, j, p, t)$ as given in Theorem 1 is log convex with respect to the parameter $a \in [1, \infty)$ for every $x \in [0, 1]$.*

Proof. Let

$$h(a) = \log\left(\int_0^1 g(x, a)\, dx\right),$$

where $g(x, a)$ is given by (2.1), and applying the Leibniz rule for differentiation under the integral sign, we have that:

$$h'(a) = \frac{pt\int_0^1 x^a (1-x)^{j-1}(1+tx^a)^{p-1}\ln x dx}{\int_0^1 (1-x)^{j-1}(1+tx^a)^p\, dx} < 0.$$

Now,

$$h''(a) = \frac{\left(\int_0^1 \frac{\partial^2}{\partial^2 a} g(x, a)\, dx\right)\left(\int_0^1 g(x, a)\, dx\right) - \left(\int_0^1 \frac{\partial}{\partial a} g(x, a)\, dx\right)^2}{\left(\int_0^1 g(x, a)\, dx\right)^2}, \tag{2.4}$$

where $g(x, a)$ is given by (2.1), $\int_0^1 \frac{\partial}{\partial a} g(x, a)\, dx$ is given by (2.2) and $\int_0^1 \frac{\partial^2}{\partial^2 a} g(x, a)\, dx$ is given by (2.3).

Since we require $h''(a) > 0$ it will suffice to prove that

$$\begin{aligned} &pt\int_0^1 (1-x)^{j-1}(1+tx^a)^{p-2}x^a(ptx^a+1)(\ln x)^2\, dx \int_0^1 (1-x)^{j-1}(1+tx^a)^p\, dx \\ &> \left(pt\int_0^1 x^a(1-x)^{j-1}(1+tx^a)^{p-1}\ln x dx\right)^2 > 0 \end{aligned} \tag{2.5}$$

Now,

$$\begin{aligned} &pt\int_0^1 (1-x)^{j-1}(1+tx^a)^{p-2}x^a(ptx^a+1)(\ln x)^2\, dx \\ &> pt\int_0^1 (1-x)^{j-1}(1+tx^a)^{p-2}x^a(ptx^a)(\ln x)^2\, dx \\ &= \int_0^1 (1-x)^{j-1}(1+tx^a)^p\left(\frac{ptx^a\ln x}{1+tx^a}\right)^2 dx > 0, \end{aligned}$$

hence from (2.5),

$$\begin{aligned} &\left(\int_0^1 (1-x)^{j-1}(1+tx^a)^p\left(\frac{ptx^a\ln x}{1+tx^a}\right)^2 dx\right)\left(\int_0^1 (1-x)^{j-1}(1+tx^a)^p\, dx\right) \\ &> \left(\int_0^1 \left(\frac{ptx^a\ln x}{1+tx^a}\right)\cdot(1-x)^{j-1}(1+tx^a)^p\, dx\right)^2 \end{aligned}$$

is satisfied by application of the Cauchy-Buniakowsky-Schwarz inequality and identifying

$$p(x) = (1-x)^{j-1}(1+tx^a)^p, \quad q(x) = \frac{ptx^a \ln x}{1+tx^a} \quad \text{and} \quad r(x) = 1.$$

From (2.4) we can claim $h''(a) > 0$ and the theorem is proved. □

Note: The series (1.1) can be represented in the generalised hypergeometric form as:

$$(2.6) \qquad {}_{a+1}F_a\left[\begin{array}{c} \frac{1}{a}, \frac{2}{a}, \frac{3}{a}, \ldots, \frac{a}{a}, -p \\ \frac{1+j}{a}, \frac{2+j}{a}, \frac{3+j}{a}, \ldots, \frac{a+j}{a} \end{array} \middle| -t\right].$$

We can therefore claim that (2.6) is a log convex function with respect to the parameter $a \geq 1$.

In the paper [5], Sofo further generalised Theorem 1 to obtain the following representation.

Theorem 4. *For $a > 0$, $p \geq 1, t \in \mathbb{R}, r \geq 0$ and $j > 0$ we have*

$$\begin{aligned} \frac{1}{j} S(a,j,p,t,r) &:= \frac{1}{j} \sum_{n=1}^{p} \frac{t^n \; n^r \binom{p}{n}}{\binom{an+j}{j}} \\ &= \int_0^1 (1-x)^{j-1} \frac{(\rho(x))^{(r)}}{a^r} dx \end{aligned}$$

where

$$\begin{cases} (\rho(x))^{(0)} = (1+tx^a)^p \\ \vdots \\ (\rho(x))^{(r)} = x\frac{d}{dx}\left(x\frac{d}{dx}\left(\cdots x\frac{d}{dx}\left((1+tx^a)^p\right)\right)\right) \end{cases}$$

is the consecutive derivative operator of the continuous function $(1+tx^a)^p$ for $x \in (0,1)$.

An example for Theorem 4 is:

(2.7)

$$\frac{1}{j} S(a,j,p,t,1) := \frac{1}{j} \sum_{n=1}^{p} \frac{t^n \; n \; \binom{p}{n}}{\binom{an+j}{j}}$$

$$(2.8) \qquad = pt \int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-1} dx$$

$$= \frac{pt}{j\binom{a+j}{j}} \; {}_{a+1}F_a\left[\begin{array}{c} \frac{a+1}{a}, \frac{a+2}{a}, \frac{a+3}{a}, \ldots, \frac{a+a}{a}, 1-p \\ \frac{a+1+j}{a}, \frac{a+2+j}{a}, \frac{a+3+j}{a}, \ldots, \frac{a+a+j}{a} \end{array} \middle| -t\right]$$

The following remark claims a convexity and log convexity property for the series $\frac{1}{j} S(a,j,p,t,1)$ by the use of its integral representation (2.8).

Remark 1. *For $a \geq 1$, $p \geq 1$, $t > 0, r \geq 0$ and $j > 0$, the function $a \mapsto \frac{1}{j} S(a,j,p,t,1)$ as given in Theorem 4 is strictly decreasing and convex with respect to the parameter $a \in [1,\infty)$ for every $x \in [0,1]$, it is also log convex.*

As in the proofs of Theorems 2 and 3 we can outline the following steps. From (2.8), let

$$G(x,a) = pt(1-x)^{j-1} x^a (1+tx^a)^{p-1} \tag{2.9}$$

be an integrable function for $x \in [0,1]$ and put

$$F(a) = \int_0^1 G(x,a)\,dx,$$

applying the Leibniz rule for differentiation under the integral sign and using (2.8), we obtain

$$F'(a) = pt\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-2}(1+ptx^a)\ln(x)\,dx < 0, \tag{2.10}$$

and

$$F''(a) = pt\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-3}\left(1+(3p-1)tx^a+(ptx^a)^2\right)(\ln(x))^2\,dx > 0, \tag{2.11}$$

since $p \geq 1$, so that (2.7) is a monotonic decreasing function for every $x \in [0,1]$.

Similarly, if we let

$$H(a) = \log\left(\int_0^1 G(x,a)\,dx\right),$$

$$H'(a) = \frac{\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-2}(1+ptx^a)\ln(x)\,dx}{\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-1}\,dx} < 0,$$

and we require that

$$H''(a) = \frac{\left(\int_0^1 \frac{\partial^2}{\partial^2 a}G(x,a)\,dx\right)\left(\int_0^1 G(x,a)\,dx\right) - \left(\int_0^1 \frac{\partial}{\partial a}G(x,a)\,dx\right)^2}{\left(\int_0^1 G(x,a)\,dx\right)^2} > 0,$$

where $G(x,a)$ is given by (2.9), $\int_0^1 \frac{\partial}{\partial a}G(x,a)\,dx$ is given by (2.10) and $\int_0^1 \frac{\partial^2}{\partial^2 a}G(x,a)\,dx$ is given by (2.11). It is sufficient to investigate

$$\begin{aligned}\left(\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-3}\left(1+(3p-1)tx^a+(ptx^a)^2\right)(\ln(x))^2\,dx\right) \\ \times\left(\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-1}\,dx\right) \\ > \left(\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-2}(1+ptx^a)\ln(x)\,dx\right)^2.\end{aligned} \tag{2.12}$$

Now since

$$\begin{aligned}&\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-3}\left(1+(3p-1)tx^a+(ptx^a)^2\right)(\ln(x))^2\,dx \\ >\ &\int_0^1 (1-x)^{j-1} x^a (1+tx^a)^{p-1}\left(\frac{(1+ptx^a)\ln(x)}{1+tx^a}\right)^2 dx,\end{aligned}$$

if we identify

$$p(x) = (1-x)^{j-1} x^a (1+tx^a)^{p-1}, \quad q(x) = \frac{(1+ptx^a)\ln x}{1+tx^a},$$

and $r(x) = 1$ and applying the Cauchy-Buniakowsky-Schwarz inequality we conclude that (2.12) is satisfied, hence (2.7) is log convex with respect to the parameter a for every $x \in [0,1]$.

We make the following observation.

For an integer $a \geq 1$, $p \geq 1$, $t > 0$, and $j > 0$,

(2.13)
$$\sum_{n=1}^{p} \frac{t^n n\binom{p}{n}}{\binom{an+j}{j}} = \frac{pt}{j\binom{a+j}{j}}\, {}_{a+1}F_a\left[\begin{array}{c} \frac{a+1}{a}, \frac{a+2}{a}, \frac{a+3}{a}, \ldots, \frac{a+a}{a}, 1-p \\ \frac{a+1+j}{a}, \frac{a+2+j}{a}, \frac{a+3+j}{a}, \ldots, \frac{a+a+j}{a} \end{array} \middle| -t \right].$$

Hence we make the claim that the generalised hypergeometric function in (2.13) is a log convex function with respect to the parameter $a \geq 1$.

3. Conclusion

We have demonstrated convexity and log convexity properties for a class of series involving ratios of binomial coefficients.

References

[1] Amghibech, S., On sums involving binomial coefficients, *Journal of Integer Sequences* **10**, 2007, article 07.2.1.

[2] Batir, N., On the series $\sum_{k=1}^{\infty} k^{-n} x^k$. *Proc. Indian Acad. Sci.* (Math. Sci.) **115**(4), 2005, 371-381.

[3] Kazarinoff, N.D., *Analytic Inequalities*, Dover Publications, New York, 2003.

[4] Purkait, S. and Sury, B., Some vanishing sums involving binomial coefficients in the denominator. *Albanian Journal of Mathematics* **2**(1), 2008, 27-32.

[5] Sofo, A., Sums of binomial coefficients in integral form, *Accepted Fibonacci Quarterly*, 2007

[6] Sofo, A., General properties involving reciprocals of binomial coefficients, *Journal of Integer Sequences* **9**, 2006, article 06.4.5.

[7] Sofo, A., *Computational Techniques for the Summation of Series*, Kluwer Academic/Plenum Publishers, 2003.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 49–53
ISSN 1930-1235: (2009)

FULLY INVARIANT τ_M-LIFTING MODULES

Y. Talebi and T. Amoozegar

Department of Mathematics,
Faculty of Science,
University of Mazandaran, Babolsar, Iran
talebi@umz.ac.ir
t.amoozegar@umz.ac.ir

Abstract. Let τ_M be any preradical for $\sigma[M]$ and N any module in $\sigma[M]$. A module N is called *τ_M-lifting* if for every submodule K of N, there is a decomposition $K = A \oplus B$, such that A is a direct summand of N and $B \subseteq \tau_M(N)$. We call N is *(strongly) FI-τ_M-lifting* if for every fully invariant submodule K of N, there is a decomposition $K = A \oplus B$, such that A is a (fully invariant) direct summand of N and $B \subseteq \tau_M(N)$. The class of FI-τ_M-lifting modules properly contains the class of τ_M-lifting modules and the class of strongly FI-τ_M-lifting modules. In this paper we investigate whether the class of (strongly) FI-τ_M-lifting modules are closed under particular class of submodules, direct summands and direct sums.

1. Introduction

Throughout this paper R will denote an arbitrary associative ring with identity and all modules will be unitary right R-modules. Let $M \in$ Mod-R. By $\sigma[M]$ we mean the full subcategory of Mod-R whose objects are submodules of M-generated modules. For any module M, τ_M will denote a preradical in $\sigma[M]$. We say that A is a *τ_M-coessential submodule of B in N* if $B/A \subseteq \tau_M(N/A)$. Like in [2], a submodule $K \subseteq N$ is called τ_M-supplement (weak τ_M-supplement) provided there exists some $U \subseteq N$ such that $U + K = N$ and $U \cap K \subseteq \tau_M(K)(U \cap K \subseteq \tau_M(N))$. M is called *τ_M-supplemented* (*weakly τ_M-supplemented*) if each of its submodules has a τ_M-supplement (weak τ_M-supplement) in M. M is called *amply τ_M-supplemented*, if for all submodules K and L of N with $K + L = N$, K contains a τ_M-supplement of L in N. A submodule A of N is said to be *τ_M-coclosed in N* if it has no proper τ_M-coessential submodule in N. According to [2] and [12], a module N is called *τ_M-lifting* if for every submodule K of N, there is a decomposition $K = A \oplus B$, such that A is a direct summand of N and $B \subseteq \tau_M(N)$. Recall that a submodule K of M is called *fully invariant* (denoted by $K \trianglelefteq M$) if $\lambda(K) \subseteq K$ for all $\lambda \in End_R(M)$.

We mainly study (strongly) FI-τ_M-lifting modules in $\sigma[M]$ in this paper. We call N is *(strongly) FI-τ_M-lifting* if for every fully invariant submodule K of N, there

1991 *Mathematics Subject Classification.* 16D90, 16D99.
Key words and phrases. τ_M-Supplement submodules, τ_M-Lifting modules, FI-τ_M-lifting modules.

is a decomposition $K = A \oplus B$, such that A is a (fully invariant) direct summand of N and $B \subseteq \tau_M(N)$. In Section 1, we show that FI-τ_M-lifting modules are closed under finite direct sums. We prove that if module R_R is FI-τ_M-lifting then R/I has a projective τ_M-cover for every two sided ideal I of R. In Section 2, We show that a direct summand of a strongly FI-τ_M-lifting module is strongly FI-τ_M-lifting and that a finite direct sum of copies of a strongly FI-τ_M-lifting module is strongly FI-τ_M-lifting.

2. FI-τ_M-Lifting Modules

Lemma 2.1. *Let X be a τ_M-supplement submodule of N and $K \subseteq X$. Then X/K is a τ_M-supplement submodule of N/K.*

Proof. See [4, 10.12(3)]. □

Lemma 2.2. *Let M be a module. Then:*

1. *Any sum or intersection of fully invariant submodules of M is again a fully invariant submodule of M (in fact the fully invariant submodules form a complete modular sublattice of the lattice of submodules of M).*
2. *If $X \subseteq Y \subseteq M$ such that Y is a fully invariant submodule of M and X is a fully invariant submodule of Y, then X is a fully invariant submodule of M.*
3. *If $M = \bigoplus_{i\in I} X_i$ and S is a fully invariant submodule of M, then $S = \bigoplus_{i\in I} \pi_i(S) = \bigoplus_{i\in I}(X_i \cap S)$, where π_i is the i-th projection homomorphism of M.*
4. *If $X \subseteq Y \subseteq M$ such that X is a fully invariant submodule of M and Y/X is a fully invariant submodule of M/X, then Y is a fully invariant submodule of M.*

Proof. (1), (2), (3) See [3, Lemma 1.1]. (4) Let $f : M \to M$ be a homomorphism. Then $f(X) \subseteq X$. Now, consider the homomorphism $g : M/X \to M/X$ defined by $g(m + X) = f(m) + X, (m \in M)$. Then $g(Y/X) \subseteq Y/X$. Clearly, $g(Y/X) = (f(Y) + X)/X$. Therefore $f(Y) \subseteq Y$.

□

We note that if $M = \bigoplus_{i=1}^{n} M_i$ and N is a fully invariant submodule of M, then $N = \bigoplus_{i=1}^{n}(N \cap M_i)$ and $N \cap M_i$ is a fully invariant submodule of M_i.

Lemma 2.3. *Let $N \in \sigma[M]$. The following are equivalent:*

1. *For every submodule K of N, there is a decomposition $K = A \oplus B$, such that A is a direct summand of N and $B \subseteq \tau_M(N)$;*
2. *For every submodule K of N,there is a direct summand A of N such that $A \subseteq K$ and $K/A \subseteq \tau_M(N/A)$;*
3. *For every submodule K of N, there is a decomposition $N = A \oplus B$ such that $A \subseteq K$ and $B \cap K \subseteq \tau_M(N)$.*

Proof. See [12, Lemma 3.1]. □

A module $N \in \sigma[M]$ is called *τ_M-lifting* if it satisfies one of the equivalent conditions of Lemma 2.3.

Proposition 2.4. *Let $N \in \sigma[M]$. The following are equivalent:*

(1) *For every fully invariant submodule K of N, there is a decomposition $K = A \oplus B$, such that A is a direct summand of N and $B \subseteq \tau_M(N)$;*
(2) *For every fully invariant submodule K of N,there is a direct summand A of N such that $A \subseteq K$ and $K/A \subseteq \tau_M(N/A)$.*
(3) *For every fully invariant submodule K of N, there is a decomposition $N = A \oplus B$ such that $A \subseteq K$ and $B \cap K \subseteq \tau_M(N)$.*

Proof. (1) $\Rightarrow$ (2) Let K be a fully invariant submodule of N. By hypothesis, there exists a direct summand A of N and $B \subseteq \tau_M(N)$ such that $K = A \oplus B$. Now $N = A \oplus A'$ for some submodule A' of N. Consider the natural epimorphism $\pi : N \to N/A$. Then $\pi(B) = (B + A)/A = K/A \subseteq \tau_M(N/A)$. Therefore N is FI-τ_M-lifting module.

(2) $\Rightarrow$ (3) By [12, Lemma 3.1].

(3) $\Rightarrow$ (1) Let K be a fully invariant submodule of N. By hypothesis, there is a decomposition $N = A \oplus B$ such that $A \subseteq K$ and $B \cap K \subseteq \tau_M(N)$. Therefore $K = A \oplus (K \cap B)$, as required.

□

A module $N \in \sigma[M]$ is called *τ_M-FI-lifting* if it satisfies one of the equivalent conditions of Proposition 2.4.

Theorem 2.5. *Let $N = \bigoplus_{i=1}^{n} N_i$ be a direct sum of τ_M-FI-lifting modules. Then N is τ_M-FI-lifting.*

Proof. Let $K \trianglelefteq N$. Then $K = \bigoplus_{i=1}^{n}(K \cap N_i)$ and $K \cap N_i$ is a fully invariant submodule of N_i. As each N_i is τ_M-FI-lifting we have $K \cap N_i = A_i \oplus B_i$ where A_i is a direct summand of N_i and $B_i \subseteq \tau_M(N_i)$. Put $A = \bigoplus_{i=1}^{n} A_i$ and $B = \bigoplus_{i=1}^{n} B_i$. Then $K = A \oplus B$ where A is a direct summand of N and $B = \bigoplus_{i=1}^{n} B_i \subseteq \bigoplus_{i=1}^{n} \tau_M(N_i) = \tau_M(\bigoplus_{i=1}^{n} N_i) = \tau_M(N)$. □

Corollary 2.6. *If N is a finite direct sum of τ_M-lifting modules, then N is τ_M-FI-lifting.*

Let $N \in \sigma[M]$. We call an epimorphism $f : P \to N$ a projective τ_M-cover of N in $\sigma[M]$ if P is projective in $\sigma[M]$ and $Ker(f) \subseteq \tau_M(P)$.

Theorem 2.7. *Let P be a projective module. If P is FI-lifting then P/A has a projective τ_M-cover for every fully invariant submodule A of P.*

Proof. Suppose P is a projective FI-lifting module and A is a fully invariant submodule of P. Then $A = X \oplus S$ where X is a direct summand of P and $S \subseteq \tau_M(P)$. Suppose $P = X \oplus Y$. As $S \subseteq \tau_M(P)$, $(X + S)/X \subseteq (X + \tau_M(P))/X \subseteq \tau_M(P/X)$. Hence the natural map $f : P/X \to P/(X + S) = P/A$ is a projective τ_M-cover. □

Corollary 2.8. *Suppose R is a ring. If module R_R is FI-τ_M-lifting then R/I has a projective τ_M-cover for every two sided ideal I of R.*

Proposition 2.9. *Let N be a FI-τ_M-lifting module. Then every fully invariant submodule of $N/\tau_M(N)$ is a direct summand.*

Proof. Let $K/\tau_M(N)$ be a fully invariant submodule of $N/\tau_M(N)$. Then K is fully invariant submodule by Lemma 2.2. By hypothesis, there is a decomposition $N = N_1 \oplus N_2$ such that $N_1 \subseteq K$ and $K \cap N_2 \subseteq \tau_M(N)$. Thus $N/\tau_M(N) = (K/\tau_M(N)) \oplus ((N_2 + \tau_M(N))/\tau_M(N))$, as required.

□

3. Strongly FI-τ_M-lifting Modules

In this section we define strongly FI-τ_M-lifting modules. This class of modules is properly contained in the class of FI-τ_M-lifting modules; but there is no containment relation between the class of strongly FI-τ_M-lifting modules and the class of lifting modules. We show that a direct summand of a strongly FI-τ_M-lifting module is strongly FI-τ_M-lifting and that a finite direct sum of copies of a strongly FI-τ_M-lifting module is strongly FI-τ_M-lifting.

As in Proposition 2.4 we can prove the following.

Proposition 3.1. *Let $N \in \sigma[M]$. The following are equivalent:*

(1) *For every fully invariant submodule K of N, there is a decomposition $K = A \oplus B$, such that A is a fully invariant direct summand of N and $B \subseteq \tau_M(N)$;*
(2) *For every fully invariant submodule K of N,there is a fully invariant direct summand A of N such that $A \subseteq K$ and $K/A \subseteq \tau_M(N/A)$.*

A module $N \in \sigma[M]$is called *strongly FI-τ_M-lifting* if it satisfies one of the equivalent conditions of Proposition 3.1.

Proposition 3.2. *Let N be an FI-τ_M-lifting with $\tau_M(N) = 0$. Then every fully invariant submodule (in particular N) is strongly FI-τ_M-lifting module.*

Proof. Let K be a fully invariant submodule of N. Suppose A is fully invariant in K. Then A is fully invariant in N also (see Lemma 2.2). As N is FI-τ_M-lifting, $A = B \oplus S$ where B is a direct summand of N and $S \subseteq \tau_M(N)$ (see Proposition 2.4). Since $\tau_M(N) = 0$, $S = 0$ and so A is a direct summand of N and hence of K. Thus K is strongly FI-lifting. □

Theorem 3.3. *A direct summand of a strongly FI-τ_M-lifting module is strongly FI-τ_M-lifting.*

Proof. Let $N = X \oplus Y$ be a strongly FI-τ_M-lifting module. Assume that $S_1 \trianglelefteq X$. Then there exists $S_2 \trianglelefteq Y$ such that $S_1 \oplus S_2 \trianglelefteq M$ [5, Lemma 1.11]. Since N is a strongly FI-τ_M-lifting, $S_1 \oplus S_2 = B \oplus S$ where $S \subseteq \tau_M(N)$ and B is a fully invariant direct summand of N. But $B \trianglelefteq N$ implies that $B = (X \cap B) \oplus (Y \cap B)$ and $X \cap B$ is fully invariant in X. Also $X \cap B$ is a direct summand of N. We have $S_1 = \pi_X(B) + \pi_X(S) = (X \cap B) + \pi_X(S)$ where $\pi_X : N \to X$ is the projection along Y. As $S \subseteq \tau_M(N), \pi_X(S) \subseteq \tau_M(X)$. By Proposition 3.1, X is a strongly FI-τ_M-lifting module. □

Proposition 3.4. *Let $N = \bigoplus_{i=1}^{n} N_i$ and let $N_i \trianglelefteq M$ for all $1 \leq i \leq n$. Then N is strongly FI-τ_M-lifting if and only if N_i is strongly FI-τ_M-lifting, for all $1 \leq i \leq n$.*

Proof. If N is strongly FI-τ_M-lifting then each N_i is so, by Proposition 3.4.

Conversely, suppose $N = \bigoplus_{i=1}^{n} N_i$ where each N_i is strongly FI-τ_M-lifting and fully invariant in N. Let $K \trianglelefteq N$. Then $K = \bigoplus_{i=1}^{n}(K \cap N_i)$ and $(K \cap N_i) \trianglelefteq N_i$, for all $1 \leq i \leq n$. As N_i is strongly FI-τ_M-lifting, $K \cap N_i = B_i \oplus S_i$ where B_i is a fully invariant direct summand of N_i and $S_i \subseteq \tau_M(N_i)$ (see Proposition 3.1). Put $B = \bigoplus_{i=1}^{n} B_i$ and $S = \bigoplus_{i=1}^{n} S_i$. Then $K = B \oplus S$ where B is a direct summand of N and $S \subseteq \tau_M(N)$. As $B_i \trianglelefteq N_i$ and $N_i \trianglelefteq N$, $B_i \trianglelefteq N$ for all $1 \leq i \leq n$. Hence $B \trianglelefteq N$. Therefore N is strongly FI-τ_M-lifting. □

Theorem 3.5. *Suppose K is a strongly FI-τ_M-lifting module and $N = \bigoplus_{i=1}^{n} N_i$ where each $N_i \simeq K$. Then N is a strongly FI-τ_M-lifting module.*

Proof. There exist isomorphisms $f_i : N_1 \to N_i$ for $i = 2, \cdots, n$. If A is a fully invariant submodule of N, then it is easy to see that $A = A_1 \oplus f_2(A_1) \oplus \cdots \oplus f_n(A_1)$ where $A_1 = N_1 \cap A$.

As N_1 is strongly FI-τ_M-Lifting and A_1 is a fully invariant submodule of N_1, we have $A_1 = L_1 \oplus S_1$ where L_1 is a fully invariant submodule of N_1 and $S_1 \subseteq \tau_M(M_1)$ (see Proposition 3.1). Put $L := L_1 \oplus f_2(L_1) \oplus \cdots \oplus f_n(L_1)$ and $S := S_1 \oplus f_2(S_1) \oplus \cdots \oplus f_n(S_1)$. Then $A = L \oplus S$, L is a fully invariant direct summand of N and $S \subseteq \tau_M(N)$. Hence N is strongly FI-τ_M-lifting. □

From Proposition 3.3 and Theorem 3.5 we get the following.

Corollary 3.6. *Suppose R is a ring and R_R is strongly FI-τ_M-lifting. Then any finitely generated projective R-module is strongly FI-τ_M-lifting.*

Proposition 3.7. *Let N be a strongly FI-τ_M-lifting module and X a fully invariant submodule of N. If X is indecomposable, then X is strongly FI-τ_M-lifting.*

Proof. Let $K \trianglelefteq X$ then $K \trianglelefteq N$. Since N is strongly FI-τ_M-lifting module, $K = B \oplus S$ where $S \subseteq \tau_M(N)$ and B is a fully invariant direct summand of N. Hence $N = B \oplus C$ for some submodule C of N. Since $X \trianglelefteq N$, then $X = B \oplus (C \cap X)$. But X is indecomposable, therefore $X = B$ and X is direct summand of N. By Theorem 3.3, X is strongly FI-τ_M-lifting. □

References

[1] F.W. Anderson, K.R. Fuller: Rings and Categories of Modules Springer-Verlog, New York, 1992.

[2] K. Al-Takhman, C. Lomp and R. Wisbaure, *τ-complemented and τ-supplemented modules*, Algebra and Discrete Mathematics, 3(2006), 1-15.

[3] G.F. Birkenmeier, B.J. Muller, S.T. Rizvi: *Modules in which every fully invariant submodule is essential in a direct summand*, Comm. Algebra, 30(2002), 1395-1415.

[4] J. Clark, C. Lomp, N. Vanaja, R. Wisbauer: Lifting Modules, Frontiers in Mathematics, Birkäuser Verlag, 2006.

[5] S. T. Rizvi, S. R. Cosmin: *Baer and Quasi-Baer Modules*, Comm. Algebra, 32(2004), 103-123.

[6] A. Facchini, L. Salce: *Uniserial modules: Sums and isomorphism of subquotients*, Comm Algebra, 18(1990), 499-517.

[7] D. Keskin: *On Lifting Modules*, Comm. Algebra, 28(2000), 3427-3440.

[8] C. Lomp: On Dual Goldie Dimension, Diplomarbeit (M.Sc. Thesis), University of Düsseldorf, Germany, 1996.

[9] S.M. Mohamed, B. J. Muller: Continuous and Discrete Modules, London Math. Soc. Lecture Notes Series 147, Cambridge, University Press, 1990.

[10] Y. Talebi, N. Vanaja: *The Torsion Theory Cogenerated by M-small Modules*, Comm. Algebra, 30(2002), 1449-1460.

[11] Y. Talebi, T. Amoozegar: *Strongly FI-Lifting Modules*, International Electronic J. of Algebra, 3(2008), 75-82.

[12] R. Tribak and D. Keskin: *On $\overline{Z}_M$-Semiperfect Modules*, East-West. J. of Mathematicals, 8(2006), 193-203.

[13] R. Wisbauer: Foundations of module and ring theory, Gordon and Breach, Reading, 1991.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 2, Pages 57–61
ISSN 1930-1235: (2009)

AUTOMORPHISMS AND DERIVATIONS ON THE CENTER OF A RING

V.K.Bhat

School of Mathematics,
SMVD University,
P/o Kakryal, Katra, J and K,
India- 182320
vijaykumarbhat2000@yahoo.com

Abstract. Let R be a ring, σ_1 an automorphism of R and δ_1 a σ_1-derivation of R. Let σ_2 be an automorphism of $O_1(R) = R[x; \sigma_1, \delta_1]$, and δ_2 be a σ_2-derivation of $O_1(R)$. Let $S \subseteq Z(O_1(R))$, the center of $O_1(R)$. Then it is proved that σ_i is identity when restricted to S, and δ_i is zero when restricted to S; $i = 1, 2$. The result is proved for iterated extensions also.

1. Introduction

A ring R means an associative ring with identity $1 \neq 0$. $Z(R)$ denotes the center of R. The set of positive integers is denoted by $\mathbb{N}$. Let A be a nonempty set and $\alpha : A \to A$ be a map and $B \subseteq A$. Then $\alpha \mid B$ means α restricted to B.

In this paper we investigate the nature of an automorphism σ and a σ-derivation δ of a ring R, when restricted to the center of R.

Recall that a σ-derivation of R is an additive map $\delta : R \to R$ such that

$$\delta(ab) = \delta(a)\sigma(b) + a\delta(b), \text{ for all } a, b \in R.$$

Let σ be an endomorphism of a ring R and $\delta : R \to R$ any map.
Let $\phi : R \to M_2(R)$ be a homomorphism defined by

$$\phi(r) = \begin{pmatrix} \sigma(r) & 0 \\ \delta(r) & r \end{pmatrix}, \text{ for all } r \in R.$$

Then δ is a σ-derivation of R.

In case σ is the identity map, δ is called just a derivation of R. For example let F be a field and $R = F[x]$. Then the formal derivative $\frac{d}{dx}$ is a derivation of R.

Recall that the Ore extension $R[x; \sigma, \delta] = \{f = \sum_{i=0}^{n} x^i a_i,\ a_i \in R,\ n \in \mathbb{N}\}$, subject to the relation $ax = x\sigma(a) + \delta(a)$ for all $a \in R$. We take coefficients on the right as followed in McConnell and Robson [13]. Some authors take coefficients on the left as in Goodearl and Warfield [7]. We denote the Extension ring $R[x; \sigma, \delta]$ by $O_1(R)$. In case σ is the identity map, we denote $R[x; \delta]$ by $D_1(R)$ and in case δ is the zero map, we denote $R[x; \sigma]$ by $S_1(R)$.

1991 *Mathematics Subject Classification.* 16-XX; Secondary 16S36,16P40,16P50,16U20.
Key words and phrases. Center; automorphism; σ-derivation; ore extension.

We also recall that the skew-Laurent extension $R[x, x^{-1}; \sigma] = \{\sum_{i=-m}^{n} x^i a_i$, $a_i \in R$; m, $n \in \mathbb{N}\}$, where multiplication is subject to the relation $ax = x\sigma(a)$ for all $a \in R$.

The rings that we deal with are the above mentioned rings and their iterations as given below:

(1) $S_t(R) = R[x_1; \sigma_1][x_2; \sigma_2]...[x_t; \sigma_t]$, the iterated skew-polynomial ring, where each σ_i is an automorphism of $S_{i-1}(R)$.
(2) $L_t(R) = R[x_1, x_i^{-1}; \sigma_1][x_2, x_2^{-1}; \sigma_2]...[x_t, x_t^{-1}; \sigma_t]$, the iterated skew-Laurent polynomial ring, where each σ_i is an automorphism of $L_{i-1}(R)$.
(3) $D_t(R) = R[x_1; \delta_1][x_2; \delta_2]...[x_t; \delta_t]$, the iterated differential operator ring, where each δ_i is a derivation of $D_{i-1}(R)$.
(4) $O_t(R) = R[x_1; \sigma_1, \delta_1][x_2; \sigma_2, \delta_2]...[x_t; \sigma_t, \delta_t]$, the iterated Ore extension, where σ_i is an automorphism of $O_{i-1}(R)$ and δ_i is a σ_i-derivation of $O_{i-1}(R)$.

We note that if σ is an automorphism of a ring R and δ is a σ-derivation of R, then σ can be extended to an automorphism of $R[x; \sigma, \delta]$ by taking $\sigma(x) = x$, i.e. $\sigma(xa) = x\sigma(a)$, for all $a \in R$. Also δ can be extended to a σ-derivation of $R[x; \sigma, \delta]$ by taking $\delta(x) = 0$, i.e. $\delta(xa) = x\delta(a)$, for all $a \in R$.

In view of this, we note that each σ_i is an automorphism of $S_t(R)$ and $O_t(R)$. Also each δ_i is a derivation (respectively σ-derivation) of $D_t(R)$ (respectively $O_t(R)$).

2. Automorphisms and derivations

We prove the following:

(1) Let $L \subseteq Z(K_t(R))$, where $K_t(R)$ is any of $S_t(R)$ or $L_t(R)$. Then $\sigma_i \mid L$ is the identity map; for all i, $1 \leq i \leq t$.
(2) Let $T \subseteq Z(D_t(R))$, where R is an integral domain. Then $\delta_i \mid T$ is the zero map; for all i, $1 \leq i \leq t$.
(3) Let $S \subseteq Z(O_t(R))$. Then $\delta_i \mid S$ is the identity map, and $\delta_i \mid S$ is the zero map; for all i, $1 \leq i \leq t$.

For more details on Ore extensions, and the basic results, the reader is referred to chapters (1) and (2) of [7]. Ore-extensions including skew-polynomial rings and differential operator rings have been of interest to many authors. For example [1, 5, 7, 8, 9, 10, 11].

Prime ideals (in particular minimal prime ideals and associated prime ideals) of these extensions have been characterized in [1, 4, 6, 14].

Recall that a ring R is said to be 2-primal if the prime radical (i.e. the intersection of prime ideals of R) coincides with the set of all nilpotent elements of R. This property has been discussed in [2, 3, 12].

We begin with the following Proposition:

Proposition 2.1. *Let R be a ring σ be an automorphism of R. Then $\sigma \mid Z(R)$ is an automorphism.*

Proof. It is enough to show that $a \in Z(R)$ implies that $\sigma(a) \in Z(R)$. Let $a \in Z(R)$ and $r \in R$. Then $\sigma(a)r = \sigma(a\sigma^{-1}(r)) = \sigma(\sigma^{-1}(r)a) = r\sigma(a)$ Therefore, $\sigma(a) \in Z(R)$. □

We now have the following proposition which is used to prove Proposition (2.5) and Theorem (2.6).

Proposition 2.2. *Let R be an integral domain. Then $O_1(R)$ is an integral domain.*

Proof. The proof is easy. We give a sketch. Let f, $g \in O_1(R)$ be such that $fg = 0$. Say $f = \sum_{i=0}^{n} x^i a_i$, and $g = \sum_{i=0}^{m} x^i b_i$, m, $n \in \mathbb{N}$. Suppose that $g \neq 0$.

To prove the result, we use induction on m, n. For $m = n = 0$, the result is trivial. For $m = n = 1$, we have $f = xa_1 + a_0$ and $g = xb_1 + b_0$. Now $fg = 0$ implies that

$$x[x\sigma(a_1) + \delta(a_1)]b_1 + [x\sigma(a_0) + \delta(a_0)]b_1 + xa_1b_0 + a_0b_0 = 0;$$

i.e.

$$x^2\sigma(a_1)b_1 + x\delta(a_1)b_1 + x\sigma(a_0)b_1 + xa_1b_0 + \delta(a_0)b_1 + a_0b_0 = 0,$$

and so we have $\sigma(a_1)b_1 = 0$, $\delta(a_1)b_1 + \sigma(a_0)b_1 + a_0b_0 = 0$, $\delta(a_0)b_1 + a_0b_0 = 0$. Now $g \neq 0$. Therefore, there are three possibilities:

(1) $b_1 \neq 0$, $b_0 \neq 0$. In this case $\sigma(a_1)b_1 = 0$ implies that $\sigma(a_1) = 0$; i.e. $a_1 = 0$. Now $\delta(a_1)b_1 + \sigma(a_0)b_1 + a_1b_0 = 0$ implies that $\sigma(a_0)b_1 = 0$. Therefore $\sigma(a_0) = 0$; i.e. $a_0 = 0$. Thus $f = 0$.
(2) $b_1 \neq 0$, $b_0 = 0$. This could be treated similarly as above.
(3) $b_1 = 0$, $b_0 \neq 0$. In this case $\delta(a_1)b_1 + \sigma(a_0)b_1 + a_1b_0 = 0$ implies that $a_1b_0 = 0$, and therefore, $a_1 = 0$. Also $\delta(a_0)b_1 + a_0b_0 = 0$ implies that $a_0b_0 = 0$, and so $a_0 = 0$. Thus $f = 0$. So, in all cases we have $f = 0$.

Therefore, the result is true for $m = n = 1$. Suppose the result is true for $m = k$ and $n = 1$. We shall prove for $m = k + 1$. Now for $m = k + 1$ and $n = 1$, $fg = 0$ implies that

$$(x^{k+1}a_{k+1} + x^k a_k + ... + a_0)(xb_1 + b_0) = 0,$$

i.e.

$$x^{k+2}\sigma(a_{k+1})b_1 + x^{k+1}\delta(a_{k+1})b_1 + x^{k+1}\sigma(a_k)b_1 + x^{k+1}a_{k+1}b_0 + ...+$$
$$x\sigma(a_0)b_1 + \delta(a_0)b_1 + a_0b_0 = 0.$$

Now for $g \neq 0$, there are three possibilities:

(1) $b_1 \neq 0$, $b_0 \neq 0$. In this case $\sigma(a_{k+1})b_1 = 0$ implies that $\sigma(a_{k+1}) = 0$; i.e. $a_{k+1} = 0$. Therefore $fg = 0$ reduces to $(x^k a_k + x^{k-1}a_{k-1} + ... + a_0)(xb_1 + b_0) = 0$, and induction hypothesis implies that $f = 0$.
(2) $b_1 \neq 0$, $b_0 = 0$. This could be treated similarly as above.
(3) $b_1 = 0$, $b_0 \neq 0$. In this case $\delta(a_{k+1})b_1 + \sigma(a_k)b_1 + a_{k+1}b_0 = 0$ implies that $a_{k+1}b_0 = 0$, and therefore, $a_{k+1} = 0$. Therefore $fg = 0$ reduces to $(x^k a_k + x^{k-1}a_{k-1} + ... + a_0)(xb_1 + b_0) = 0$, and induction hypothesis implies that $f = 0$.

Therefore, in all the cases $f = 0$. In a similar way the result could be proved for higher degrees of g. Hence $O_1(R)$ is an integral domain. □

Proposition 2.3. *Let R be a ring and consider $S_t(R)$. Let $L \subseteq S_t(R)$. Then $\sigma_i \mid L$ is the identity map for all i, $1 \leq i \leq t$.*

Proof. Consider $S_1(R)$ and its automorphism σ_2. Let $a \in L$. Now $af_1 = f_1a$ for all $f_1 = \sum_{i=0}^{n} x_1^i b_i \in S_1(R)$, $n \in \mathbb{N}$,

$$a(x_1^n b_n + ... + b_0) = (x_1^n b_n + ... + b_0)a.$$

So we have

$$(x_1^n\sigma_1^n(a)b_n + ... + x_1\sigma_1(a)b_1 + ab_0 = (x_1^n b_n a + ... + x_1 b_1 a + b_0 a).$$

Therefore $\sigma_1(a) = a$.

Now consider $S_2(R)$ and its automorphism σ_3. Let $a \in L$. Then $af_2 = f_2a$ for all $f_2 \in S_2(R)$. Let $f_2 = x_2^k f_k + ... + x_2 f_1 + f_0$, where $f_i \in S_1(R)$. Then $af_2 = f_2a$ implies that

$$a(x_2^k f_k + ... + x_2 f_1 + f_0) = (x_2^k f_k + ... + x_2 f_1 + f_0)a;$$

i.e.

$$x_2^k\sigma_2^k(a)f_k + ... + x_2\sigma_2(a)f_1 + af_0 = x_2^k f_k a + ... + x_2 f_1 a + f_0 a.$$

Therefore, $\sigma_2(a)f_1 = f_1a = af_1$ as $a \in Z(S_2(R))$. Hence $\sigma_2(a) = a$. With the same process, we can see that $\sigma_i \mid L$ is the identity map for all i, $1 \leq i \leq t$. □

Remark 2.4. The above result holds if $S_t(R)$ is replaced by $L_t(R)$, and the proof follows on the same lines.

Proposition 2.5. *Let R be an integral domain and consider $D_t(R)$. If $T \subseteq Z(D_t(R))$. Then $\delta_i \mid T$ is the zero map, for all i, $1 \leq i \leq t$.*

Proof. Let $a \in T$. Consider $D_1(R)$. Let $f_1 = x_1b + c$, $b \neq 0$. Then $af_1 = f_1a$; i.e. $a(x_1 1b + c) = (x_1b + c)a$, which implies that

$$x_1ab + \delta_1(a)b + ac = x_1ba + ca.$$

Now $a \in Z(D_1(R))$ implies that $\delta_1(a)b + ac = ca = ac$, and $\delta_1(a)b = 0$. Thus $\delta_1(a) = 0$. Polynomials of higher degree could be treated in a similar way.

Now consider $D_2(R)$. Let $f_2 = x_2g_1 + g_0$, where $g_1 \neq 0$; g_1, $g_0 \in D_1(R)$. Then $af_2 = f_2a$ implies that

$$a(x_2g_1 + g_0) = (x_2g_1 + g_0)a,$$

or,

$$x_2ag_1 + \delta_2(a)g_1 + ag_0 = x_2g_1a + g_0a.$$

Now a $\in Z(D_2(R))$ implies that

$$\delta_2(a)g_1 + ag_0 = g_0a = ag_0.$$

Therefore $\delta_2(a)g_1 = 0$, and so Proposition (2.2) implies that $\delta_2(a) = 0$. With the same process it can be shown that $\delta_i \mid T$ is the zero map, for all i, $1 \leq i \leq t$. □

Theorem 2.6. *Let R be an integral domain and consider $O_t(R)$. If $S \subseteq Z(O_t(R))$, then $\sigma_i \mid S$ is the identity map and $\delta_i \mid S$ is the zero map, for all i, $1 \leq i \leq t$.*

Proof. Let $a \in S$. Let $f_1 = x_1b + c \in O_1(R)$, $b \neq 0$. Then $af_1 = f_1a$, and we have $a(x_1b + c) = (x_1b + c)a$, which implies that

$$x_1\sigma_1(a)b + \delta_1(a)b + ac = x_1ba + ca.$$

Therefore $\sigma_1(a)b = ba = ab$ as $a \in Z(O_t(R))$. So we have $\sigma_1(a) = a$. Also, $\delta_1(a)b + ac = ca = ac$. Thus $\delta_1(a)b = 0$, and so $\delta_1(a) = 0$. Polynomials of higher degree can be treated similarly.

Now let $f_2 = x_2g_1 + g_0 \in O_2(R)$, $g_1 \neq 0$. Then $af_2 = f_2a$ implies that

$$a(x_2g_1 + g_0) = (x_2g_1 + g_0)a.$$

Therefore

$$x_2\sigma_2(a)g_1 + \delta_2(a)g_1 + ag_0 = x_2g_1a + g_0a$$

Now $a \in Z(O_t(R))$ implies that

$$x_2\sigma_2(a)g_1 = g_1a + ag_1.$$

Thus $\sigma_2(a) = a$. Also $\delta_2(a)g_1 + ag_0 = g_0a = ag_0$ as $a \in Z(O_t(R))$. Therefore $\delta_2(a)g_1 = 0$ and thus Proposition (2.2) implies that $\delta_2(a) = 0$. Polynomials of higher degree can be treated similarly.

With the same process it can be shown that $\sigma_i \mid S$ is the identity map for all i, $1 \leq i \leq t$ and $\delta_i \mid S$ is the zero map for all i, $1 \leq i \leq t$. □

References

[1] S. Annin, Associated primes over skew polynomial rings. Comm. Algebra, Vol. 30 (2002), 2511-2528.

[2] V. K. Bhat, On 2-primal Ore extensions, Ukr. Math. Bull., Vol. 4(2) (2007), 173-179.

[3] V. K. Bhat, Differential operator rings over 2-primal rings, Ukr. Math. Bull., Vol. 5(2) (2008), 153-158.

[4] V. K. Bhat, Associated prime ideals of skew polynomial rings, Beitrge Algebra Geom., Vol. 49(1) (2008), 277-283.

[5] V. K. Bhat, Decomposability of extension rings, Albanian J. Math., Vol. 2(4) (2008), 283-291.

[6] C. Faith, Associated primes in commutative polynomial rings, Comm. Algebra, Vol. 28 (2000), 3983-3986.

[7] K. R. Goodearl and R. B. Warfield Jr., An introduction to non-commutative Noetherian rings, Cambridge Uni. Press, 1989.

[8] C. Y. Hong, N. K. Kim and T.K.Kwak, Ore-extensions of baer and p.p.-rings, J. Pure Appl. Algebra, Vol. 151(3) (2000), 215-226.

[9] A. V. Jategaonkar, Skew-Polynomial rings over order in artinian rings, J. Algebra, Vol. 21 (1972), 51-59.

[10] J. Krempa, Some examples of reduced rings. Algebra Colloq., Vol. 3(4) (1996), 289-300.

[11] T. K. Kwak, Prime radicals of skew-polynomial rings, Int. J. Math. Sci., Vol. 2(2) (2003), 219-227.

[12] G. Marks, On 2-primal Ore extensions, Comm. Algebra, Vol. 29 (5) (2001), 2113-2123.

[13] J. C. McConnell and J. C. Robson, Noncommutative Noetherian Rings, (Wiley 1987; revised edition: American Math. Society 2001).

[14] H. Nordstrom, Associated primes over Ore extensions, J. Algebra, Vol. 286(1) (2005), 69-75.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 75–79
ISSN 1930-1235: (2009)

A NOTE ON LIGHT INDUCED MAPPINGS

Ivan Lončar

Faculty of Organization and Informatics
Varaždin (University of Zagreb),
Pavlinska 2, HR-42000 Varaždin.
ivan.loncar1@vz.htnet.hr

Abstract. Let a mapping $f : X \to Y$ between continua X and Y be given. We shall prove: a) if the induced mapping $2^f : 2^X \to 2^Y$ is light, then $w(X) = w(Y)$. In particular, if Y is metrizable, then X is metrizable, b) if the induced mapping $C(f) : C(X) \to C(Y)$ is light and X is a D-continuum, then $w(X) = w(Y)$.

1. Introduction

All spaces in this paper are compact Hausdorff and all mappings are continuous. The weight of a space X is denoted by $w(X)$. The cardinality of a set A is denoted by $card(A)$.

Let X be a space. We define its hyperspaces as the following sets:

$$2^X = \{F \subseteq X : F \text{ is closed and nonempty}\},$$
$$C(X) = \{F \in 2^X : F \text{ is connected}\},$$
$$X(n) = \{F \in 2^X : F \text{ has at most } n \text{ points}\},\ n \in \mathbb{N}.$$

For any finitely many subsets S_1, ..., S_n, let

$$\langle S_1, ..., S_n\rangle = \left\{ F \in 2^X : F \subset \bigcup_{i=1}^{n} S_i, \text{ and } F \cap S_i \neq \emptyset, \text{ for each } i \right\}.$$

The topology on 2^X is the Vietoris topology, i.e., the topology with a base $\{< U_1, ..., U_n >: U_i$ is an open subset of X for each i and each $n < \infty\}$, and $C(X)$ is a subspace of 2^X.

Given a mapping $f : X \to Y$ between continua X and Y, we let $2^f : 2^X \to 2^Y$ to denote the corresponding *induced* mapping defined by $2^f(F) = f(F)$ for $F \in 2^X$. By [8, 5.10] 2^f is continuous and $2^f(C(X)) \subset C(Y)$ and $2^f(X(n)) \subset Y(n)$. The restriction $2^f|C(X)$ is denoted by $C(f)$.

A continuous mapping $f : X \to Y$ is *light (zero-dimensional)* if all fibers $f^{-1}(y)$ are hereditarily disconnected (zero-dimensional or empty) [3, p. 450], i.e., if $f^{-1}(y)$ does not contain any connected subsets of cardinality larger that one

1991 *Mathematics Subject Classification.* 54F15, 54C10.
Key words and phrases. Continuum, induced mapping, light mapping.

($\dim f^{-1}(y) \leq 0$). Every zero-dimensional mapping is light, and in the realm of mappings with compact fibers the two classes of mappings coincide.

In this paper we shall prove that the lightness of $C(f)$ or 2^f implies the equality of the weights of continua.

It is clear that the lightness of $2^f : 2^X \to 2^Y$ implies the lightness of $C(f) : C(X) \to C(Y)$, but not conversely. The following result is known.

THEOREM 1.1. [1, Theorem 5.4]. *Let continua X and Y and a mapping $f : X \to Y$ be given. Consider the following conditions:*

(a): *$C(f) : C(X) \to C(Y)$ is light;*
(b): *for every two continua $P, Q \in C(X) \setminus X(1)$ with $P \cap Q = \emptyset$ the inequality $f(P) \setminus f(Q) \neq \emptyset$ holds;*
(c): *$2^f : 2^X \to 2^Y$ is light.*

Then (c) implies (b), and (b) implies (a). Consequently, (c) implies (a). The other implications do not hold.

A family $\mathcal{N} = \{M_s : s \in S\}$ of a subsets of a topological space X is a *network* for X if for every point $x \in X$ and any neighbourhood U of x there exists an $s \in S$ such that $x \in M_s \subset U$ [3, p. 170]. The *network weight* of a space X is defined as the smallest cardinal number of the form $card(\mathcal{N})$, where $\mathcal{N}$ is a network for X; this cardinal number is denoted by $nw(X)$.

Remark. It is known that for every compact space X we have $nw(X) = w(X)$ [3, p. 171, Theorem 3.1.19].

2. Lightness of $2^f : 2^X \to 2^Y$ implies $w(X) = w(Y)$

In this section we shall prove the following result.

THEOREM 2.1. *Let a mapping $f : X \to Y$ between continua X and Y be given. If the induced mapping $C(f) : C(X) \to C(Y)$ satisfies the condition that for every two continua $C, D \in C(X) \setminus X(1)$ with $C \cap D = \emptyset$ the inequality $f(C) \setminus f(D) \neq \emptyset$ holds, then $w(X) = w(Y)$.*

Proof. It is obvious that $w(Y) \leq w(X)$ [3, p. 171, Theorem 3.1.22]. Let us prove that $w(Y) \geq w(X)$. The proof is broken into several steps.

Step 1. *$C(f) : C(X) \to C(Y)$ is one-to-one on $C(X) \setminus X(1)$. Moreover, $C(f)$ is a homeomorphism of $C(X) \setminus X(1)$ onto $C(f)(C(X) \setminus X(1))$.* Suppose that $C(f)$ is not one-to-one. Then there exists a continuum F in Y and two continua C, D in X such that $f(C) = f(D) = F$. We have to consider the following cases.

a) $C \cap D = \emptyset$. Now $f(C) \setminus f(D) = \emptyset$. This is impossible because of the condition (b) of Theorem 1.1.

b) $C \subset D$ *or* $D \subset C$. Suppose that $C \subset D$. The proof is similar if $D \subset C$. By [7, p. 1209, Theorem] we infer that there exists an order arc $L \subset C(X)$ from C to D. If a subcontinuum E of X is in L then $f(E) = F$ since $f(C) = f(D) = F$. This means that $C(f)(L) = F$, i.e., $(C(f))^{-1}(F)$ contains a non-degenerate continuum L. This is impossible since $C(f)$ is light (see Theorem 1.1).

c) $C \cap D \neq \emptyset$ and $C \setminus D \neq \emptyset, C \setminus D \neq \emptyset$. Let $C \cup D = K$. It is clear $f(K) = f(C) = f(D) = F$.

Moreover $C \subset K$. By b) this is impossible.

Hence, the proof of Step 1 is completed.

We infer that $C(f)^{-1}[Y \setminus Y(1)] = C(X) \setminus X(1)$. It follows that the restriction $P = C(f)|(C(X) \setminus X(1))$ is one-to-one and closed [3, p. 95, Proposition 2.1.4]. From $C(f)^{-1}[Y \setminus Y(1)] = C(X) \setminus X(1)$ it follows that P is surjective. Hence, P is a homeomorphism.

Step 2. $w(C(X) \setminus X(1)) \leq w(Y)$. Now we have

$$w(C(X) \setminus X(1)) = w(C(f)|(C(X) \setminus X(1))) \leq w(C(Y) \setminus Y(1)) \leq w(2^X) = w(Y)$$

since $w(2^X) = w(Y)$ [3, p. 306, Problem 3.12.26 (a)].

Step 3. $w(X) \leq w(Y)$. Let $\mathcal{B} = \{B_\alpha : \alpha \in A\}$ be a base of $C(X) \setminus X(1)$. For each B_α let $C_\alpha = \{x \in X : x \in B,\ B \in B_\alpha\}$, i.e., the union of all continua B contained in B_α.

Claim 1. *The family $\{C_\alpha : \alpha \in A\}$ is a network of X.* Let X be a point of X and let U be an open subsets of X such that $x \in U$. There exists and open set V such that $x \in V \subset \mathrm{Cl}V \subset U$. Let K be a component of $\mathrm{Cl}V$ containing x. By Boundary Bumping Theorem [10, p. 73, Theorem 5.4] K is non-degenerate and, consequently, $K \in C(X) \setminus X(1)$. Now, $\langle U \rangle \cap (C(X) \setminus X(1))$ is a neighbourhood of K in $C(X) \setminus X(1)$. It follows that there exists a $B_\alpha \in \mathcal{B}$ such that $K \in B_\alpha \subset \langle U \rangle \cap (C(X) \setminus X(1))$. It is clear that $C_\alpha \subset U$ and $x \in C_\alpha$ since $x \in K$. Hence, the family $\{C_\alpha : \alpha \in A\}$ is a network of X.

Claim 2. $nw(X) = w(C(X) \setminus X(1))$. Apply Claim 1. Moreover, by Remark at the end of Introduction, it follows that $w(X) = w(C(X) \setminus X(1))$. Finally, from Step 2 we obtain $w(X) \leq w(Y)$. □

The condition that for every two continua $C, D \in C(X) \setminus X(1)$ with $C \cap D = \emptyset$ the inequality $f(C) \setminus f(D) \neq \emptyset$ holds, used in the proof of Theorem 2.1, is actually condition (b) of Theorem 1.1. Hence, Theorems 2.1 and 1.1 imply the following result.

COROLLARY 2.2. *Let a mapping $f : X \to Y$ between continua X and Y be given. If the induced mapping $2^f : 2^X \to 2^Y$ is light, then $w(X) = w(Y)$.*

3. The lightness of $C(f) : C(X) \to C(Y)$ implies $w(X) = w(Y)$ for D-continua

A continuum X is called a *D-continuum* if for every pair C, D of its disjoint non-degenerate subcontinua there exists a subcontinuum $E \subset X$ such that $C \cap E \neq \emptyset \neq D \cap E$ and $(C \cup D) \setminus E \neq \emptyset$.

The class of D-continua is very large. Each arcwise connected continuum and each locally connected continuum is a D-continuum. Moreover, each aposyndetic continuum is a D-continuum.

In the proof of Theorem 2.1 only the subspace $C(X)$ of 2^X and the lightness of the mapping $C(f) : C(X) \to C(Y)$ is used. If X is a D-continuum then the lightness of the mapping $2^f : 2^X \to 2^Y$ can be omitted. In this case the condition (b) of Theorem 1.1 is replaced by the assumption that X is a D-continuum. This assumption enables to prove the step of the new proof similar to proof of Step1 of the proof of Theorem 2.1. The remaining part of the proof of Theorem 2.1 works in a new situation. Hence we have the following result.

THEOREM 3.1. *Let X be a D-continuum and let $f : X \to Y$ be a mapping such that $C(f) : C(X) \to C(Y)$ is light. Then $w(X) = w(Y)$.*

4. The lightness of $C(f) : C(X) \to C(Y)$ and Whitney map for $C(X)$

The lightness of the mapping $C(f) : C(X) \to C(Y)$ play important role in theory of continua, in particular, in the study of Whitney maps.

Let Λ be a subspace of 2^X. By a *Whitney map* for Λ [9, p. 24, (0.50)] we will mean any mapping $g : \Lambda \to [0, +\infty)$ satisfying

a) if $A, B \in \Lambda$ such that $A \subset B$ and $A \neq B$, then $g(A) < g(B)$ and

b) $g(\{x\}) = 0$ for each $x \in X$ such that $\{x\} \in \Lambda$.

If X is a metric continuum, then there exists a Whitney map for 2^X and $C(X)$ ([9, pp. 24-26], [4, p. 106]). On the other hand, if X is non-metrizable, then it admits no Whitney map for 2^X [2]. It is known that there exist non-metrizable continua which admit and ones which do not admit a Whitney map for $C(X)$ [2].

The following theorem explains the role of light mappings in the study of Whitney maps for continua.

THEOREM 4.1. *A continuum X admits a Whitney map for $C(X)$ if and only if there exists a light mapping $f : C(X) \to Y$ onto a metric continuum Y.*

Proof. **a)** Suppose that X admits a Whitney map for $C(X)$. By [5, Theorem 1.8] there exists a σ-directed inverse system $\mathbf{X} = \{X_a, p_{ab}, A\}$ of metric continua X_a such that X is homeomorphic to $\lim \mathbf{X}$. Now we have a σ-directed inverse system $C(\mathbf{X}) = \{C(X_a), C(p_{ab}), A\}$ of metric continua such that $C(X)$ is homeomorphic to $\lim C(\mathbf{X})$. From [6, Corollary 3.2.] it follows that the projections $C(p_b) : C(\lim \mathbf{X}) \to C(X_b)$ are light for every $b \in B$, where B is cofinal subset of A. Hence, each $C(p_b)$ is a required light mapping onto a metric continuum $Y = C(p_b)(\lim C(\mathbf{X}))$.

b) Suppose now that there exist a light mapping $f : C(X) \to Y$ onto a metric continuum Y. Consider, as in a), a σ-directed inverse system $C(\mathbf{X}) = \{C(X_a), C(p_{ab}), A\}$ of metric continua such that $C(X)$ is homeomorphic to $\lim C(\mathbf{X})$. There is a subset B cofinal in A such that there exists a mapping $f_b : C(p_b)(\lim C(X)) \to Y$ such that $f = f_b C(p_b)$ since $C(\mathbf{X})$ is σ-directed and Y is metric. Let us prove that $C(p_b)$ is light. Suppose that it is not light. Then there exist a point $z \in C(p_b)(\lim C(X))$ such that $C(p_b)^{-1}(z)$ contains a continuum Z. It follows that $f^{-1}(f_b(z))$ contains Z since $C(p_b)^{-1}(z) \subset f^{-1}(f_b(z))$. This is impossible since f is light. Hence, $C(p_b)$ is light. By [6, Corollary 3.2.] we infer that X admits a Whitney map for $C(X)$. The proof of Theorem is completed. □

The notion of an irreducible mapping was introduced by Whyburn [11, p. 162]. If X is a continuum, a surjection $f : X \to Y$ is *irreducible* provided no proper subcontinuum of X maps onto all of Y under f. Some theorems for the case when X is semi-locally-connected are given in [11, p. 163].

A mapping $f : X \to Y$ is said to be *hereditarily irreducible* [9, p. 204, (1.212.3)] provided that for any given subcontinuum Z of X, no proper subcontinuum of Z maps onto $f(Z)$.

Proposition 1. [9, p. 204, (1.212.3)]. *If $f : X \to Y$ is a mapping between continua, then $C(f) : C(X) \to C(Y)$ is light if and only if f is hereditarily irreducible.*

Proposition 1 and Theorem 4.1 imply the following result.

COROLLARY 4.2. *A continuum X admits a Whitney map for $C(X)$ if and only if there exists a hereditarily irreducible mapping $f : X \to Y$ onto a metric continuum Y.*

COROLLARY 4.3. *Let $f : C(Y) \to C(Y)$ be a light mapping. If Y admits a Whitney map for $C(Y)$, then X admits a Whitney map for $C(X)$.*

Proof. Consider a σ-directed inverse system $C(\mathbf{Y}) = \{C(Y_a), C(q_{ab}), A\}$ of metric continua such that $C(Y)$ is homeomorphic to $\lim C(\mathbf{Y})$. There is a subset B cofinal in A such that the projections $C(q_b)$ are light. Now, the composition $C(q_b)f : C(X) \to Y_b$ is light since the composition of light mappings is light. By Theorem 4.1 X admits a Whitney map for $C(X)$. □

We close this Section with theorem which shows that the existence of Whitney map for $C(X)$ is equivalent to the metrizability of X.

THEOREM 4.4. *A D-continuum X admits a Whitney map for $C(X)$ if and only if X is metrizable. In particular, if X is either an arcwise connected, or locally connected or aposyndetic continuum, then X admits a Whitney map for $C(X)$ if and only if X is metrizable.*

Proof. By Theorem 4.1 a continuum X admits a Whitney map for $C(X)$ if and only if there exists a light mapping $f : C(X) \to Y$ onto a metric continuum Y. Moreover, from Theorem 3.1 it follows that $w(X) = w(Y)$. Hence, X is metrizable since $w(Y) = \aleph_0$. IF X is either an arcwise connected continuum or a locally connected continuum or aposyndetic continuum, then X is a D-continuum and, consequently, metrizable. □

References

[1] J. J. Charatonik and W. J. Charatonik, *Lightness of induced mappings*, Tsukuba J. Math. 22 (1998), 179-192.

[2] J. J. Charatonik and W. J. Charatonik, *Whitney maps—a non-metric case*, Colloq. Math. 83 (2000), 305-307.

[3] R. Engelking, General Topology, PWN, Warszawa, 1977.

[4] A. Illanes and S.B. Nadler, Jr., *Hyperspaces: Fundamentals and Recent advances*, Marcel Dekker, New York-Basel 1999.

[5] I. Lončar, *A fan X admits a Whitney map for C(X) iff it is metrizable*, Glas. Mat. Ser. III, 38 (58) (2003), 395-411.

[6] I. Lončar, *A note on the spaces which admit a Whitney map*, Rad Hrvatske akademije znanosti i umjetnosti, Matematičke znanosti 491 (2005), 195-206.

[7] M. M. McWaters, *Arcs, semigroups, and hyperspace* , Canad. J. Math. 20 (1968), 1207-1210.

[8] E. Michael, *Topologies on spaces of subsets*, Trans. Amer. Math. Soc. 7(1951), 152-182.

[9] S. B. Nadler, *Hyperspaces of sets*, Marcel Dekker, Inc., New York, 1978.

[10] S. B. Nadler, Jr., Continuum theory: An Introduction, Marcel Dekker,Inc.,New York,1992, Zbl 0757.54009.

[11] G.T. Whyburn, *Analytic Topology*, vol. 28, American Mathematical Society, Providence, R.I, 1963.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 2, Pages 63–74
ISSN 1930-1235: (2009)

NEAR-EXTREMES AND RELATED POINT PROCESSES

N. BALAKRISHNAN, E. HASHORVA, AND J. HÜSLER

ABSTRACT. Let $X_i, i \geq 1$ be a sequence of random variables with continuous distribution functions and let $\{N(t), t \geq 0\}$ be a random counting process. Denote by $X_{i:N(t)}, i \leq N(t)$ the i-th lower order statistics of $X_1, \ldots, X_{N(t)}, t \geq 0$ and define a point process in $\mathbb{R}$ by $\mathbf{M}_{t,m}(\cdot) := \sum_{i=1}^{N(t)} \mathbf{1}(X_{N(t)-m+1:N(t)} - X_i \in \cdot), m \in \mathbb{N}$. In this paper we derive distributional and asymptotical results for $\mathbf{M}_{t,m}(\cdot)$. For special marginals of the point process we retrieve some general results for the number of m-th near-extremes.

1. INTRODUCTION

Let $X_i, i \geq 1$ be a sequence of random variables with continuous distribution functions and let $\{N(t), t \geq 0\}$ be a random counting process independent of $X_n, n \geq 1$. Denote by $X_{N(t)-i+1:N(t)}$ the i-th largest order statistic of $X_1, \ldots, X_{N(t)}$, if $N(t) \geq i$. For any positive constant a and $m \in \mathbb{N}$ define the discrete random variable $\mathbf{K}_t(a, m)$ by

$$\mathbf{K}_t(a,m) \quad := \quad \sum_{i=1}^{N(t)} \mathbf{1}(X_{N(t)-m+1:N(t)} - X_i \in [0,a)), \qquad \text{if } N(t) \geq m,$$

and 0, otherwise. $\mathbf{K}_t(a, m)$ counts the number of sample points X_i which fall in the random window $W_{t,a,m} := (X_{N(t)-m+1:N(t)} - a, X_{N(t)-m+1:N(t)}]$ ($\mathbf{1}(\cdot)$ stands for the indicator function).

Basic asymptotic properties of $\mathbf{K}_t(a, m)$ are obtained in Hashorva (2003), Hashorva and Hüsler (2008). The motivation for considering the random variable $\mathbf{K}_t(a, m)$ comes from the fact that for some applications the randomly indexed order statistics are of direct interest, for instance when dealing with claim sizes in an insurance context. Statistical applications can be found in Hashorva and Hüsler (2005).

Distributional and asymptotical results in connection with the number of sample points X_i such that $X_{n-m+1:n} - X_i \in B$, where $B = [0, a)$ or $B = (-a, 0]$ are derived in Balakrishnan and Stepanov (2004, 2005) and Dembinska et al. (2007).

In an asymptotic context it is of some interest to allow the length of the random window $W_{t,a,m}$ to depend directly on t. This can be achieved for instance if $a = a(t)$ or $a = a(N(t))$. In Balakrishnan and Stepanov (2004, 2005) fixed length random windows are dealt with in detail.

In this paper we have following objectives in mind:
a) Instead of defining different random variables (like $\mathbf{K}_t(a, m), a > 0$), we choose a

2000 *Mathematics Subject Classification.* Primary 60F15; Secondary 60G70.
Key words and phrases. Near-extremes; extreme value theory; point processes; asymptotic results.

more general approach utilising point processes. In fact a point processes approach (considering only the maxima) is suggested in Hashorva and Hüsler (2000). One advantage of the point process approach is that several previously studied random quantities are retrieved when the Borel set B is an interval $[a,b) \subset \mathbb{R}$.

b) We allow the random window to grow/shrink with t by considering a scaling of the Borel set B.

c) Besides the iid case (independence and common distribution assumption on $X_i, i \geq 1$) we consider the general setup where $X_i, i \geq 1$ can be dependent. From the statistical point of view this extension is interesting since dependence is often observed in practical situations.

Explicitly, define a family of point processes $\mathbf{M}_{t,m}(\cdot)$ by

$$\mathbf{M}_{t,m}(B) \quad := \quad \sum_{i=1}^{N(t)} \mathbf{1}(X_{N(t)-m+1:N(t)} - X_i \in B).$$

The random variable $\mathbf{M}_{t,m}(B)$ counts the number of sample points X_i in the Borel set $B \subset \mathbb{R}$ near the m-th randomly indexed order statistics. We suppose without loss of generality that $N(0) = m$ almost surely. Further, we assume throughout this paper that $\{N(t), t \geq 0\}$ has almost surely non-decreasing sample paths. If $m = 1$ and $B \subset (-\infty, 0]$ put $\mathbf{M}_{t,1}(B) := \mathbf{1}(0 \in B)$. Hashorva and Hüsler (2008) derive distributional and asymptotic properties of the point process

$$M_{n,m}(B) \quad := \quad \sum_{i=1}^{n} \mathbf{1}(X_{n-m+1:n} - X_i \in B), \quad n > 1, \quad B \subset [0, \infty)$$

assuming that $X_n, n \geq 1$ possess a common continuous distribution function F.
In this paper we deal with distributional and asymptotic properties of $\mathbf{M}_{t,m}(\cdot)$. For $m > 1$ we consider in some detail also the interesting case $B \subset (-\infty, 0]$.
When $B = [0, a)$, or $B = (-a, 0], a > 0$ Balakrishnan and Stepanov (2005), and Dembinska et al. (2007) derive some distributional and asymptotical properties of $\mathbf{M}_{t,m}(B)|N(t) = n$.

Outline of the rest of the paper: In the next section we provide few preliminary results. In Section 3 we begin with some asymptotic results for the iid case. Then we focus on the situation where the sample points $X_i, i \geq 1$ can be dependent. Two illustrating examples are presented in Section 4. The proofs of all the results are relegated to Section 5.

2. Preliminaries

Let $X_i, i \geq 1$ be independent random variables with common continuous distribution function F and let $N(t)$ be as defined above independent of $X_i, i \geq 1$.
In this section we derive the probability generating function (p.g.f.) of marginals of the point process $\mathbf{M}_{t,m}(\cdot)$. Then we give a preliminary result on the joint weak convergence of randomly indexed upper order statistics.

Write in the following $\stackrel{d}{=}$ to mean equality of distribution functions of two given random variables. In the next lemma we derive the p.g.f. of the point process of interest.

Lemma 1. *Let $\{X_i, i \geq 1\}$ be independent random variables with common continuous distribution function F. Let $x \in \mathbb{R}$ and m, n be two integers such that*

$F(x) \in (0,1)$, and $1 \le m < n, m, n \in \mathbb{N}$. Then we have for any Borel set $B \subset [0,\infty)$ or $B \subset (-\infty, 0]$

$$\Big(M_{n,m}(B)|X_{n-m+1:n} = x\Big) \quad \stackrel{d}{=} \quad \mathbf{1}(0 \in B) + \sum_{i=1}^{n_{B,m}} \mathbf{1}(x - \eta_i^{[x]} \in B), \tag{1}$$

where $n_{B,m} := n - m, \eta_i^{[x]} \stackrel{d}{=} X_1 | X_1 \le x, i \ge 1$ if $B \subset [0,\infty)$, and $n_{B,m} := m - 1, \eta_i^{[x]} \stackrel{d}{=} X_1 | X_1 > x, i \ge 1$ if $B \subset (-\infty, 0]$ and $m > 1$, with $\eta_i^{[x]}, i \ge 1$ independent random variables.
Furthermore, if $N(t), t \ge 0$ is a counting process such that $N(0) = m$ almost surely being further independent of $X_i, i \ge 1$, then we have

$$\begin{aligned} \boldsymbol{E}\Big\{ s^{\mathbf{M}_{t,m}(B) - \mathbf{1}(0 \in B)} \Big\} \quad &= \quad \sum_{n=m}^{\infty} \boldsymbol{P}\{N(t) = n\} \int_{\mathbb{R}} \Big[1 - (1-s) \boldsymbol{P}\Big\{ x - \eta_1^{[x]} \in B \Big\} \Big]^{n_{B,m}} \\ &\qquad \times dF_{n-m+1:n}(x), \quad \forall s \in (0,1), \end{aligned} \tag{2}$$

with $F_{n-m+1:n}$ the distribution function of $X_{n-m+1:n}$.

By the above lemma for $n > m > 1$ we obtain (suppose $0 \not\in B$)

$$\boldsymbol{E}\{\mathbf{M}_{t,m}(B) | N(t) = n\} \quad = \quad n_{B,m} \int_{\mathbb{R}} \boldsymbol{P}\{x - \eta_1^{[x]} \in B\} \, dF_{n-m+1:n}(x), \tag{3}$$

where the distribution function $F_{n-m+1:n}$ of $X_{n-m+1:n}$ has F-density (cf. Theorem 1.5.1 of Reiss (1989))

$$\frac{n! F^{n-m}(x)(1 - F(x))^{m-1}}{(n-m)!(m-1)!}, \quad x \in \mathbb{R}. \tag{4}$$

Consequently $\boldsymbol{E}\{\mathbf{M}_{t,m}(B)\} < \infty$ if $\boldsymbol{E}\{N(t)\} < \infty, t > 0$.

Remark 1. If $B = B_1 \cup B_2$ with B_1, B_2 two disjoint Borel sets such that $B_1 \subset (-\infty, 0], B_2 \subset [0,\infty)$ we have

$$M_{n,m}(B) = M_{n,m}(B_1) + M_{n,m}(B_2), \quad n > m > 1.$$

For any $x \in \mathbb{R}$ such that $F(x) \in (0,1)$ the random variable $M_{n,m}(B_1)$ and $M_{n,m}(B_2)$ are conditionally independent given $X_{n-m+1:n}$. This fact is important and leads to general results for general Borel sets $B \subset \mathbb{R}$.

A common asymptotic assumption on the counting process $\{N(t), t \ge 0\}$, which we want to impose for our asymptotic results is the convergence in probability

$$N(t)/t \xrightarrow{p} Z, \quad t \to \infty, \tag{5}$$

where Z is a non-negative random variable such that $\boldsymbol{P}\{Z \in (0,\infty)\} = 1$.

The second important asymptotic assumption concerns the asymptotic behaviour of the sample maxima of the random sequence $X_i, i \ge 1$. Specifically, we assume that the underlying distribution function F is in the max-domain of attraction of a univariate extreme value distribution function H (write this as $F \in MDA(H)$), i.e.

$$\lim_{t \to \infty} \sup_{x \in \mathbb{R}} \Big| F^t(q(t)x + r(t)) - H(x) \Big| \quad = \quad 0, \tag{6}$$

with $q(t) > 0, r(t)$ two measurable functions. For further details on extreme value theory we refer the reader to the following monographs: Leadbetter et al. (1983), Resnick (1987), Reiss (1989), Falk et al. (2004), De Haan and Ferreira (2006).

Denote by α_H, x_H the lower and the upper endpoint of the distribution function H. The univariate extreme value distribution function H is either the Gumbel distribution $\Lambda(x) = \exp(-\exp(-x)), x \in \mathbb{R}$, the Weibull distribution $\Psi_\alpha(x) = \exp(-|x|^\alpha), x < 0, \alpha > 0$, or the Fréchet distribution $\Phi_\alpha(x) = \exp(-x^{-\alpha}), x > 0, \alpha > 0$. Note in passing that if

$$\lim_{x\to\infty} \frac{1-F(x+a)}{1-F(x)} = \beta(a) \in (0,1), \quad \forall a > 0, \tag{7}$$

then F is in the Gumbel max-domain of attraction with $q(t) := 1, t > 0$.

The asymptotic condition on F in (6) is equivalent with the joint convergence in distribution (see e.g. Falk et al. (2004))

$$\Big(\frac{X_{n:n} - r(n)}{q(n)}, \ldots, \frac{X_{n-k+1:n} - r(n)}{q(n)}\Big) \quad \xrightarrow{d} \quad (Y_1, \ldots, Y_k), \quad \forall k \geq 2 \tag{8}$$

as $n \to \infty$, with $(Y_1, \ldots, Y_k)$ a random vector in $\mathbb{R}^k$ with density function

$$h_k(x_1, \ldots, x_k) \quad = \quad H(x_k) \prod_{i=1}^{k} \frac{H'(x_i)}{H(x_i)} \tag{9}$$

which is positive for $\alpha_H < x_l < x_{l-1} < \cdots < x_1 < x_H$. If $X_i, i \geq 1$ are dependent, then the convergence in distribution of the upper order statistics follows under additional asymptotic restrictions. Indeed, several results for asymptotic behaviour of univariate sample extremes of non-iid sequences are available in the literature. For instance, if $X_i, i \geq 1$ is a stationary random sequence such that (6) holds and the weak distributional mixing conditions $D_l(\boldsymbol{u}_n), l \in \mathbb{N}, D'(u_n)$ (see Falk et al. (2004)) are satisfied with $u_n = q(n) + r(n), \boldsymbol{u}_n = (u_n, \ldots, u_n) \in \mathbb{R}^k$, then (8) holds with $l = k$. The definitions of $D_k(\boldsymbol{u}_n)$ and $D'(u_n)$ are given in Leadbetter et al. (1983). The mixing conditions are satisfied if $X_n, n \geq 1$ are independent with distribution function F such that (6) holds.

3. Main Results

In this section we shall derive several asymptotic results for the scaled point process

$$\widetilde{\mathbf{M}}_{t,m}(B) := \mathbf{M}_{t,m}(\widetilde{q}(t)B), \quad B \subset \mathbb{R},$$

where $\widetilde{q}(t)$ is a positive measurable scaling function. In our asymptotic results we relate $\widetilde{q}(t)$ with the scaling function $q(t)$ (provided that assumption (6) is valid) by the following relation

$$\lim_{t\to\infty} \frac{\widetilde{q}(t)}{q(t)} \quad = \quad Q \in [0, \infty). \tag{10}$$

We consider briefly the iid setup, i.e., we assume that $X_i, i \geq 1$ are independent with common continuous distribution function F. As previously shown in Hashorva and Hüsler (2008), Hashorva (2003), Hashorva and Hüsler (2005), under this assumption a convenient approach to derive asymptotic results for the scaled point process of interest is to utilise (2).

If both (5) and (6) hold, then Proposition 2.1 of Hashorva (2003) implies for any $k \geq 1$ as $t \to \infty$

$$\Big(\frac{X_{N(t):N(t)} - r(t)}{q(t)}, \ldots, \frac{X_{N(t)-k+1:N(t)} - r(t)}{q(t)}\Big) \quad \stackrel{d}{\to} \quad (Y_1^*, \ldots, Y_k^*), \tag{11}$$

where for any $i \geq 1$ we have if $H = \Lambda$

$$Y_i^* \stackrel{d}{=} Y_i + \ln Z$$

and

$$Y_i^* \stackrel{d}{=} Z^{-1/\alpha} Y_i, \quad Y_i^* \stackrel{d}{=} Z^{1/\alpha} Y_i$$

holds if $H = \Psi_\alpha$ or $H = \Phi_\alpha$, respectively. Furthermore, Z is independent of $Y_i, i \geq 1$.

When $H = \Lambda$ or $H = \Psi_\alpha, \alpha > 0$ we obtain with similar arguments as in Hashorva (2004) using (2) and (11) for all $s \in (0,1)$

$$\lim_{t\to\infty} \boldsymbol{E}\{s^{\widetilde{\mathbf{M}}_{t,m}(B)}\} = \boldsymbol{E}\Big\{\exp(-(1-s)Z \ln\Big(H(Y_m^* - Qb)/H(Y_m^* - Qa)\Big)\Big\}, \tag{12}$$

with $B := [a,b), 0 < a < b < \infty$. The above limiting expression is the p.g.f. of a mixed Poisson random variable. Hence convergence in distribution for $\widetilde{\mathbf{M}}_{t,m}(B)$ follows. If $H = \Lambda$, then the limiting p.g.f. in (12) does not depend on Z. This fact is mentioned in Corollary 2.7 of Hashorva (2003) (only for the case a, b positive and $m = 1$). $F \in MDA(\Lambda)$ follows if for instance F satisfies (7) so that we can choose the scaling function $q(t)$ as a positive constant. Consequently, (12) implies the result of Theorem 2.1 of Balakrishnan and Stepanov (2005) (for $\beta(a) \in (0,1)$). If (10) holds with $Q = 0$, then by (12)

$$\lim_{t\to\infty} \boldsymbol{E}\{s^{\widetilde{\mathbf{M}}_{t,m}(B)}\} \quad = \quad \boldsymbol{E}\{\exp(-(1-s)Z \ln(H(Y_m^*)/H(Y_m^*))\} = 1, \quad \forall s \in (0,1)$$

implying the convergence in probability

$$\widetilde{\mathbf{M}}_{t,m}(B) \stackrel{p}{\to} 0, \quad t \to \infty.$$

In case that $H = \Phi_\alpha$ the sequence $\mathbf{M}_{t,m}(B), t > 0$ is not tight.

Similarly, if $F \in \mathrm{MDA}(H)$ we obtain for any $m > 1, B := [a,b), -\infty < a < b < 0$

$$\lim_{t\to\infty} \boldsymbol{E}\{s^{\widetilde{\mathbf{M}}_{t,m}(B)}\} \quad = \quad \boldsymbol{E}\Big\{\Big[1 - (1-s)\frac{1}{\ln H(Y_m^*)} \ln\Big(\frac{H(Y_m^* - Qb)}{H(Y_m^* - Qa)}\Big)\Big]^{m-1}\Big\} \tag{13}$$

for all $s \in (0,1)$. The limiting expression in (13) is the p.g.f. of a mixed binomial random variable. It is interesting, that again if $H = \Lambda$, the limiting p.g.f. does not depend on Z. Explicitly, for any $s \in (0,1)$ we have

$$\lim_{t\to\infty} \boldsymbol{E}\{s^{\widetilde{\mathbf{M}}_{t,m}(B)}\} \quad = \quad \Big[1 - (1-s)[\exp(Qb) - \exp(Qa)]\Big]^{m-1}. \tag{14}$$

The above convergence holds if F satisfies (7) implying thus the result of Theorem 3.1 in Balakrishnan and Stepanov (2005).

The iid case is tractable due to the fact that we have a compact formula for the p.g.f. of the marginals of the point process given in (2). As in Hashorva and Hüsler (2008) we discuss next the asymptotic behaviour of the scaled point process dropping the independence assumption on $X_n, n \geq 1$.

Our next results are motivated by the following observation (see Pakes and Steutel

(1997)): If ξ, ξ^* are two positive constants and i, i^*, m, m^* are given integers such that $m-1 \geq i \geq 1, m^*-1 \geq i^* \geq 1$, then we may write using (5) and (11)

$$\begin{aligned}
&\boldsymbol{P}\Big\{\widetilde{\mathbf{M}}_{t,m}([0,\xi)) > i, \widetilde{\mathbf{M}}_{t,m^*}((-\xi^*,0]) > i^*\Big\}\\
&= \boldsymbol{P}\Big\{\widetilde{\mathbf{M}}_{t,m}([0,\xi)) > i, \widetilde{\mathbf{M}}_{t,m^*}((-\xi^*,0]) > i^*,\, N(t) > \max(i+m, m^*)\Big\}\\
&= \boldsymbol{P}\Big\{X_{N(t)-m+1:N(t)} - X_{N(t)-i-m+1:N(t)} \leq \xi q(t),\\
&\qquad X_{N(t)-(m^*-i^*)+1:N(t)} - X_{N(t)-m^*+1:N(t)} \leq \xi^* q(t), N(t) > \max(i+m, m^*)\Big\}.
\end{aligned}$$

Consequently, as $t \to \infty$

$$\begin{aligned}
&\boldsymbol{P}\Big\{\widetilde{\mathbf{M}}_{t,m}([0,\xi)) > i, \widetilde{\mathbf{M}}_{t,m^*}((-\xi^*,0]) > i^*\Big\}\\
&\to \boldsymbol{P}\{Y^*_m - Y^*_{m+i} \leq \xi, Y^*_{m^*-i^*} - Y^*_{m^*} \leq \xi^*\}. \qquad (15)
\end{aligned}$$

In the above derivation we do not use explicitly the fact that $X_i, i \geq 1$ are iid. In the following we suppose that (11) holds, dropping thus the independence assumption on $X_i, i \geq 1$. We consider next the joint weak convergence of the point processes $\widetilde{\mathbf{M}}_{t,1}(\cdot), \ldots, \widetilde{\mathbf{M}}_{t,m}(\cdot)$.

Theorem 2. *Let $X_i, i \geq 1$ be random variables with common continuous distribution function F, and let $\{N(t), t \geq 0\}$ be a counting stochastic process. Assume that* (11) *holds with $q(t) > 0$ and $r(t)$ two real functions. If the convergence in probability $N(t) \xrightarrow{p} \infty$ as $t \to \infty$ holds, then for indices $\boldsymbol{j} := \{j_{i,k}\}_{i\leq I, k\leq K}, \boldsymbol{j}^* := \{j^*_{i,k}\}_{i\leq I,k\leq K}, I, K \in \mathbb{N}, j^*_{i,k} < K, i \leq I, k \leq K$ and positive constants $\boldsymbol{\xi} := \{\xi_{i,k}\}_{i\leq I,k\leq K}, \boldsymbol{\xi}^* := \{\xi^*_{i,k}\}_{i\leq I,k\leq K}$ we have*

$$\begin{aligned}
&\lim_{t\to\infty} \boldsymbol{P}\{\widetilde{\mathbf{M}}_{t,k}([0,\xi_{i,k})) \leq j_{i,k}, \widetilde{\mathbf{M}}_{t,k}((-\xi^*_{i,k},0]) \leq j^*_{i,k},\ \textit{for all } 1 \leq i \leq I, 1 \leq k \leq K\}\\
&= \boldsymbol{P}\{Y^*_k - Y^*_{k+j_{i,k}} > \xi_{i,k}, Y^*_{k-j^*_{i,k}} - Y^*_k > \xi^*_{i,k},\ \textit{for all } 1 \leq i \leq I, 1 \leq k \leq K\}\\
&:= G_K(\boldsymbol{\xi}, \boldsymbol{\xi}^*, \boldsymbol{j}, \boldsymbol{j}^*) \qquad (16)
\end{aligned}$$

and $\{\widetilde{\mathbf{M}}_{t,k}((-\xi^*_{i,k},0])\}_{1\leq i\leq I, 1\leq k\leq K}$ converge in distribution to a random vector in $\mathbb{R}^{IK}$. If in addition

$$Y^*_n \xrightarrow{p} -\infty, \quad n \to \infty \qquad (17)$$

holds, then we have the weak convergence

$$(\widetilde{\mathbf{M}}_{t,1}(\cdot), \ldots, \widetilde{\mathbf{M}}_{t,K}(\cdot)) \xrightarrow{w} \boldsymbol{L}(\cdot), \quad t \to \infty, \qquad (18)$$

with $\boldsymbol{L}(\cdot)$ a point processes defined on $\mathbb{R}^K$.

The joint distribution function of the marginals of $\boldsymbol{L}(\cdot)$ can be obtained using (16). If we impose some additional assumptions on the dependence of $X_i, i \geq 1$ and further assume (5) it is possible to obtain a more explicit description of the limiting point process.

Corollary 3. *Under the assumptions of Theorem 2 if* (5) *holds with $X_i, i \geq 1$ independent of $N(t), t > 0$ and further* (6) *holds and conditions $D_{2K}(\boldsymbol{u}_n), D'(u_n)$*

are satisfied with $u_n = q(n) + r(n), \boldsymbol{u}_n = \mathbf{1}u_n, K \in \mathbb{N}$, *then we have the stochastic representation*

$$(Y_1^*, \ldots, Y_{2K}^*) \stackrel{d}{=} (Z^\gamma Y_1 + \beta \ln Z, \ldots, Z^\gamma Y_{2K} + \beta \ln Z), \tag{19}$$

where $\gamma := 0, 1/\alpha, -1/\alpha$ *if* $H = \Lambda, \Phi_\alpha, \Psi_\alpha, \alpha > 0$, *respectively, and* $\beta := 1$ *if* $H = \Lambda$ *and 0 otherwise. Furthermore,*

$$G_K(\boldsymbol{\xi}, \boldsymbol{\xi}^*, \boldsymbol{j}, \boldsymbol{j}^*)$$

$$= \boldsymbol{P}\{Z^\gamma[Y_k - Y_{k+j_{i,k}}] > \xi_{i,k}, Z^\gamma[Y_{k-j_{i,k}^*} - Y_k] > \xi_{i,k}^*, 1 \le i \le I, 1 \le k \le K\}. \tag{20}$$

In the case $H = \Lambda$ above we have a stochastic representation (see Hashorva (2006))

$$(Y_1, \ldots, Y_m)$$

$$\stackrel{d}{=} \Big(E_1 + \sum_{l=2}^{\infty} \frac{E_l - 1}{l} + C_1, \ldots, E_m + \sum_{l=m+1}^{\infty} \frac{E_l - 1}{l} + C_m\Big), \quad 2 \le m \le K, \tag{21}$$

where $E_i, i \ge 1$ are independent random variables with unit exponential distribution and $C_i := C - \sum_{l=1}^{i} \frac{1}{l}, i \ge 1$ where $C == 0.5772$ is the Euler constant. Remark that (19) is initially obtained in Hashorva (2003).

Making use of Corollary 3 weak convergence of $\widetilde{\mathbf{M}}_{t,m}(\cdot)$ for $H = \Lambda$ or $H = \Phi_\alpha, \alpha > 0$ can be easily established utilising further (12) and (13). We discuss below briefly two special cases. Next, write $Y \sim Nb(m, q)$ if the random variable Y has a negative binomial distribution function with parameters m, q and probability density function

$$\frac{\Gamma(m+k)}{\Gamma(m)\Gamma(k+1)} q^m p^k, \quad k \ge 0, \quad q \in (0,1), p := 1 - q,$$

where $\Gamma(\cdot)$ is the Gamma function.

Corollary 4. *Under the assumption of Corollary 3 if further* $H = \Lambda$, *then we have:*
i) For any $m \ge 2$ *and* $-\infty < a < b \le 0$ *two negative constants*

$$\widetilde{\mathbf{M}}_{t,m}((a,b]) \stackrel{d}{\to} U_m(a,b) + \mathbf{1}(b \in \{0\}), \quad t \to \infty, \tag{22}$$

where $U_m(a,b)$ *is a Binomial random variable with parameters* $m-1, p := e^b - e^a \in (0,1)$.
ii) For any $0 \le a < b \le \infty$ *and* $m \in \mathbb{N}$

$$\widetilde{\mathbf{M}}_{t,m}((a,b]) \stackrel{d}{\to} V_m(a,b) + \mathbf{1}(a \in \{0\}), \quad t \to \infty, \tag{23}$$

with $V_m(a,b) \sim Nb(m, [1 + e^b - e^a]^{-1})$. *iii) Furthermore, for any* $k \ge 2, r \ge 1$ *and* a_i, b_i *such that* $-\infty < a_i < b_i \le 0, i = 1, \ldots, k$ *we have* $(U_2(a_2, b_2), \ldots, U_k(a_k, b_k))$ *is independent of* $V_k(a_k, b_k), \ldots, V_{k+r}(a_{k+r}, b_{k+r})$ *with* $0 \le a_{k+i} < b_{k+i} < \infty, i = 0, \ldots, r$.

Remark 2. *a*) As noted above Z and $Y_1, \ldots, Y_m, m \ge 2$ in Corollary 3 are independent random variables.

b) By Corollary 4 we have that under iii) both $\widetilde{\mathbf{M}}_{t,m}((a,b])$ and $\widetilde{\mathbf{M}}_{t,m}((a',b'])$ with $0 \le a < b < \infty, -\infty < b' < a' \le 0$ are asymptotically independent. Balakrishnan and Stepanov (2005) show in Theorem 4.2 this fact for the case $a = 0, a' = 0$

and assuming that F satisfies (7) . The result of Corollary 4 subsumes that of Theorem 4.2 of Balakrishnan and Stepanov (2005).

4. Examples

To illustrate the results we choose two special distribution functions F.

Example 1. Assume that $N(t)$ is independent of $\{X_i, i \geq 1\}$ which are independent standard exponential random variable, i.e. $F(x) = 1 - \exp(-x)\mathbf{1}(x > 0)$. It is well-known that

$$X_{n:n} - \ln n \xrightarrow{d} Y, \quad n \to \infty,$$

with Y a unit Gumbel random variable. A convenient representation for order statistics exists in the exponential case (cf. Reiss (1989))

$$\{X_{n-m+1:n}\}_{m=1,\ldots,n} \stackrel{d}{=} \Big\{\sum_{i=m}^{n} E_i/i\Big\}_{m=1,\ldots,n,n\in\mathbb{N}}.$$

Using further (4) we may write for $m, j \in \mathbb{N}, m + j \leq n$

$$\begin{aligned}
\boldsymbol{P}\{\mathbf{M}_{t,m}([0,a)) > j | N(t) = n\} &= \boldsymbol{P}\{X_{n-m+1:n} - X_{n-m+1-j:n} \leq a\} \\
&= \boldsymbol{P}\Big\{\sum_{i=m}^{m+j-1} E_i/i \leq a\Big\} \\
&= \boldsymbol{P}\{X_{j:(m+j-1)} \leq a\} \\
&= \frac{(m+j-1)!}{(j-1)!(m-1)!}\int_0^a e^{-ms}(1-e^{-s})^{j-1}\,ds \\
&= \frac{(m+j-1)!}{(j-1)!(m-1)!}\int_0^{1-e^{-a}} y^{j-1}(1-y)^{m-1}dy.
\end{aligned}$$

Note that the above probability does not dependent of n, if n is sufficiently large $(n \geq j + m)$.

So we get for t large assuming further that $N(t) \xrightarrow{p} \infty$ as $t \to \infty$

$$\begin{aligned}
\boldsymbol{P}\{\mathbf{M}_{t,m}([0,a)) > j\} &= \boldsymbol{P}\{\mathbf{K}_t(a,m) > j, N(t) \geq j+m\} \\
&= \sum_{n=j+m}^{\infty} \boldsymbol{P}\{X_{j:m+j-1} \leq a\}\boldsymbol{P}\{N(t) = n\} \\
&= \boldsymbol{P}\{X_{j:m+j-1} \leq a\}\boldsymbol{P}\{N(t) \geq j+m\},
\end{aligned}$$

hence Corollary 4 yields

$$\lim_{t\to\infty} \boldsymbol{P}\{\mathbf{M}_{t,m}([0,a)) > j\} = \boldsymbol{P}\{V > j-1\},$$

with V a negative binomial random variable with parameters m and $q := e^{-a}$. Consequently we obtain for any $x \in (0,1)$ and $1 \leq j \leq m, j, m \in \mathbb{N}$ the following Taylor expansion

$$(1-x)^{-m}\frac{(m+j-1)!}{(j-1)!(m-1)!}\int_0^x y^{j-1}(1-y)^{m-1}dy = \sum_{k=j}^{\infty}\frac{\Gamma(m+k)}{\Gamma(m)k!}x^k. \tag{24}$$

For $\mathbf{M}_{t,m}((-a,0]), m>1, 1\le j\le m-1$

$$\begin{aligned}\boldsymbol{P}\{\mathbf{M}_{t,m}((-a,0])>j|N(t)=n\} &= \boldsymbol{P}\{X_{n-m+j+1:n}-X_{n-m+1:n}\le a\}\\ &= \boldsymbol{P}\Big\{\sum_{i=m-j}^{m-1}E_i/i\le a\Big\}\\ &= \boldsymbol{P}\{X_{j:m-1}\le a\}\\ &= \frac{(m-1)!}{(j-1)!(m-j-1)!}\int_0^{1-e^{-a}}y^{j-1}(1-y)^{m-j-1}dy.\end{aligned}$$

Example 2. Another tractable instance is when F is the uniform distribution on $(0,1)$. Corollary 1.6.10 in Reiss (1989) implies the following stochastic representation (Renyi representation)

$$\{X_{n-m+1:n}\}_{m=1,\dots,n}\stackrel{d}{=}\Big\{\frac{\sum_{i=1}^{n-m+1}E_i}{\sum_{i=1}^{n+1}E_i}\Big\}_{m=1,\dots,n},$$

with $E_1,\dots,E_{n+1}$ iid standard exponential random variables. Thus for $1\le j\le n-m$ and $a>0$

$$\begin{aligned}\boldsymbol{P}\{\mathbf{M}_{t,m}([0,a))>j|N(t)=n\} &= \boldsymbol{P}\{X_{n-m+1:n}-X_{n-m+1-j:n}\le a\}\\ &= \boldsymbol{P}\Big\{\frac{\sum_{i=n-m-j+2}^{n-m+1}E_i}{\sum_{i=1}^{n+1}E_i}\le a\Big\}\\ &= \boldsymbol{P}\{X_{j:n}\le a\}\\ &= \frac{n!}{(j-1)!(n-j)!}\int_0^a s^{j-1}(1-s)^{n-j}\,ds\end{aligned}$$

depending on n but not on m, if $j\le n-m$. Hence again

$$\begin{aligned}\boldsymbol{P}\{\mathbf{M}_{t,m}([0,a))>j\} &= \boldsymbol{P}\{\mathbf{K}_t(a,m)>j, N(t)\ge j+m\}\\ &= \sum_{n=j+m}^{\infty}\boldsymbol{P}\{X_{j:n}\le a\}\boldsymbol{P}\{N(t)=n\}\\ &= \boldsymbol{P}\{X_{j:N(t)}\le a, N(t)\ge j+m\}.\end{aligned}$$

Similarly we get for $1\le j\le m-1$

$$\begin{aligned}\boldsymbol{P}\{\mathbf{M}_{t,m}((-a,0])>j|N(t)=n\} &= \boldsymbol{P}\{X_{n-m+j+1:n}-X_{n-m+1:n}\le a\}\\ &= \boldsymbol{P}\{X_{j:n}\le a\}.\end{aligned}$$

The asymptotics of $\mathbf{M}_{t,m}([0,a)$ and $\mathbf{M}_{t,m}((-a,0])$ follows now easily by the properties of the order statistics $X_{j:n}$.

5. Proofs

Proof of Lemma 1 Let B be a Borel set of $[0,\infty)$. Rearranging the terms we may write

$$M_{n,m}(B)=\mathbf{1}(0\in B)+\sum_{i=1}^{n-m}\mathbf{1}(X_{n-m+1:n}-X_{i:n}\in B),\quad n>m,n,m\in\mathbb{N}.$$

For any $x \in \mathbb{R}$ such that $F(x) \in (0,1)$ the stochastic representation (cf. Reiss (1989) p. 52)

$$\Big((X_{1:n},\dots,X_{n-m:n})|X_{n-m+1:n}=x\Big) \stackrel{d}{=} (Y_{1:n-m},\dots,Y_{n-m:n-m})$$

holds, where the random variables $(Y_{1:n-m},\dots,Y_{n-m:n-m})$ are the order statistics of iid random variables $\eta_1^{[x]},\dots,\eta_{n-m}^{[x]}$ with distribution function $F_x(y) := F(y)/F(x), \forall y \le x$. If $B \subset (-\infty,0]$ we have

$$M_{n,m}(B) = \mathbf{1}(0 \in B) + \sum_{i=1}^{m-1} \mathbf{1}(X_{n-m+1:n} - X_{n-m+i+1:n} \in B),$$

hence (1) follows by conditioning on $X_{n-m+1:n}$. Since $\{N(t), t \ge 0\}$ is independent of the random sequence $X_i, i \ge 1$ the expression of the p.g.f. follows easily using (1). □

Proof of Theorem 2 The result in (16) follows along the same arguments as in (15). The limit of $G_K(\boldsymbol{\xi},\boldsymbol{\xi}^*,\boldsymbol{j},\boldsymbol{j}^*)$ as $j_{ik} \to \infty$ is a proper distribution function in $\mathbb{R}^{IK}$, hence $\{\widetilde{\mathbf{M}}_{t,k}((-\xi_{i,k}^*,0])\}_{1\le i\le I, 1\le k\le K}$ converge in distribution. If (17) holds, then it follows that $G_K(\boldsymbol{\xi},\boldsymbol{\xi}^*,\cdot,\cdot)$ is a proper distribution function in $\mathbb{R}^{2IK}$. Hence by the continuous mapping theorem the convergence of the point process in (18) follows, thus the proof is complete. □

Proof of Corollary 3 By the assumptions (11) is satisfied. Since $N(t)$ is independent of $X_i, i \ge 1$ and (5) then Proposition 2.2 of Hashorva (2003) implies (11) with $k = 2K$, and furthermore

$$(Y_1^*,\dots,Y_k^*) \stackrel{d}{=} (Z^\gamma Y_1 + \beta \ln Z,\dots, Z^\gamma Y_k + \beta \ln Z),$$

where $\gamma = 0, 1/\alpha, -1/\alpha$ if $H = \Lambda, \Phi_\alpha, \Psi_\alpha, \alpha > 0$, respectively and $\beta = 1$ if $H = \Lambda$ and 0 otherwise. Hence the result follows from Theorem 2. □

Proof of Corollary 4 In view of (9) we have

$$\boldsymbol{P}\{Y_i^* \le x\} = \boldsymbol{E}\{\Gamma_i(-Z \ln H(x))\}$$

for $x \in (\alpha_H, x_H)$ where $\Gamma_i(s) = \int_s^\infty t^{i-1}e^{-t}\,dt/\Gamma(i)$ is the upper tail of the standard Gamma distribution. Since for all $s > 0$

$$\Gamma_n(s) = \sum_{r=0}^{n-1} e^{-s}s^r/\Gamma(r+1) \to 1, \quad n \to \infty$$

the dominated convergence theorem yields

$$\lim_{n\to\infty} \boldsymbol{P}\{Y_n^* \le x\} = 1.$$

Consequently, if $H = \Lambda$ or $H = \Psi_\alpha$ we get the almost sure convergence

$$Y_n^* \stackrel{a.s.}{\to} \alpha_H = -\infty.$$

Thus the weak convergence follows by Theorem 2 using further Corollary 3.

Both (22) and (23) follow then using further (12), (13) and (19). In the following we show directly (23) for $H = \Lambda$ using (2). We may write for $s \in (0,1)$ and

$b > 0, b > a \geq 0$ (set $q := e^b - e^a$)

$$\begin{aligned}
&\lim_{t\to\infty} \boldsymbol{E}\{s^{\widetilde{\mathbf{M}}_{t,m}((a,b])-\mathbf{1}(a\in\{0\})}\} \\
&= \int_{\mathbb{R}} \left(\frac{H(x-b)}{H(x-a)}\right)^{1-s} d(\boldsymbol{P}\{Y_m \leq x\}) \\
&= \int_{\mathbb{R}} e^{-(1-s)qe^{-x}}\, d(\boldsymbol{P}\{Y_m \leq x\}) \\
&= -\int_0^\infty e^{-(1-s)qt}\, d\Big(\sum_{r=0}^{m-1} t^r e^{-t}/\Gamma(r+1)\Big) \\
&= \sum_{r=0}^{m-1} \frac{1}{\Gamma(r+1)} \int_0^\infty e^{-(1+(1-s)q)t} t^r\, dt - \sum_{r=1}^{m-1} \frac{1}{\Gamma(r)} \int_0^\infty e^{-(1+(1-s)q)t} t^{r-1}\, dt \\
&= \sum_{r=0}^{m-1} \left(\frac{1}{1+(1-s)q}\right)^{r+1} - \sum_{r=1}^{m-1} \left(\frac{1}{1+(1-s)q}\right)^{r} \\
&= \left(\frac{1}{1+(1-s)q}\right)^{m} = \left(\frac{[1+q]^{-1}}{1-sq/[1+q]}\right)^{m}.
\end{aligned}$$

The last claim on the independence of the random vectors $(U_2(a_2, b_2), \ldots, U_k(a_k, b_k))$ and $V_k(a_k, b_k), \ldots, V_{k+r}(a_{k+r}, b_{k+r}))$ follows easily by calculating the limit of the joint probability density function of the corresponding marginals, or using the stochastic representation (21) together with (20). □

References

[1] Balakrishnan, N., and Stepanov, A. (2004) A note on the paper of Khmaladze et al. *Statist. Probab. Lett.* **68**(4): 415-419.

[2] Balakrishnan, N., and Stepanov, A. (2005) A note on the number of observations near an order statistic. *J. Statist. Planning Infer.* **134**(1), 1–14.

[3] De Haan, L., and Ferreira, A. (2006) *Extreme Value Theorey. An Introduction.* Springer, New York.

[4] Dembinska, A., Stepanov, A., and Wesolowski, J. (2007) How many observations fall in a neighbourhood of an order statistic? *Comm. Stat - Theory Meth.* **36**(5), 851–868.

[5] Falk, M., Hüsler, J., and Reiss R.-D. (2004) *Laws of small numbers: extremes and rare events.* DMV Seminar **23**, Second Edition, Birkhäuser, Basel.

[6] Hashorva, E. (2003) On the number of near-maximum insurance claim under dependence. *Insurance: Mathematics and Economics*, **32**(1): 37–49.

[7] Hashorva, E. (2004) Bivariate maximum insurance claim and related point processes. *Statist. Prob. Letters*, **69**(2): 117–128.

[8] Hashorva, E. (2006) On the asymptotic distribution of certain bivariate reinsurance treaties. *www.arXiv:math.PR/0603719.*

[9] Hashorva, E., and Hüsler, J. (2000) On the number of near-maxima. *Suppl. Rendic. Circ. Matemat. Palermo,* Serie II, **65**, 121–136.

[10] Hashorva, E., and Hüsler, J. (2005) Estimation of tails and related quantities using the number of near-extremes. *Comm. Stat. Theory. Meth.* **34**,(2): 337–349.

[11] Hashorva, E., and Hüsler, J. (2008) On the near m-th extreme points and related sums. *Albanian J. Math.*, **1**,(3), 33–43.

[12] Leadbetter, M.R., Lindgren, G., and Rootzén, H. (1983) *Extremes and related properties of random sequences and processes.* Springer-Verlag, New York.

[13] Pakes, A.G., and Steutel, F.W. (1997) On the number of records near the maximum. *The Austral. J. Statist.* **39**, 172–192.

[14] Reiss, R-D. (1989) *Approximate Distributions of Order Statistics: With Applications to Nonparametric Statistics.* Springer, New York.

[15] Resnick, S.I. (1987) *Extreme Values, Regular Variation, and Point Processes*. Springer, New York.

N. Balakrishnan, Department of Mathematics and Statistics, McMaster University, 1280 Main Street West, Hamilton, Ontario, Canada L8S 4K1
E-mail address: bala@mcmail.cis.mcmaster.ca

E. Hashorva, University of Bern, Institute of Mathematical Statistics and Actuarial Sciences, Sidlerstrasse 5, CH-3012 Bern, Switzerland, and, Allianz Suisse Insurance Company, Laupenstrasse 27, CH-3001 Bern, Switzerland
E-mail address: enkelejd@stat.unibe.ch

J. Hüsler, University of Bern, Institute of Mathematical Statistics and Actuarial Sciences,, Sidlerstrasse 5, CH-3012 Bern, Switzerland
E-mail address: huesler@stat.unibe.ch

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 2, Pages 81–85
ISSN 1930-1235: (2009)

A REMARK ON GIUGA'S CONJECTURE AND LEHMER'S TOTIENT PROBLEM

WILLIAM D. BANKS, C. WESLEY NEVANS, AND CARL POMERANCE

Abstract. Giuga has conjectured that if the sum of the $(n-1)$-st powers of the residues modulo n is $-1 \pmod n$, then n is 1 or prime. It is known that any counterexample is a Carmichael number. Lehmer has asked if $\varphi(n)$ divides $n-1$, with φ being Euler's function, must it be true that n is 1 or prime. No examples are known, but a composite number with this property must be a Carmichael number. We show that there are infinitely many Carmichael numbers n that are not counterexamples to Giuga's conjecture and also do not satisfy $\varphi(n) \mid n-1$.

1. Introduction

1.1. **Carmichael numbers.** In a letter to Frenicle dated October 18, 1640, Fermat wrote that if p is a prime number, then p divides $a^{p-1}-1$ for any integer a not divisible by p. This result, known as *Fermat's little theorem*, is equivalent to the statement:

$$a^p \equiv a \pmod p \qquad \text{for all } a \in \mathbb{Z}.$$

Almost three centuries later, Carmichael [5] began an in-depth study of *composite* natural numbers n with the property that

$$a^n \equiv a \pmod n \qquad \text{for all } a \in \mathbb{Z};$$

these are now called *Carmichael numbers*. More than eighty years elapsed after Carmichael's initial investigations before the existence of infinitely many Carmichael numbers was established by Alford, Granville, and Pomerance [1]. Denoting by $\mathcal{C}$ the set of Carmichael numbers, it is shown in [1] that for every $\varepsilon > 0$ and all sufficiently large X, the lower bound

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C}\}\big| \geqslant X^{\beta-\varepsilon} \tag{1}$$

holds, where

$$\beta = \beta_0 = \frac{5}{12}\left(1 - \frac{1}{2\sqrt{e}}\right) = 0.290306\cdots > \frac{2}{7}\,.$$

More recently, Harman [7] has shown that the lower bound (1) holds with the larger constant $\beta = \beta_1 = 0.3322408$.

The purpose of the present note is to show that the bound (1) with $\beta = \beta_1$ also holds with a set of Carmichael numbers $n \leqslant X$ that are consistent with *Giuga's conjecture* and support the nonexistence of examples to *Lehmer's totient problem*. Our results are described in more detail below.

2000 *Mathematics Subject Classification.* Primary 11A07; Secondary 11N25.

1.2. **Giuga's conjecture.** Fermat's little theorem implies

$$p \mid 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} + 1$$

for every prime p. In 1950, Giuga [6] conjectured that the converse is true, i.e., that there are no *composite* natural numbers n for which

$$1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} \equiv -1 \pmod{n},$$

and he verified this conjecture for all $n \leqslant 10^{1000}$. Any counterexample to Giuga's conjecture is called a *Giuga number*.

Denoting by $\mathcal{G}$ the (presumably empty) set of Giuga numbers, Giuga showed that $n \in \mathcal{G}$ if and only if n is composite and

$$p^2(p-1) \mid n - p \qquad \text{for every prime } p \text{ dividing } n. \tag{2}$$

As this condition implies that n is squarefree, every Giuga number is a Carmichael number in view of the following criterion.

Korselt's criterion. *For a positive integer n, $a^n \equiv a \pmod{n}$ for all integers a if and only if n is squarefree and $p-1$ divides $n-1$ for every prime p dividing n.*

The condition (2) appears to be a much stronger requirement for a composite natural number n to satisfy than Korselt's criterion, thus it is reasonable to expect that there are infinitely many Carmichael numbers which are *not* Giuga numbers. Indeed, it is widely believed (see [1]) that

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C}\}\big| = X^{1+o(1)} \qquad \text{as } X \to \infty,$$

whereas Luca, Pomerance and Shparlinski [10] have established the bound

$$\big|\{n \leqslant X \ : \ n \in \mathcal{G}\}\big| \ll \frac{X^{1/2}}{(\log X)^2}\,, \tag{3}$$

improving slightly on a result of Tipu [15]. However, the result that $\mathcal{C} \setminus \mathcal{G}$ is an infinite set does not follow from (3) and the unconditional bound (1) with $\beta = \beta_1$. Nevertheless, we are able to prove the following result.

Theorem 1. *For any fixed $\varepsilon > 0$ and all sufficiently large X, we have*

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C} \setminus \mathcal{G}\}\big| \geqslant X^{\beta_1 - \varepsilon}.$$

It is known that if n is a Giuga number, then

$$-\frac{1}{n} + \sum_{p \mid n} \frac{1}{p} \in \mathbb{N}. \tag{4}$$

There are known composites that satisfy (4), for example $n = 30$. A *weak Giuga number* is a composite number n satisfying (4). Denoting by $\mathcal{W}$ the set of weak Giuga numbers, we have $\mathcal{G} \subset \mathcal{W}$, hence Theorem 1 is an immediate consequence of the following theorem.

Theorem 2. *For any fixed $\varepsilon > 0$ and all sufficiently large X, we have*

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C} \setminus \mathcal{W}\}\big| \geqslant X^{\beta_1 - \varepsilon}.$$

Our proof of Theorem 2 is given in §2 below.

1.3. **Lehmer's totient problem.** Let φ denote *Euler's function*. In 1932, Lehmer [8] asked whether there are any *composite* natural numbers n for which $\varphi(n) \mid n-1$. This question, known as Lehmer's totient problem, remains unanswered to this day.

Denote by $\mathcal{L}$ the (possibly empty) set of composite natural numbers n such that $\varphi(n) \mid n-1$. It follows easily from Euler's theorem that every element of $\mathcal{L}$ is a Carmichael number. On the other hand, one expects that there are infinitely many Carmichael numbers which do *not* lie in $\mathcal{L}$.

In a series of papers (see [11, 12, 13]), Pomerance considered the problem of bounding the number of natural numbers $n \leqslant X$ that lie in $\mathcal{L}$. In his third paper [13], he established the bound

$$\big|\{n \leqslant X \ : \ n \in \mathcal{L}\}\big| \ll X^{1/2}(\log X)^{3/4}. \tag{5}$$

Refinements of the underlying method of [13] led to subsequent improvements of the bound (5) by Shan [14], Banks and Luca [4], Banks, Güloğlu and Nevans [3], and Luca and Pomerance [9]; however, it is still unknown whether the bound

$$\big|\{n \leqslant X \ : \ n \in \mathcal{L}\}\big| \ll X^{\alpha}$$

holds with some constant $\alpha < 1/2$. In particular, the result that $\mathcal{C} \setminus \mathcal{L}$ is an infinite set does not follow from only the unconditional bound (1) with $\beta = \beta_1$. In this note we prove the following theorem.

Theorem 3. *For any fixed $\varepsilon > 0$ and all sufficiently large X, we have*

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C} \setminus \mathcal{L}\}\big| \geqslant X^{\beta_1 - \varepsilon}.$$

Our proof of Theorem 3 is given in §2 below.

2. Construction

Let $\mathcal{N}$ denote the set of composite natural numbers n such that

$$\sum_{p \,|\, n} \frac{1}{p} < \frac{1}{3}\,.$$

Lemma 1. *The sets $\mathcal{N}$ and $\mathcal{W}$ are disjoint.*

Proof. Let $n \in \mathcal{N}$. Since

$$\frac{1}{n} < \sum_{p \,|\, n} \frac{1}{p} < \frac{1}{3} < 1 + \frac{1}{n}\,,$$

it is clear that

$$\sum_{p \,|\, n} \frac{1}{p} \not\equiv \frac{1}{n} \pmod 1,$$

hence n is not a weak Giuga number. □

Lemma 2. *The sets $\mathcal{N}$ and $\mathcal{L}$ are disjoint.*

Proof. Let $n \in \mathcal{N}$. Using the inequality

$$\log(1-t) > -2\,t \qquad (0 < t \leqslant 1/2),$$

we have

$$\log \frac{\varphi(n)}{n} = \log \prod_{p \,|\, n} \left(1 - \frac{1}{p}\right) = \sum_{p \,|\, n} \log\left(1 - \frac{1}{p}\right) > -2 \sum_{p \,|\, n} \frac{1}{p} > -\frac{2}{3}\,.$$

Consequently,

$$\frac{n-1}{\varphi(n)} < \frac{n}{\varphi(n)} < e^{2/3} < 2, \tag{6}$$

and it follows that $n \notin \mathcal{L}$. Indeed, (6) and the condition $\varphi(n) \mid n-1$ together imply that $n = 1$ or $\varphi(n) = n-1$, which possibilities cannot occur for a composite natural number n. □

In view of Lemmas 1 and 2, Theorems 2 and 3 follow from the following result.

Theorem 4. *For any fixed $\varepsilon > 0$ and all sufficiently large X, we have*

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C} \cap \mathcal{N}\}\big| \geqslant X^{\beta_1 - \varepsilon}.$$

Proof. With the existing proofs of the infinitude of Carmichael numbers given in [1] and [7], a careful reading, or with small changes, shows that the Carmichael numbers constructed lie in $\mathcal{N}$. Since Harman [7, Theorem 1] has the stronger result, we give the details on how that proof supports our assertion. As mentioned, he has shown that for every $\varepsilon > 0$ and all sufficiently large X, the lower bound

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C}\}\big| \geqslant X^{\beta_1 - \varepsilon} \tag{7}$$

holds. To prove Theorem 4, it suffices to show that the Carmichael numbers constructed by Harman all lie in $\mathcal{N}$ if X is large enough. We begin with the following statement, which is [7, Theorem 3].

Lemma 3. *Let $\varepsilon > 0$, and suppose $y \geqslant y_0(\varepsilon)$. Put*

$$\delta = \frac{\varepsilon\,\theta}{1.888}, \qquad x = \exp\big(y^{1+\delta}\big), \qquad \theta = \frac{1}{0.2961}.$$

Then there is a positive integer $k < x^{0.528}$ and a set of squarefree numbers $\mathcal{B}$ such that

- (i) $\mathcal{B} \subset [x^{0.4}, x^{0.472}]$;
- (ii) $|\mathcal{B}| > x^{\beta_1 - \varepsilon}$;
- (iii) $dk+1$ *is prime for every* $d \in \mathcal{B}$;
- (iv) *if* $p \mid d$, *then*

$$0.5\,y^{\theta} < p < y^{\theta}, \qquad p \nmid k, \qquad P(p-1) < y,$$

where $P(n)$ denotes the greatest prime factor of n.

Let n be one of the Carmichael numbers constructed in [7, Theorem 1]. Such a number n is composed of at most $t = \exp\big(y^{1+\delta/2}\big)$ primes of the form $p = dk+1$ with $d \in \mathcal{B}$, so that

- $n \leqslant X$, where $X = x^t$;
- $p \geqslant x^{0.4}$ for every prime $p \mid n$.

Taking into account that $t = x^{o(1)}$ as $x \to \infty$, it follows that

$$\sum_{p \mid n} \frac{1}{p} \leqslant t\,x^{-0.4} < \frac{1}{3}$$

if x is sufficiently large. Since the value of x is determined uniquely by X, this shows that the Carmichael number n lies in $\mathcal{N}$ once X is large enough, completing the proof. □

We remark that in [2] it is shown that for each fixed k there are infinitely many Carmichael numbers n with $\sum_{p \mid n} 1/p < 1/(\log n)^k$. This result too supports our principal assertion that $\mathcal{C} \cap \mathcal{N}$ is infinite, but the bound for the counting function proved here is even smaller than that given in [1]. On the other hand, it is not known if there is some $\varepsilon > 0$ such that for infinitely many Carmichael numbers n we have $\sum_{p \mid n} 1/p > \varepsilon$. In particular, it is not known if the set $\mathcal{C} \setminus \mathcal{N}$ is infinite.

Acknowledgment. The third author was supported in part by NSF grant DMS-0703850.

References

[1] W. Alford, A. Granville and C. Pomerance, 'There are infinitely many Carmichael numbers,' *Ann. of Math. (2)* **139** (1994), no. 3, 703–722.

[2] W. Alford, A. Granville and C. Pomerance, 'On the difficulty of finding reliable witnesses,' in Algorithmic Number Theory Proceedings (ANTS-I), Lecture Notes in Computer Sci. **877** (1994), Springer-Verlag, Berlin, pp. 1–16.

[3] W. Banks, A. Güloğlu and W. Nevans, 'On the congruence $n \equiv a \pmod{\varphi(n)}$,' *Integers* **8(1)** (2008), A59, 8 pp. (electronic)

[4] W. Banks and F. Luca, 'Composite integers n for which $\varphi(n) \mid n-1$,' *Acta Math. Sinica, English Series* **23** (2007), no. 10, 1915–1918.

[5] R. D. Carmichael, 'Note on a new number theory function,' *Bull. Amer. Math. Soc.* **16** (1910), no. 5, 232–238.

[6] G. Giuga, 'Su una presumible proprietá caratteristica dei numeri primi,' *Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat.* **14(83)** (1950), 511–528.

[7] G. Harman, 'On the number of Carmichael numbers up to x,' *Bull. London Math. Soc.* **37** (2005), 641–650.

[8] D. H. Lehmer, 'On Euler's totient function,' *Bull. Amer. Math. Soc.* **38** (1932), 745–757.

[9] F. Luca and C. Pomerance, 'On composite integers n for which $\phi(n) \mid n-1$,' preprint, 2009.

[10] F. Luca, C. Pomerance and I. Shparlinski, 'On Giuga numbers,' *Int. J. Mod. Math.* **4** (2009), 13–28.

[11] C. Pomerance, 'On the congruences $\sigma(n) \equiv a \pmod{n}$ and $n \equiv a \pmod{\varphi(n)}$,' *Acta Arith.* **26** (1974/75), no. 3, 265–272.

[12] C. Pomerance, 'On composite n for which $\varphi(n) \mid n-1$,' *Acta Arith.* **28** (1975/76), no. 4, 387–389.

[13] C. Pomerance, 'On composite n for which $\varphi(n) \mid n-1$, II,' *Pacific J. Math.* **69** (1977), no. 1, 177–186.

[14] Z. Shan, 'On composite n for which $\varphi(n) \mid n-1$,' *J. China Univ. Sci. Tech.* **15** (1985), 109–112.

[15] V. Tipu, 'A note on Giuga's conjecture,' *Canad. Math. Bull.* **50** (2007), 158–160.

Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
E-mail address: bankswd@missouri.edu

Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
E-mail address: cwnxxb@mizzou.edu

Mathematics Department, Dartmouth College, Hanover, NH 03755 USA
E-mail address: carl.pomerance@dartmouth.edu

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 87–94
ISSN 1930-1235: (2009)

AUXILIARY PRINCIPLE TECHNIQUE FOR NONCONVEX VARIATIONAL INEQUALITIES

MUHAMMAD ASLAM NOOR

Abstract. In this paper, we suggest and analyze some iterative methods for solving nonconvex variational inequalities using the auxiliary principle technique, the convergence of these methods either requires only pseudomonotonicity or partially relaxed strongly monotonicity. Our proofs of convergence are very simple. As special cases, we obtain earlier known results for solving variational inequalities involving the convex sets.

1. Introduction

Variational inequalities theory, which was introduced by Stampacchia [30], can be viewed as an important and significant extension of the variational principles, the origin of which can be traced back to Fermat, Bernoulli brother, Euler, Lagrange. This provides us with a simple, general and unified framework to study a wide class of problems arising in pure and applied sciences. This theory combines the theory of extremal problems and monotone operators under a unified viewpoint. It is perhaps part of the fascinating of this theory that so many branches of pure and applied sciences are involved. During the last five decades, there has been considerable activity in the development of numerical techniques for solving variational inequalities. There are a substantial number of numerical methods including projection method and its variant forms, Wiener-Hopf equations, auxiliary principle, and descent framework for solving variational inequalities and complementarity problems; see [1,2,4-28]. It is worth mentioning that almost all the results regarding the existence and iterative schemes for solving variational inequalities and related optimization problems are being considered in the convexity setting. This is because all the techniques are based on the properties of the projection operator over convex sets, which may not hold in general, when the sets are nonconvex. In recent years, Noor [13, 18-21,24], Bounkhel et al [2] and Pang et al [28] have considered variational inequality in the context of uniformly prox-regular sets. They have shown that the nonconvex variational inequalities are equivalent to the fixed point problems using the projection techniques. They have used this alternative equivalent formulation to suggest and analyze some projection-type iterative schemes for solving nonconvex variational inequalities. It has been shown that the convergence of these projection-type methods requires that the operator must be both strongly

Received by the editors April 2, 2009 .
2000 *Mathematics Subject Classification.* Primary 49J40; Secondary 90C33.
Key words and phrases. Variational inequalities; nonconvex functions; auxiliary principle technique, convergence.

monotone and Lipschitz continuous. These strict conditions rule out many its applications. Secondly it is very difficult to evaluate the projection of the space onto the uniformly prox-regular sets. To overcome this drawback, we use the auxiliary principle technique, which is mainly due to Glowinski, Lions and Tremolieres [5]. Noor [10-15, 24] has used this technique to develop some iterative schemes for solving various classes of variational inequalities. We point out that this technique does not involve the projection of the operator and is flexible. In this paper, we show that the auxiliary principle technique can be used to suggest and analyze a class of iterative methods for solving nonconvex variational inequalities. We also prove that the convergence of these new methods either require pseudomonotonicity or partially relaxed strongly monotonicity, which are weaker conditions. In this respect, our results represent an improvement and refinement of the known results for nonconvex variational inequalities.

2. Preliminaries

Let H be a real Hilbert space whose inner product and norm are denoted by $\langle \cdot, \cdot \rangle$ and $\|.\|$ respectively. Let K be a nonempty and convex set in H.

We, first of all, recall the following well-known concepts from nonlinear convex analysis and nonsmooth analysis [3,29].

Definition 2.1. The proximal normal cone of K at $u \in H$ is given by

$$N_K^P(u) := \{\xi \in H : u \in P_K[u + \alpha\xi]\},$$

where $\alpha > 0$ is a constant and

$$P_K[u] = \{u^* \in K : d_K(u) = \|u - u^*\|\}.$$

Here $d_K(.)$ is the usual distance function to the subset K, that is

$$d_K(u) = \inf_{v \in K} \|v - u\|.$$

The proximal normal cone $N_K^P(u)$ has the following characterization.

Lemma 2.1. Let K be a nonempt, closed and convex subset in H. Then $\zeta \in N_K^P(u)$ if and only if there exists a constant $\alpha > 0$ such that

$$\langle \zeta, v - u \rangle \leq \alpha \|v - u\|^2, \quad \forall v \in K.$$

Definition 2.2. The Clarke normal cone, denoted by $N_K^C(u)$, is defined as

$$N_K^P(u) = \overline{co}[N_K^P(u)],$$

where $\overline{co}$ means the closure of the convex hull. Clearly $N_K^P(u) \subset N_K^C(u)$, but the converse is not true. Note that $N_K^P(u)$ is always closed and convex, whereas $N_K^C(u)$ is convex, but may not be closed, see [29].

Poliquin et al. [29] and Clarke et al [3] have introduced and studied a new class of nonconvex sets, which are called uniformly prox-regular sets. This class of uniformly prox-regular sets has played an important part in many nonconvex applications such as optimization, dynamic systems and differential inclusions.

Definition 2.3. For a given $r \in (0, \infty]$, a subset K_r is said to be normalized uniformly r-prox-regular if and only if every nonzero proximal normal to K_r can be realized by an r-ball, that is, $\forall u \in K_r$ and $0 \neq \xi \in N_{K_r}^P(u)$, one has

$$\langle (\xi)/\|\xi\|, v - u \rangle \leq (1/2r)\|v - u\|^2, \quad \forall v \in K.$$

It is clear that the class of normalized uniformly prox-regular sets is sufficiently large to include the class of convex sets, p-convex sets, $C^{1,1}$submanifolds (possibly with boundary) of H, the images under a $C^{1,1}$ diffeomorphism of convex sets and many other nonconvex sets; see [3,29]. It is clear that if $r = \infty$, then uniformly prox-regularity of K_r is equivalent to the convexity of K. It is known that if K_r is a uniformly prox-regular set, then the proximal normal cone $N^P_{K_r}(u)$ is closed as a set-valued mapping.

For a given nonlinear operator T, we consider the problem of finding $u \in K_r$ such that

$$\langle Tu, v - u\rangle \geq 0, \quad \forall v \in K_r, \tag{1}$$

which is called the *nonconvex variational inequality,* which was introduced and studied by Noor [18-21,24]. See also [2, 27] for the variant forms of nonconvex variational inequalities.

We note that, if $K_r \equiv K$, the convex set in H, then problem (2.1) is equivalent to finding $u \in K$ such that

$$\langle Tu, v - u\rangle \geq 0, \qquad \forall v \in K. \tag{2}$$

Inequality of type (2) is called the *variational inequality*, which was introduced and studied by Stampacchia [30] in 1964. It turned out that a number of unrelated obstacle, free, moving, unilateral and equilibrium problems arising in various branches of pure and applied sciences can be studied via variational inequalities, see [1-30] and the references therein.

It is well-known that problem (2) is equivalent to finding $u \in K$ such that

$$0 \in Tu + N_K(u), \tag{3}$$

where $N_K(u)$ denotes the normal cone of K at u in the sense of convex analysis. Problem (3) is called the variational inclusion associated with variational inequality (2).

Similarly, if K_r is a nonconvex (uniformly prox-regular) set, then problem (1) is equivalent to finding $u \in K_r$ such that

$$0 \in Tu + N^P_{K_r}(u), \tag{4}$$

where $N^P_{K_r}(u)$ denotes the normal cone of K_r at u in the sense of nonconvex analysis. Problem (4) is called the nonconvex variational inclusion problem associated with nonconvex variational inequality (1). This implies that the variational inequality (1) is equivalent to finding a zero of the sum of two monotone operators (4).

3. Main Results

In this section, we use the auxiliary principle technique of Glowinski, Lions and Tremolieres [5] to suggest and analyze a some iterative methods for solving the nonconvex variational inequality (1). The main advantage of this technique does not involve the concept of the projection, which is the main advantage of this technique.

For a given $u \in K_r$, a uniformly prox-regular set in H, consider the problem of finding a u solution $w \in K_r$ such that

$$\langle \rho Tw + w - u, v - w\rangle \geq 0, \quad \forall v \in K_r, \tag{5}$$

where $\rho > 0$ is a constant. Inequality of type (5) is called the auxiliary nonconvex variational inequality. Note that if $w = u$, then w is a solution of (1). This simple observation enables us to suggest the following iterative method for solving the nonconvex variational inequalities (1).

Algorithm 3.1. For a given $u_0 \in K_r$, compute the approximate solution u_{n+1} by the iterative scheme

$$\langle \rho T u_{n+1} + u_{n+1} - u_n, v - u_{n+1} \rangle \geq 0, \quad \forall v \in K_r. \tag{6}$$

Algorithm 3.1 is called the proximal point algorithm for solving noconvex variational inequality (1). In particular, if $r = \infty$, then the uniformly prox-regular set K_r becomes the standard convex set K, and consequently Algorithm 3.1 reduces to:

Algorithm 3.2. For a given $u_0 \in K$, compute the approximate solution u_{n+1} by the iterative scheme

$$\langle \rho T u_{n+1} + u_{n+1} - u_n, v - u_{n+1} \rangle \geq 0, \quad \forall v \in K,$$

which is known as the proximal point algorithm for solving variational inequalities (2) and has been studied extensively, see [2,4-27].

For the convergence analysis of Algorithm 3.1, we recall the following concepts and results.

Definition 3.1. For all $u, v, z \in H$, an operator $T : H \to H$ is said to be:
(i) *monotone*, if

$$\langle Tu - Tv, u - v \rangle \geq 0.$$

(ii) *pseudomonotone*, if

$$\langle Tu, v - u \rangle \geq 0 \quad \text{implies that} \quad \langle Tv, u - v \rangle \leq 0.$$

(iii) *partially relaxed strongly monotone,* if there exists a constant $\alpha > 0$ such that

$$\langle Tu - Tv, z - v \rangle \geq -\alpha \|z - u\|^2.$$

Note that for $z = u$, partially relaxed strongly monotonicity reduces to monotonicity. It is known that cocoercivity implies partially relaxed strongly monotonicity, but the converse is not true. It is known that monotonicity implies pseudomonotonicity; but the converse is not true. Consequently, the class of pseudomonotone operators is bigger than the one of monotone operators.

Lemma 3.1. $\forall u, v \in H$,

$$2\langle u, v \rangle = \|u + v\|^2 - \|u\|^2 - \|v\|^2. \tag{7}$$

We now consider the convergence criteria of Algorithm 3.1. The analysis is in the spirit of Noor [13,14,15,24].

Theorem 3.1. Let the operator $T : K_r \longrightarrow H$ be pseudomonotone. If u_{n+1} is the approximate solution obtained from Algorithm 3.2 and $u \in K_r$ is a solution of (1), then

$$\|u - u_{n+1}\|^2 \leq \|u - u_n\|^2 - \|u_n - u_{n+1}\|^2. \tag{8}$$

Proof. Let $u \in K_r$ be a solution of (1). Then

$$\langle Tv, v - u \rangle \geq 0, \quad \forall v \in K_r, \tag{9}$$

since T is pseudomonotone.

Taking $v = u_{n+1}$ in (5), we have

$$\langle Tu_{n+1}, u_{n+1} - u\rangle \geq 0. \tag{10}$$

Setting $v = u$ in (6), and using (10), we have

$$\langle u_{n+1} - u_n, u - u_{n+1}\rangle \geq \rho\langle Tu_{n+1}, u_{n+1} - u\rangle \geq 0. \tag{11}$$

Setting $v = u - u_{n+1}$ and $u = u_{n+1} - u_n$ in (7), we obtain

$$2\langle u_{n+1} - u_n, u - u_{n+1}\rangle = \|u - u_n\|^2 - \|u_n - u_{n+1}\|^2 - \|u - u_{n+1}\|^2. \tag{12}$$

From (11) and (12), we obtain (8), the required result. □

Theorem 3.2. Let H be a finite dimension subspace and let u_{n+1} be the approximate solution obtained from Algorithm 3.1. If $u \in K_1$ is a solution of (1), then $\lim_{n\longrightarrow\infty} u_n = u$.

Proof. Let $u \in K_r$ be a solution of (1). Then it follows from (8) that the sequence $\{u_n\}$ is bounded and

$$\sum_{n=0}^{\infty} \|u_n - u_{n+1}\|^2 \leq \|u_0 - u\|^2,$$

which implies that

$$\lim_{n\longrightarrow\infty} \|u_n - u_{n+1}\| = 0. \tag{13}$$

Let $\hat{u}$ be a cluster point of the sequence $\{u_n\}$ and let the subsequence $\{u_j\}$ of the sequence $\{u_n\}$ converge to $\hat{u} \in K_r$. replacing u_n by u_{n_j} in (6) and taking the limit $n_j \longrightarrow \infty$ and using (13), we have

$$\langle T\hat{u}, v - \hat{u}\rangle \geq 0, \quad \forall \quad v \in K_r,$$

which implies that $\hat{u}$ solves the nonconvex variational inequality (1) and

$$\|u_n - u_{n+1}\|^2 \leq \|\hat{u} - u_n\|^2.$$

Thus it follows from the above inequality that the sequence $\{u_n\}$ has exactly one cluster point $\hat{u}$ and $\lim_{n\longrightarrow\infty} u_n = \hat{u}$. the required result. □

We note that for $r = \infty$, the r-prox-regular set K becomes a convex set and nonconvex variational inequality (1) collapses to variational inequality (2). Thus our results include the previous known results as special cases.

It is well-known that to implement the proximal point methods, one has to calculate the approximate solution implicitly, which is in itself a difficult problem. To overcome this drawback, we suggest another iterative method, the convergence of which requires only partially relaxed strongly monotonicity, which is a weaker condition that cocoercivity.

For a given $u \in K_r$, consider the problem of finding $w \in K_r$ such that

$$\langle \rho Tu + w - u, v - w\rangle \geq 0, \quad \forall \quad v \in K_r, \tag{14}$$

which is also called the auxiliary variational inequality. Note that problems (6) and (14) are quite different. If $w = u$, then clearly w is a solution of the nonconvex variational inequality (1). This fact enables us to suggest and analyze the following iterative method for solving the nonconvex variational inequality (1).

Algorithm 3.3. For a given $u_0 \in K_r$, compute the approximate solution u_{n+1} by the iterative scheme

$$\langle \rho T u_n + u_{n+1} - u_n, v - u_{n+1} \rangle \geq 0, \quad \forall v \in K_r. \tag{15}$$

Note that for $r = \infty$, the uniformly prox-regular set K_r becomes a convex set K and Algorithm 3.3 reduces to:

Algorithm 3.4. For a given $u_0 \in K$, calculate the approximate solution u_{n+1} by the iterative scheme

$$\langle \rho T u_n + u_{n+1} - u_n, v - u_{n+1} \rangle \geq 0, \quad \forall v \in K,$$

or equivalently

$$u_{n+1} = P_K[u_n - \rho T u_n], \quad n = 0, 1, 2, \ldots,$$

which is known as the projection iterative method for solving convex variational inequalities (2) and have been studied extensively.

We now study the convergence of Algorithm 3.3 and this is the main motivation of our next result.

Theorem 3.3. Let the operator T be partially relaxed strongly monotone with constant $\alpha > 0$. If u_{n+1} is the approximate solution obtained from Algorithm 3.3 and $u \in K_r$ is a solution of (1), then

$$\|u - u_{n+1}\|^2 \leq \|u - u_n\|^2 - \{1 - 2\rho\alpha\}\|u_n - u_{n+1}\|^2. \tag{16}$$

Proof. Let $u \in K_r$ be a solution of (1). Then

$$\langle Tu, v - u \rangle \geq 0, \quad \forall \quad v \in K_r. \tag{17}$$

Taking $v = u_{n+1}$ in (17), we have

$$\langle Tu, u_{n+1} - u \rangle \geq 0. \tag{18}$$

Letting $v = u$ in (15), we obtain

$$\langle \rho T u_n + u_{n+1} - u_n, u - u_{n+1} \rangle \geq 0,$$

which implies that

$$\begin{aligned} \langle u_{n+1} - u_n, u - u_{n+1} \rangle &\geq \langle \rho T u_n, u_{n+1} - u \rangle \\ &\geq \rho \langle T u_n - T u, u_{n+1} - u \rangle \\ &\geq -\alpha\rho \|u_n - u_{n+1}\|^2. \end{aligned} \tag{19}$$

since T is partially relaxed strongly monotone with constant $\alpha > 0$.

Combining (19) and (12), we obtain the required result (16). □

Using essentially the technique of Theorem 3.2, one can study the convergence analysis of Algorithm 3.3.

Acknowledgement. The author would like to express his gratitude to Dr. M. Junaid Zaidi, Rector, CIIT, for providing excellent research facilities.

References

[1] H. Brezis, Operateurs maximaux monotone, Mathematical Studies, No. 5, North-Holland, 1973.

[2] M. Bounkhel, L. Tadji and A. Hamdi, Iterative schemes to solve nonconvex variational problems, J. Inequal. Pure Appl. Math.,**4**(2003), 1-14.

[3] F. H. Clarke, Y. S. Ledyaev and P. R. Wolenski, Nonsmooth Analysis and Control Theory, Springer-Verlag, Berlin, 1998.

[4] D. Kinderlehrer and G. Stampacchia, An Introduction to Variational Inequalities and Their Applications, SIAM, Philadelphia, 2000.

[5] R. Glowinski, J. L. Lions and R. Tremolieres, Numerical Analysis of Variational Inequalities, North-Holland, Amsterdam, Holland, 1981.

[6] M. Aslam Noor, On Variational Inequalities, PhD Thesis, Brunel University, London, UK, 1975.

[7] M. Aslam Noor, General variational inequalities, Appl. Math. Letters, **1**(1988), 119-121.

[8] M. Aslam Noor, Quasi variational inequalities, Appl. Math. Letters, **1**(1988), 367-370.

[9] M. Aslam Noor, Wiener-Hopf equations and variational inequalities, J. Optim. Theory Appl. **79**(1993), 197-206.

[10] M. Aslam Noor, Some recent advances in variational inequalities, Part II, other concepts, New Zealand J. Math. **26**(1997), 229-255.

[11] M. Aslam Noor, New approximation schemes for general variational inequalities, J. Math. Anal. Appl. , **251**(2000), 217-229.

[12] M. Aslam Noor, Some developments in general variational inequalities, Appl. Math. Computation, **152**(2004), 199-277.

[13] M. Aslam Noor, Iterative schemes for nonconvex variational inequalities, J. Optim. Theory Appl. **121**(2004), 385-395.

[14] M. Aslam Noor, Fundamentals of mixed quasi variational inequalities, Inter. J. Pure Appl. Math. **15**(2004), 137-258.

[15] M. Aslam Noor, Fundamentals of equilibrium problems, Math. Inequal. Appl. **9**(2006), 529-566.

[16] M. Aslam Noor, Merit functions for general variational inequalities, J. Math. Anal. Appl. **316**(2006), 736-752.

[17] M. Aslam Noor, Differentiable nonconvex functions and general variational inequalities, Appl. Math. Computation, **199** (2008), 623-630

[18] M. Aslam Noor, Some iterative methods for general nonconvex variational inequalities, Comput. Math. Modeling, **21**(2010).

[19] M. Aslam Noor, Projection methods for nonconvex variational inequalities, Optim. Letters, **3**(2009), 411-418.

[20] M. Aslam Noor, Implicit Iterative Methods for Nonconvex Variational Inequalities, J. Optim. Theory Appl. DOI 10.1007/s10957-009-9567-7

[21] M. Aslam Noor, Iterative methods for general nonconvex variational inequalities, Albanian J. Math. **3**(2009).

[22] M. Aslam Noor, On a class of general variational inequalities, J. Advanced Math. Studies, **1**(2008), 75-86.

[23] M. Aslam Noor, Extended general variational inequalities, Appl. Math. Letters, **22**(2009), 182-186.

[24] M. Aslam Noor, Variational Inequalities and Applications, Lecture Notes, Mathematics Department, COMSATS Institute of Information Technology, Islamabad, Pakistan, 2007-2009.

[25] M. Aslam Noor and K. Inayat Noor, Projection algorithms for solving system of general variational inequalities, Nonl. Anal. **70**(2009), 2700-2706.

[26] M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Some aspects of variational inequalities, J. Comput. Appl. Math. **47**(1993), 285-312.

[27] M. Aslam Noor, K. Inayat Noor and H. Yaqoob, On general mixed variational inequalities, Acta Appl. Math. (2008), DOI 10.1007/s10440-008-9402.4

[28] L. P. Pang, J. Shen and H. S. Song, A modified predictor-corrector algorithm for solving nonconvex generalized variational inequalities, Computers Math. Appl. **54**(2007), 319-325.

[29] R. A. Poliquin, R. T. Rockafellar and L. Thibault, Local differentiability of distance functions, Trans. Amer. Math. Soc., **352**(2000), 5231-5249.

[30] G. Stampacchia, Formes bilineaires coercitives sur les ensembles convexes, C. R. Acad. Sci, Paris, **258**(1964), 4413-4416

COMSATS Institute of Information Technology, Mathematics Department, Islamabad, Pakistan
E-mail address: noormaslam@gmail.com and noormaslam@hotmail.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 3, Pages 95–105
ISSN 1930-1235: (2009)

FIELDS GENERATED BY ROOTS OF $x^n + ax + b$

Mohamed Ayad
Laboratoire de Mathématiques Pures et Appliquées
Université du Littoral
F-62228 Calais, France
ayad@lmpa.univ-littoral.fr

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

1. Introduction

Let $n \geq 2$ be a fixed integer. Let a and b be integers and put $f_{a,b}(X) = X^n + aX + b$. Let $\theta_{a,b}^{(1)}, \ldots, \theta_{a,b}^{(n)}$ be all the roots of $f_{a,b}(X)$. In this paper, we investigate the properties of the fields $\mathbb{Q}(\theta_{a,b}^{(i)})$ for $i = 1, \ldots, n$, as the pair (a, b) ranges in $(\mathbb{Z} \cap [-T, T])^2$, where T is some positive real number. Given the pair (a, b), there are at most n distinct fields among $\mathbb{Q}(\theta_{a,b}^{(i)})$ for $i = 1, \ldots, n$. Clearly, there are $(2T + O(1))^2 = 4T^2 + O(T)$ pairs of positive integers (a, b) both in $[-T, T]$. The first question we ask is for how many of such pairs is one of the fields $\mathbb{Q}(\theta_{a,b}^{(i)})$ for some $i = 1, \ldots, n$ (hence, for all such i) of degree n over $\mathbb{Q}$, or, equivalently, for how many such pairs (a, b) is $f_{a,b}(X) \in \mathbb{Q}[X]$ irreducible? Note that by choosing pairs (a, b) such that $p \| b$ and $a \equiv 0 \pmod{p}$ for some prime p, the polynomials $f_{a,b}(X)$ are irreducible by Eisenstein's criterion. However, this gives us only a positive proportion of pairs (a, b) of integers in $[-T, T]$. In fact, as $T \to \infty$, $(6/\pi^2 + o(1))(2T)^2$ of the pairs (a, b) have the property that a and b are coprime, therefore the above argument will not work for them. Our first result shows that $f_{a,b}(X) \in \mathbb{Q}[X]$ is irreducible for almost all pairs $(a, b) \in (\mathbb{Z} \cap [-T, T])^2$.

Theorem 1. *Assume that $n \geq 2$. The set of pairs $(a, b) \in (\mathbb{Z} \cap [-T, T])^2$ such that $f_{a,b} \in \mathbb{Q}[X]$ is not irreducible is of cardinality $O(T^{3/2})$ as $T \to \infty$.*

The proof of Theorem 1 is given in Section 2. We observe that in Theorem 2.1 in reference [2], S. D. Cohen gives, for arbitrary irreducible polynomials $f(Y_1, \ldots, Y_t, X) \in \mathbb{Z}[Y_1, \ldots, Y_t, X]$, an upper bound for the number of integer tuples $(m_1, \ldots, m_t) \in (\mathbb{Z} \cap [-T, T])^t$ such that $f(m_1, \ldots, m_t, X)$ is irreducible in $\mathbb{Z}[X]$. In the special case considered by us, this gives an upper bound of $O(T^{3/2} \log T)$ on the number of pairs $(a, b) \in (\mathbb{Z} \cap [-T, T])^2$ for which $f_{a,b}(X)$ is not irreducible in

$\mathbb{Z}[X]$, which is slightly worse than the conclusion of our Theorem 1. Furthermore, the proof of our Theorem 1 is elementary.

The next natural question we ask is when does the same field arise from two different pairs (a, b)? That is, when can it happen that there exist two pairs $(a, b) \neq (a_1, b_1)$ and two roots $\theta_{a,b}$ of $f_{a,b}(X)$ and θ_{a_1,b_1} of $f_{a_1,b_1}(X)$, respectively, such that $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{Q}(\theta_{a,b})$? Clearly, if

$$(a_1, b_1) = (\lambda^{n-1}a, \lambda^n b)$$

holds for some rational number λ, then $\theta_{a_1,b_1} = \lambda\theta_{a,b}$, therefore certainly $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{Q}(\theta_{a,b})$. Are there any other instances when this phenomenon happens? We cannot answer this question. However, here is a small contribution towards this problem. Let

$$\mathcal{D} = \{(a, b) \in \mathbb{Z}^2 : a \neq 0,\ \mu(b) \neq 0\},$$

where $\mu(m)$ is the Möbius function of m which is zero if m is divisible by a square of a prime and is $(-1)^k$ if m is a product of k distinct primes.

Theorem 2. *Assume that $n \geq 5$. For each number field $\mathbb{K}$, there are at most finitely many pairs $(a, b) \in \mathcal{D}$ such that $\mathbb{K} = \mathbb{Q}(\theta_{a,b})$ for some root $\theta_{a,b}$ of $f_{a,b}(X)$.*

The proof of Theorem 2 is given in Section 3. Let

$$m(\mathbb{K}) = \#\{(a, b) \in \mathcal{D} : \mathbb{K} = \mathbb{Q}(\theta_{a,b}) \text{ for some root } \theta_{a,b} \text{ of } f_{a,b}(X)\}.$$

Theorem 2 implies that $m(\mathbb{K}) < \infty$ holds for all algebraic number fields $\mathbb{K}$. We conjecture that a stronger statement holds, namely the following:

Conjecture 1. *Assume that $n \geq 5$. There exists a constant c_n depending only on n such that $m(\mathbb{K}) < c_n$ holds for all algebraic number fields $\mathbb{K}$.*

We make a remark about this conjecture at the end of Section 3.

We may ask how important is the condition $n \geq 5$ in the statement of Theorem 2? Section 4 is dedicated to comments regarding this condition. In that section, we show that the conclusion of Theorem 2 is false for $n = 2$ and $n = 3$, and present evidence that it is perhaps false for $n = 4$ as well.

For any real number T, let

$$F(T) = \#\{\mathbb{Q}(\theta_{a,b}^{(i)}),\ i = 1, \ldots, n : a, b \in \mathbb{Z},\ \max\{|a|, |b|\} \leq T\}. \tag{1}$$

Hence, $F(T)$ counts the number of distinct fields of the form $\mathbb{Q}(\theta_{a,b})$, where $\theta_{a,b}$ can be any root of $f_{a,b}(X)$, as a and b vary through integers of absolute value at most T.

We would like to suggest the following conjecture:

Conjecture 2. *There exists a positive constant c_n depending on n such that*

$$F(T) > c_n T^2$$

holds for all sufficiently large real numbers T.

Note that Conjecture 1 implies Conjecture 2, but perhaps Conjecture 2 is easier to prove than Conjecture 1. Note also that $F(T) \ll T^2$ trivially. Thus, Conjecture 2 above suggests that the true order of magnitude of $F(T)$ is T^2.

We have not succeeded in proving Conjecture 2. We have however the following result whose proof is given in Section 5.

Theorem 3. *Assume that $n \geq 4$. There exists a positive constant c_n depending on n such that*

$$F(T) \geq T \exp\left(c_n \frac{\log T}{\log\log T}\right)$$

holds as $T \to \infty$.

One can ask whether it is true that for every algebraic number field $\mathbb{K}$ there exists a pair of integers (a, b) such that $\mathbb{K} = \mathbb{Q}(\theta_{a,b})$ for some root $\theta_{a,b}$ of $f_{a,b}(X)$. The answer to this is yes for $n = 2,\ 3$ and no for $n \geq 4$. To see this, let us note that $\mathbb{Q}(\theta_{a,b})$ does not have too many real conjugates. That is, it is easy to see that $f_{a,b}(X)$ can have at most three real roots. Indeed, for if not, then by Rolle's theorem $f'_{a,b}(x) = nX^n + a$ will have at least three real roots, and this is clearly impossible. Thus, if $n \geq 4$ and $\mathbb{K}$ is a totally real number field of degree ≥ 4, then $\mathbb{K} \neq \mathbb{Q}(\theta_{a,b})$ for any pair of integers (a, b) and any root $\theta_{a,b}$ of $f_{a,b}(X)$.

We conclude this section by pointing out that the Galois group of the polynomial $f_{a,b}(X)$ has been extensively studied. For example, Theorem 1.1 of [3] shows, in particular, that if $\gcd(a, n) = \gcd(a(n-1), b) = 1$, and $f_{a,b}(X)$ is irreducible, then the Galois group of $\mathbb{Q}(\theta_{a,b})$, for any root $\theta_{a,b}$ of $f_{a,b}(X)$, contains A_n. Under these restrictions, and assuming further than $n \geq 5$, then, by the proof of Theorem 2 and the remark at the end of it, there are only finitely many pairs of integers (a, b) such that the discriminant of $f_{a,b}(X)$ is a square (see also [8] and [10] for conditional and unconditional results concerning the square-free values of discriminants of $f_{a,b}(X)$ as a and b range over the integers in certain intervals). Thus, except for such finitely many pairs, the Galois group of $\mathbb{Q}(\theta_{a,b})$ over $\mathbb{Q}$ is S_n. However, note that the conditions $\gcd(n, a) = \gcd(a(n-1), b) = 1$ are fulfilled for a set of positive asymptotic density of pairs of integers (a, b) in $[-T, T]$ as $T \to \infty$. Since by Theorem 1, $f_{a,b}(X)$ is also irreducible for almost all pairs of integers (a, b) in $[-T, T]$ as $T \to \infty$, we deduce, by Theorem 2.1 in [2], the following result.

Theorem 4. *The Galois group of $f_{a,b}(X)$ over the rationals is S_n for all pairs of integers $(a, b) \in [-T, T]$ except for a set of such pairs of cardinality $O(T^{3/2} \log T)$ as $T \to \infty$.*

2. Proof of Theorem 1

Since there are only $O(T)$ pairs $(a, 0)$ with $|a| \leq T$, we may assume that $b \neq 0$. Let (a, b) be a pair for which $f_{a,b}(X)$ is not irreducible and write $f_{a,b}(X) = g(X)h(X)$, where

$$g(X) = X^k + p_0 X^{k-1} + \cdots + p_{k-1} \qquad \text{and} \qquad h(X) = X^\ell + q_0 X^{\ell-1} + \cdots + q_{\ell-1},$$

and k and ℓ positive integers. If $k = 1$, then $-p_0$ is a root of $f_{a,b}(X)$. Hence, $p_0 \mid b$, therefore p_0 can be chosen in at most $2\tau(|b|)$ ways, where $\tau(m)$ is the number of divisors of m, and once p_0 is fixed then

$$a = -\frac{p_0^n + b}{p_0}$$

is also fixed. Since

$$\sum_{0<|b|\leq T} \tau(|b|) = O(T \log T),$$

it follows that there are $O(T \log T)$ pairs (a, b) for which $k = 1$. Similar arguments apply to the case when $\ell = 1$. This takes care, in particular, of the cases when $n = 2$ and $n = 3$.

Assume now that $n \geq 4$ and that both $k \geq 2$ and $\ell \geq 2$. Identifying coefficients, we get

$$p_0 + q_0 = 0, \quad \cdots, \quad p_{k-2}q_{\ell-1} + p_{k-1}q_{\ell-2} = a, \quad p_{k-1}q_{\ell-1} = b.$$

This is a polynomial system of n equations in the $n = k + \ell$ integer unknowns

$$(p_0, \ldots, p_{k-1}, q_0, \ldots, q_{\ell-1}),$$

where we treat a and b as coefficients. By variable elimination, p_{k-1} satisfies a polynomial equation $P_{k,\ell}(p_{k-1}, a, b) = 0$, whose coefficients are polynomials in $\mathbb{Z}[a, b]$. To detect this relation, note that if we write $\theta_1, \ldots, \theta_n$ for all the roots of $f_{a,b}(X)$, then, by the Viète relations,

$$p_{k-1} = (-1)^k \prod_{i \in I} \theta_i$$

for some subset I of $\{1, \ldots, n\}$ of cardinality k. The polynomial

$$P_{k,\ell}(X) = \prod_{\substack{J \subset \{1,\ldots,n\} \\ \#J = k}} \left(X + (-1)^{k+1} \prod_{j \in J} \theta_j \right)$$

is symmetric in the roots $\theta_1, \ldots, \theta_n$ and admits p_{k-1} as a root. By the Fundamental Theorem of Symmetric Polynomials, $P_{k,\ell}(X)$ is a polynomial whose coefficients are in $\mathbb{Z}[a, b]$. The last coefficient (free term) of $P_{k,\ell}(X)$ is

$$(-1)^{(k+1)\binom{n}{k}} \left(\prod_{j=1}^{n} \theta_j \right)^{\binom{n-1}{k-1}} = \delta b^{\binom{n-1}{k-1}}, \qquad \text{where } \delta = (-1)^{(k+1)\binom{n}{k} + n\binom{n-1}{k-1}},$$

again by the Viète relations, because there are $\binom{n}{k}$ subsets J of $\{1, \ldots, n\}$ of cardinality k and each fixed $j \in \{1, \ldots, n\}$ belongs to precisely $\binom{n-1}{k-1}$ such subsets J. Since $p_{k-1}q_{\ell-1} = b$, it follows that for a fixed b, p_{k-1} can be chosen in at most $\tau(|b|) = b^{o(1)}$ ways as $T \to \infty$. When both b and p_{k-1} are fixed, then $P_{k,\ell}(p_{k-1}, a, b) = 0$ is a polynomial relation for a of degree at most $\binom{n}{k}$, so if $P_{k,\ell}(p_{k-1}, A, b) \in \mathbb{Z}[A]$ is not the zero polynomial, then a can take at most $\binom{n}{k}$ values. Thus, in this case we get at most $T^{1+o(1)}$ possibilities for the pair (a, b) as $T \to \infty$. Assume now that $P_{k,\ell}(p_{k-1}, A, b) = 0$. In particular, its free (constant) term is zero. But the constant term is achieved by taking $a = 0$ in the definition of $f_{a,b}(X) = X^n + b$, getting that $\theta_j = e^{j\pi i/n} b^{1/n}$ for $j = 1, \ldots, n$, where $b^{1/n}$ is a fixed determination of the nth root of b. Thus,

$$P_{k,\ell}(X, 0, b) = \prod_{\substack{J \subset \{1,\ldots,n\} \\ \#J = k}} \left(X + \varepsilon_J b^{k/n} \right),$$

where $\varepsilon_J = e^{(k+1+\sum_{j \in J} j)\pi i/n}$ is some root of unity. Thus, if (p_{k-1}, b) are such that $P_{k,\ell}(p_{k-1}, 0, b) = 0$, then $p_{k-1} = -\varepsilon_J b^{k/n}$ holds for some subset J of $\{1, \ldots, n\}$ with k elements. Since $p_{k-1} \in \mathbb{Z}$, we get that $p_{k-1} = \pm |b|^{k/n}$. Since $1 \leq k < n$, we get that $|b|$ must be a power of exponent > 1 of some other integer. The number of

such values for b in $[-T, T]$ is $O(T^{1/2})$. Since a can take at most $2T + 1$ values, it follows that the pair (a, b) can be chosen in at most $O(T^{3/2})$ ways, which completes the proof of this theorem.

3. Proof of Theorem 2

Assume that $\mathbb{K} = \mathbb{Q}(\theta_{a,b})$ for some pair $(a, b) \in \mathcal{D}$ and some root $\theta_{a,b}$ of $f_{a,b}(X)$. We fix the pair (a, b). Let (a_1, b_1) be some other pair in $\mathcal{D}$ such that $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{K}$ for some root θ_{a_1,b_1} of $f_{a_1,b_1}(X)$. Assume that p is a prime dividing both a_1 and b_1. Then, in $\mathbb{K}$, we have

$$\theta(\theta^{n-1} + a_1) = -b_1, \tag{2}$$

where $\theta = \theta_{a_1,b_1}$ is in $\mathcal{O}_{\mathbb{K}}$. Assume further that p does not ramify in $\mathbb{K}$. Then

$$p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{j} \pi_i$$

for some distinct prime ideals π_i of $\mathbb{K}$. Since b_1 is square-free, we get that π_1 appears with power 1 in the factorization of b_1 in $\mathcal{O}_{\mathbb{K}}$. But $\pi_1 \mid p \mid \gcd(a_1, b_1)$, therefore $\pi_1 \mid a_1$. Equation (2) shows that $\pi_1 \mid \theta^n$, therefore $\pi_1 \mid \theta$. Thus, π_1^2 divides $\theta(\theta^{n-1} + a_1)$, contradicting that fact that π_1 appears with power 1 in b_1. This argument shows that if $p \mid \gcd(a_1, b_1)$, then $p \in \mathcal{P}_{\mathbb{K}}$, where $\mathcal{P}_{\mathbb{K}}$ is the finite set of primes dividing the discriminant of $\mathbb{K}$.

It is well-known that the discriminant $\Delta_{a,b}$ of $f_{a,b}(X)$ is

$$\Delta_{a,b} = b^{n-1}n^n + (-1)^{n-1}a^n(n-1)^{n-1} \tag{3}$$

(see, for example, [7]). Put $\Delta_{\mathbb{K}}$ for the discriminant of $\mathbb{K}$. Then Δ_{a_1,b_1} is the volume of the lattice $\mathbb{Z}[\theta_{a_1,b_1}]$ inside $\mathcal{O}_{\mathbb{K}}$, so $\Delta_{a_1,b_1} = \Delta_{\mathbb{K}}x^2$ holds, where x is the index of $\mathbb{Z}[\theta_{a_1,b_1}]$ in $\mathcal{O}_{\mathbb{K}}$. Hence, the above discriminant calculation shows that

$$b_1^{n-1}n^n + (-1)^{n-1}a_1^n(n-1)^{n-1} = \Delta_{\mathbb{K}}x^2.$$

Let $D_1 = \gcd(n^n b_1^{n-1}, a_1^n(n-1)^{n-1})$. If $p \mid D_1$, then either $p \le n$ or the divisibility relation $p \mid \gcd(a_1, b_1)$ holds. Thus, either $p \le n$ or $p \in \mathcal{P}_{\mathbb{K}}$ by the arguments from the beginning of this proof. Since b_1 is square-free, we get that

$$D_1 \mid n^n \left(\prod_{p \in \mathcal{P}_{\mathbb{K}}} p \right)^{n-1},$$

so D_1 can take only finitely many values. Fix a value for D_1. For this fixed value of D_1, we must have $b_1 = b_1' X$, where X is a positive integer coprime to D_1, and b_1' is a square-free integer all of whose prime factors are among the prime factors of D_1. Clearly, b_1' can be fixed in only finitely many ways as well. Assume that b_1' is also fixed. Then a_1 is such that $a_1 = a_1' Y$, where Y is an integer and a_1' is the smallest positive integer such that $(n-1)^{n-1}a_1'^n$ is a multiple of D_1. Finally, $x = x_1 Z$, where Z is an integer and x_1 is the smallest positive integer such that $\Delta_{\mathbb{K}}x_1^2$ is a multiple of D_1. We thus get the equation

$$n^n(b_1')^n X^n + (-1)^{n-1}(n-1)^{n-1}(a_1')^n Y^{n-1} = (\Delta x_1^2)Z^2,$$

or, after simplifying by D_1,

$$A_1 X^n + B_1 Y^{n-1} = C_1 Z^2, \tag{4}$$

where

$$A_1 = n^n(b_1')^n/D_1, \quad B_1 = (-1)^{n-1}(n-1)^{n-1}(a_1')^n/D_1, \quad C_1 = \Delta_{\mathbb{K}} x_1^2/D_1.$$

Furthermore, notice that in the above equation (4), we have the relation

$$\gcd(A_1X^n, B_1Y^n, C_1Z^2) = 1.$$

Since the sum of the reciprocals of the three exponents $1/n+1/(n-1)+1/2 < 1$ for $n \geq 5$, a result of Darmon and Granville [4] shows that the Diophantine equation (4) has at most finitely many solutions (X_1, Y_1, Z_1). Since D_1 can be chosen in only finitely many ways, the theorem is proved.

Remark. Let $\mathcal{D}_1$ be the subset of $\mathcal{D}$ such that $\gcd(a, n) = \gcd(a(n-1), b) = 1$. Fix $(a, b) \in \mathcal{D}_1$ and let Δ be the discriminant of $\mathbb{Q}(\theta_{a,b})$. If $(a_1, b_1) \in \mathcal{D}_1$ is such that $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{Q}(\theta_{a,b})$, then

$$nX^{n-1} - (n-1)^{n-1}Y^n = \Delta Z^2 \tag{5}$$

holds with $X = nb_1$ and $Y = -a_1$ and $\gcd(nX, (n-1)Y) = 1$. Darmon and Granville's proof [4] of the finiteness of integer solutions of the above equation proceeds by showing that every integer solution of the above equation produces a rational point on a curve of genus $2n(n-1)(1-1/2-1/n-1/(n-1)) = n^2-5n+2 \geq 2$ defined over an algebraic number field $\mathbb{L}$ of degree and discriminant bounded in terms of n and Δ, and this association is injective. The conclusion follows by appealing to Falting's theorem concerning the finiteness of rational points on a curve of genus $g > 1$. It has been suggested by Lang (see [1]) that there should be a bound on the number of rational points on a curve of genus $g > 1$ which depends only on the genus g, but not on the curve itself. This is usually referred to as the *Rigidity Conjecture*. It thus makes sense to conjecture that the number of solutions (X, Y, Z) of the Diophantine equation (5) with $\gcd(nX, (n-1)Y) = 1$ is bounded by a number depending only on n (hence, not on Δ). This may be interpreted as (weak) evidence in favor of Conjecture 2. Even assuming the rigidity conjecture, the proof of Darmon of Granville does not seem to immediately lead to the above conclusion since it also uses Minkowski's convex body theorem to bound the candidates for $\mathbb{L}$, which are number of fields of degree bounded in terms of n only and unramified at the places not dividing $n(n-1)\Delta$, and this last number does depend on Δ. Perhaps a closer analysis of the arguments from [4] will show that the number of such fields can be bounded by some power of $\tau(\Delta)$. If true, then since $\omega(\Delta) \ll \log\log T$ holds for almost all pairs of integers $(a, b) \in [-T, T]$ as $T \to \infty$, it would follow, under the rigidity conjecture, that $m(\mathbb{K}_{a,b}) \ll (\log T)^{c_n}$ holds for almost all pairs $(a, b) \in [-T, T]$ as $T \to \infty$, where c_n is some constant depending on n. In turn, this will imply that $F(T) \gg T^2/(\log T)^{c_n}$ which is still short by the logarithmic factor from the lower bound conjectured by Conjecture 2, but it is much better than the unconditional lower bound of Theorem 3 of $F(T)$.

4. Theorem 2 and small values of n

In this section, we show that the conclusion of Theorem 2 is false when $n = 2$ and $n = 3$, and present evidence that it is perhaps also false when $n = 4$.

If $n = 2$, then we may assume that $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, where $d \neq 0, 1$ is a square-free positive integer. We prove that there are infinitely many quadratic polynomials $f(x) = x^2 + ax + b$ with $a \neq 0$ and b square-free whose roots generate $\mathbb{K}$. Clearly,

this is equivalent to the fact that $a^2 - 4b = d\lambda^2$ for some integer λ. Taking $a = 2a_0,\ \lambda = 2$, it suffices to show that the number $b = a_0^2 - d$ is square-free for infinitely many positive integers a_0. However, it is well-known and easy to prove that the polynomial $X^2 - d$ represents infinitely many square-free positive integers. In fact, this is true for all quadratic polynomials $f(X)$ such that for each prime p there is an integer n with $p^2 \nmid f(n)$.

Assume now that $n = 3$ and fix $a \neq 0$ and b square-free. We let α, β, γ be some integers to be determined later and compute the resultant with respect to X of the polynomial $X^3 + aX + b$ and $\alpha X^2 + \beta X + \gamma - T$. We obtain the polynomial

$$\begin{aligned} R(T) &= -T^3 + (-2a\alpha + 3\gamma)T^2 + (-a^2\alpha^2 - 3\alpha b\beta - a\beta^2 + 4a\alpha\gamma - 3\gamma^2)T \\ &+ (\alpha^3 b^2 - a\alpha^2 b\beta - b\beta^3 + a^2\alpha^2\gamma + 3\alpha b\beta\gamma + a\beta^2\gamma - 2a\alpha\gamma^2 + \gamma^3). \end{aligned}$$

Imposing that the coefficient of T is zero, we get $\gamma = 2a\alpha/3$. Replacing this value of γ in the remaining coefficients of $R(T)$ we get

$$\begin{aligned} R_1(T) &= -T^3 + \left(\frac{a^2\alpha^2}{3} - 3\alpha b\beta - a\beta^2\right) T \\ &+ \frac{2a^3\alpha^3}{27} + \alpha^3 b^2 + a\alpha^2 b\beta^2 + \frac{2a^2\alpha\beta^2}{3} - b\beta^3. \end{aligned}$$

Choosing $a = 3,\ b = 1$ (note that $f_{3,1}(X) = X^3 + 3X + 1$ is irreducible in $\mathbb{Q}[X]$), we get

$$R_1(T) = -T^3 + 3(\alpha^2 - \alpha\beta - \beta^2)T + (3\alpha^3 + 3\alpha^2\beta + 6\alpha\beta^2 - \beta^3).$$

Thus, if we choose $a_1 = 3(\alpha^2 - \alpha\beta - \beta^2)$ and $b_1 = 3\alpha^3 + 3\alpha^2\beta + 6\alpha\beta^2 - \beta^3$, then $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{Q}(\theta_{3,1})$, for some appropriately chosen roots θ_{a_1,b_1} and $\theta_{3,1}$ of $f_{a_1,b_1}(X)$ and $f_{3,1}(X)$, respectively. It is clear that $a_1 \neq 0$ unless both α and β are zero. Thus, it suffices, in order for (a_1, b_1) to belong to $\mathcal{D}$, that b_1 is square-free. However, it is well-known that there are infinitely many square-free integers of the form $3X^3 + 3X^2Y + 6XY^2 - Y^3$ (see, for example, [6]).

Finally, let $n = 4$. We let again $(a, b) \in \mathcal{D}$, $\alpha, \beta, \gamma, \delta$ be integers and we take

$$\begin{aligned} S(T) &= \mathrm{Res}_X(X^4 + aX + b, \alpha X^3 + \beta X^2 + \gamma X + \delta - T) \\ &= T^4 + (3a\alpha - 4\delta)T^3 + (3a^2\alpha^2 + 2b\beta^2 + 4\alpha b\gamma + 3a\beta\gamma - 9a\alpha\delta + 6\delta^2)T^2 \\ &+ CT + D, \end{aligned}$$

where C and D are some polynomials in $a, b, \alpha, \beta, \gamma, \delta$ which we no longer explicitly write down. Imposing that the coefficients of T^3 and T^2 in $S(T)$ are zero, we get

$$\delta = \frac{3a\alpha}{4} \qquad \text{and} \qquad \gamma = \frac{3a^2\alpha^2 - 16b\beta^2}{8(4\alpha b + 3a\beta)}.$$

We now choose $\beta = (3 - 4\alpha b)/(3a)$. Putting now $a = 1$ and $b = 6$ (note that $f_{1,6}(X) = X^4 + X + 6$ is irreducible in $\mathbb{Q}[X]$), and $\alpha = 4(17 + 36\alpha_0)$ for some integer α_0, we get that

$$S(T) = T^4 + A(\alpha_0)T + B(\alpha_0),$$

where A and B are polynomials with integer coefficients in the variable α_0. We have that $A(Z)$ is nonzero and

$$\begin{aligned} B(Z) = 6\,(&193103517037550444796315 7 + 32774253999060620818245978Z \\ &+ 24336241399338483321730497 6Z^2 + 10326095711996981147285886 72Z^3 \end{aligned}$$

$$+27384121042695974466388604 16Z^4 + 46477358797502103250255257 60Z^5$$
$$+49301949499976162649237258 24Z^6 + 29884685993091551033247006 72Z^7$$
$$+79252205948530080088168857 6Z^8\big).$$

Since $B(Z)$ is an irreducible polynomial of degree 8 and

$$B(1)/6 = 23159 \cdot 83381630052053389523$$

is a product of two primes each exceeding 8, Schinzel's Hypothesis H implies that $B(Z)/6$ should be prime for infinitely many Z. Indeed, the only condition to be verified is that for each prime p, there exists m such that $p \nmid B(m)/6$. For $p \le 11$ this is true by taking $m = 1$, and for $p > 11$ this is true because the equation $B(m)/6 \equiv 0 \pmod p$ is a polynomial equation of degree ≤ 8, so it can have at most 8 solutions modulo p, therefore there exist at least $p - 8 > 0$ congruence classes m modulo p such that $B(m)/6$ is not zero modulo p. In particular, certainly $B(\alpha_0)$ should be square-free for infinitely many choices of the integer α_0, showing that there should be infinitely many pairs $(a_1, b_1) \in \mathcal{D}$ (namely, all these of the form $(A(\alpha_0), B(\alpha_0))$ with the second component square-free) such that $\mathbb{Q}(\theta_{a,b}) = \mathbb{Q}(\theta_{1,6})$. All this is conditional upon Schinzel's Hypothesis H. We would like to suggest the following problem for the reader.

Problem 1. *Find a pair $(a, b) \in \mathcal{D}$ and an unconditional proof of the fact that $\mathbb{Q}(\theta_{a,b}) = \mathbb{Q}(\theta_{a_1,b_1})$ for infinitely many pairs $(a_1, b_1) \in \mathcal{D}$ when $n = 4$.*

5. Proof of Theorem 3

Let $\mathcal{P}_T$ be a fixed finite set of prime numbers, which will depend on T. We write $s = s(T)$ for the cardinality of $\mathcal{P}_T$. We choose (a, b) such that $2 \mid a$, $b \equiv 2 \pmod 4$, $|a| \le T$, $|b| \le T$, $\gcd(a, b) = 2$, and all prime factors of b are in $\mathcal{P}_T$. Note that $f_{a,b}(X)$ is irreducible for such pairs (a, b) because it is Eisenstein with respect to the prime 2.

We also assume that $|a| > nT^{(n-1)/n}$. We let $\mathbb{K}$ be some fixed field and count how many pairs (a, b) can give rise to $\mathbb{K}$. Letting (a, b) be such a pair, then

$$\theta(\theta^{n-1} + a) = -b.$$

Let $\mathbb{L}$ be the normal closure of $\mathbb{K}$. Passing to ideals in $\mathbb{L}$, we get that $\theta\mathcal{O}_{\mathbb{L}}$ is a divisor of b. Let $\mathcal{Q}_{\mathbb{L}}$ be the set of all prime ideals in $\mathbb{L}$ dividing some prime number $p \in \mathcal{P}_T$. Since every prime in $\mathcal{P}_T$ has at most $[\mathbb{L} : \mathbb{Q}] \le n!$ prime ideal divisors in $\mathcal{Q}_{\mathbb{L}}$, it follows that $t = \#\mathcal{Q}_{\mathbb{K}} \le n!s$. Let these ideals be $\pi_1, \ldots, \pi_t$. Let $\zeta_1, \ldots, \zeta_m$ be generators for the free part of the group of units of $\mathbb{L}$. Note that $m \le n! - 1$. Let h be the class number of $\mathbb{L}$. Then π_i^h is principal. For each $i = 1, \ldots, t$, let η_i be a generator of π_i^h. Then the equation

$$\theta(\theta^{n-1} + a) = -b,$$

gives

$$\theta\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{t} \pi_i^{\alpha_i} \qquad \text{and} \qquad (\theta^{n-1} + a)\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{t} \pi_i^{\beta_i},$$

for some nonnegative integers α_i and β_i, $i = 1, \ldots, t$. Raising these relations to the power h, we get

$$\theta^h\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{t} (\pi_i^h)^{\alpha_i} = \prod_{i=1}^{t} \eta_i^{\alpha_i}\mathcal{O}_{\mathbb{L}},$$

and similarly

$$(\theta^{n-1} + a)^h \mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{t} \eta_i^{\beta_i} \mathcal{O}_{\mathbb{L}}.$$

Passing to elements, we get

$$\theta^h = \nu \prod_{i=1}^{t} \eta_i^{\alpha_i} \prod_{j=1}^{m} \zeta_j^{\gamma_j} \tag{6}$$

and

$$(\theta^{n-1} + a)^h = \mu \prod_{i=1}^{t} \eta_i^{\beta_i} \prod_{j=1}^{m} \zeta_j^{\delta_j}, \tag{7}$$

where γ_j and δ_j are integers for $j = 1, \ldots, m$ and ν and μ are roots of unity in $\mathbb{L}$ (their order does not exceed the largest positive integer N such that $\phi(N) \leq n!$). Let η_i' and ζ_j' be fixed determinations of the hth roots of η_i and ζ_j, respectively, where $i = 1, \ldots, t$ and $j = 1, \ldots, m$. Let also λ be a generator of the group of torsion units in $\mathbb{L}$ and λ' be a fixed determination of its hth root. Extracting h'th roots in equations (6) and (7), we get

$$\theta = \lambda'^k \prod_{i=1}^{t} \eta_i'^{\alpha_i} \prod_{i=1}^{m} \zeta_j'^{\gamma_j} \qquad \text{and} \qquad \theta^{n-1} + a = \lambda'^{\ell} \prod_{i=1}^{t} \eta_i'^{\beta_i} \prod_{i=1}^{m} \zeta_j'^{\delta_j}.$$

Let G be the multiplicative group inside the field of complex numbers generated by the numbers $\{\lambda', \eta_i', \zeta_j' : i = 1, \ldots, t,\ j = 1, \ldots, m\}$. Note that it is easy to see that G may be assumed to be invariant under the conjugations from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then the above equation shows that

$$a = s_1 - s_2,$$

where $s_1 = \theta^{n-1}$ and $s_2 = \theta^{n-1} + a$ are elements in G. Conjugating (or replacing θ by one of its conjugates θ'), we get $a = s_3 - s_4$, where $s_3 = (\theta')^{n-1}$ and $s_4 = (\theta')^{n-1} + a$ are also in G. Hence, we have obtained the $\mathcal{S}$-unit equation

$$s_1 - s_2 - s_3 + s_4 = 0. \tag{8}$$

Recall that an $\mathcal{S}$-unit equation is *degenerate* if some sub-sum of it is zero. In this case, being degenerate means that one of $s_1 - s_2,\ s_1 - s_3$ and $s_1 + s_4$ is zero. Observe that:

(i) If $s_1 - s_2 = 0$, then $a = 0$, which is not allowed.

(ii) If $s_1 - s_3 = 0$, then $\theta^{n-1} = (\theta')^{n-1}$. Since $\theta(\theta^{n-1} + a) = -b = \theta'((\theta')^{n-1} + a)$, it follows that $\theta = \theta'$. This is impossible because $f_{a,b}(X)$ is irreducible in $\mathbb{Q}[X]$.

(iii) If $s_1 + s_4 = 0$, then $\theta^{n-1} - (\theta')^{n-1} - a = 0$. Hence, $\theta^{n-1} = \theta'^{n-1} + a = -b/\theta'$. We now get easily that $|\theta|^{n-1}|\theta'| = |b|$. If this is true for all conjugates of θ' of θ, we get that all the roots of $f_{a,b}(X)$ have the same absolute value $|b|^{1/n}$. Thus, by the Viète relations, $|a| \leq n|b|^{(n-1)/n} \leq nT^{(n-1)/n}$, which is false by our initial assumption on a. Hence, there must be two conjugates θ and θ' having different absolute values, and for these we have $s_1 + s_4 \neq 0$.

The above argument shows that for each of the pairs (a, b) under consideration, there exists an $\mathcal{S}$-unit equation of the form (8) which is nondegenerate. By results of Evertse, Schmidt and Schlickewei [5], the set of ratios s_1/s_2 is of cardinality

$$\leq \exp(24^{12}(m+t+1)) \leq \exp(24^{12}n!(s+1)).$$

Now let $u = s_1/s_2$ be fixed. Then $-\theta^n/b = u = 1 + a/\theta^{n-1}$. We get $\theta = (-bu)^{1/n}$, so $a = -(1-u)\theta^{n-1} = -(1-u)(-u)^{(n-1)/n}b^{(n-1)/n}$. Thus, $|a|/|b|^{(n-1)/n}$ is uniquely determined in terms of u. Assume that (a, b) and (a_1, b_1) are such that $|a|/|b|^{(n-1)/n} = |a_1|/|b_1|^{(n-1)/n}$. Raising this equality to nth power, we get $|a|^n/|b|^{n-1} = |a_1|^n/|b_1|^{n-1}$. Since $2\|b$ and $\gcd(a, b) = 2$, we get $a = \pm a_1$ and $b = \pm b_1$. Thus, each solution of the nondegenerate equation (8) determines a and b uniquely up to signs.

All we have to do is count. We choose y such that

$$s = \pi(y) \leq \frac{c \log T}{\log\log T},$$

where $c < 1$ is some constant to be determined later. Then

$$\prod_{p \leq y} p = \exp((1 + o(1))y)$$

holds as $T \to \infty$. Thus, if we let $\varepsilon > 0$ be fixed and we put

$$K = \left\lfloor (1-\varepsilon)\frac{\log T}{y} \right\rfloor,$$

then any number $b = \prod_{p \leq y} p^{\alpha_p}$ with $2\|b$ and $\alpha_p \leq K$ for all $p \leq y$ works. Let $\mathcal{B}$ be the set of such numbers. Then

$$\#\mathcal{B} \gg (K+1)^{\pi(y)-1} = \exp\left((1+o(1))s \log\left(\frac{\log T}{y}\right) + O(s\varepsilon)\right)$$

holds as $T \to \infty$. Let a be an integer such that $2\|a$, a is free of odd primes $p \leq y$, and $|a| > T^{1-1/2n}$. Let $\mathcal{A}$ be the set of such acceptable a's. Then the inequality

$$\#\mathcal{A} \geq (1+o(1)) \prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1} T + O(T^{1-1/2n}) \geq (e^{-\gamma} + o(1))\frac{T}{\log y}$$

holds as $T \to \infty$. Let $m(\mathbb{K})$ be the multiplicity of $\mathbb{K}$ when (a, b) range in $\mathcal{A} \times \mathcal{B}$. Note that all conditions from beginning of this proof are fulfilled by these pairs (a, b) when T is large. The above argument shows that the number of different fields created in this way is at least

$$\frac{\#\mathcal{A} \times \#\mathcal{B}}{\max\{m(\mathbb{Q}(\theta_{a,b})) : (a, b) \in \mathcal{A} \times \mathcal{B}\}} \geq T \exp\left((s + o(s)) \log\left(\frac{\log T}{c_1 y}\right) + O(s\varepsilon)\right)$$

as $T \to \infty$, where $c_1 = 24^{12}n!$. We now put $c_2 = (c_1 e)^{-1}$, choose $y = c_2 \log T$ for which $s = (c_2 + o(1)) \log T / \log\log T$ as $T \to \infty$, and get that the number of distinct fields we have created is

$$\geq T \exp\left((c_2 + o(1) + O(\varepsilon))\frac{\log T}{\log\log T}\right)$$

as $T \to \infty$. Making now also ε tend to zero, we get the desired result.

Acknowledgements. We thank the referee for suggestions which improved the quality of this paper. This paper was written during a very enjoyable visit by the

second author to the LMPA of the Université du Littoral Côte d'Opale of Calais; he wishes to express his thanks to that institution for the hospitality and support. During the preparation of this paper, F. L. was also partly supported by grant SEP-CONACyT 79685 and PAPIIT 100508.

References

[1] C. Caporaso, J. Harris and B. Mazur, 'Uniformity of rational points', *J. American Math. Soc.* **10** (1997), 1–35.

[2] S. D. Cohen, 'The distribution of Galois groups and Hilbert's irreducibility theorem', *Proc. London Math. Soc. (3)* **43** (1981), 227–250.

[3] S. D. Cohen, A. Movahhedi and A. Salinier, 'Galois groups of trinomials', *J. Algebra* **222** (1999), 561–573.

[4] H. Darmon and A. Granville, 'On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$', *Bull. London Math. Soc.* **27** (1995), 513–543.

[5] J.-H. Evertse, H. P Schlickewei and W. M. Schmidt, 'Linear equations in variables which lie in a multiplicative group', *Ann. of Math. (2)* **155** (2002), 807–836.

[6] F. Gouvêa and B. Mazur,'The square-free sieve and the rank of elliptic curves', *J. Amer. Math. Soc.* **4** (1991), no. 1, 1–23.

[7] P. Lefton, 'On the Galois groups of cubics and trinomials', *Bull. Amer. Math. Soc.* **82** (1976), 754–756.

[8] A. Mukhopadhyay, M. R. Murty and K. Srinivas, 'Counting squarefree discriminants of trinomials under *abc*', *Proc. Amer. Math. Soc.* **137**, 3219–3226.

[9] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, third. ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997.

[10] I. Shparlinski, 'On Quadratic Fields Generated by Discriminants of Irreducible Trinomials', *Preprint*, 2009, http://arxiv.org/abs/0811.1300.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 3, Pages 107–116
ISSN 1930-1235: (2009)

RESOLVENT EQUATIONS METHOD FOR GENERAL VARIATIONAL INCLUSIONS

Eman Al-Shemas *Mathematics Department,*
College of Basic Education
Main Campus, Shamiya, Kuwait

Abstract. In this paper, we introduce a new class of variational inclusions involving three operator. Using the resolvent operator technique, we establish the equivalence between the general variational inclusions and the resolvent equations. We use this alternative equivalent formulation to suggest and analyze some iterative methods for solving the general variational inclusions. We also consider the criteria of these iterative methods under suitable conditions. Since the general variational inclusions include the variational inequalities and the related optimization problems as special cases, our results continue to hold for these problems.

1. Introduction

Variational inclusions involving three operators are useful and important extensions and generalizations of the the general variational inequalities with a wide range of applications in industry, mathematical finance, economics, decision sciences, ecology, mathematical and engineering sciences, see [1-45] and the references therein. It is well known that the projection method and its variant forms including the Wiener-Hopf equations can not be extended and modified for solving the variational inclusions. These facts and comments have motivated to use the technique of the resolvent operators. This technique can lead to the development of very efficient and robust methods since one can treat each part of the original operator independently. A useful feature of these iterative methods for solving the general variational inclusion is that the resolvent step involves the the maximal monotone operator only, while other parts facilitates the problem decomposition. Essentially using the resolvent technique, one can show that the variational inclusions are equivalent to the fixed point problems. This alternative equivalent formulation has played very crucial role in developing some very efficient methods for solving the variational inclusions and related optimization problems, see [15-38] and the references therein. Related to the variational inclusions, we have the problem of solving the resolvent equations, which are mainly due to Noor [20,21,23]. Essentially using the resolvent operator technique, we can establish the equivalence between the resolvent equations and the variational inclusions. This equivalence formulations is more general and flexible than the resolvent operator method. Resolvent equations

Received by the editors Feb 15, 2008 and, in revised form, June 15, 2008.
2000 *Mathematics Subject Classification.* Primary 49J40; Secondary 90C33.
Key words and phrases. Variational inclusion; approximation methods; resolvent equations; variational inequalities.

technique has been used to suggest and analyze several iterative methods for solving variational inclusions and related problems, see [24-27,32,34-38] and the references therein.

Motivated and inspired by the recent research activities in these areas, we introduce some new classes of variational inclusions and resolvent equations. Essentially using the resolvent operator methods, we establish the equivalence between the resolvent equations and the general variational inclusions. This alternative equivalent formulation is used to suggest some iterative methods for solving the general variational inclusions. We study the convergence criteria of the new iterative method under some mild conditions. Since the variational inclusions include the mixed variational inequalities and related optimization problems as special cases, results proved in this paper continue to hold for these problems.

2. Basic Results

Let K be a nonempty closed and convex set in a real Hilbert space, whose inner product and norm are denoted by $\langle \cdot, \cdot \rangle$ and $\|.\|$ respectively. Let $T, A, g : H \longrightarrow H$ be three nonlinear operators.

We consider the problem of finding $u \in H$ such that

$$0 \in \rho Tu + u - g + \rho A(u), \quad \rho > 0, \quad \text{a constant}, \tag{1}$$

which is known as the general variational inclusion $GVI(T, A, g)$. Problem (1) is also known as finding the zero of the sum of two (or more) monotone operators. Variational inclusions and related problems are being studied extensively by many authors and have important applications in operations research, optimization, mathematical finance, decision sciences and other several branches of pure and applied sciences, see [2-45] and the references therein.

If $A(.) \equiv \partial\varphi(.)$, where $\partial\varphi(.)$ is the subdifferential of a proper, convex and lower-semicontinuous function $\varphi : H \longrightarrow R \cup \{+\infty\}$, then the problem (1) reduces to finding $u \in H$ such that

$$0 \in \rho Tu + u - g(u) + \rho\partial\varphi(u),$$

or equivalently, finding $u \in H$ such that

$$\langle \rho Tu + u - g(u), g(v) - u \rangle + \rho\varphi(g(v)) - \rho\varphi(u) \geq 0, \quad \forall v \in H. \tag{2}$$

The inequality (2) is called the general mixed variational inequality or the general variational inequality of the second kind. It has been shown that a wide class of linear and nonlinear problems arising in various branches of pure and applied sciences can be studied in the unified framework of mixed variational inequalities, see [2-38].

We note that if φ is the indicator function of a closed convex set K in H, that is,

$$\varphi(u) \equiv I_K(u) = \begin{cases} 0, & \text{if} \quad u \in K \\ +\infty, & \text{otherwise}, \end{cases}$$

then the general mixed variational inequality (2) is equivalent to finding $u \in K$ such that

$$\langle \rho Tu + u - g(u), g(v) - u \rangle \geq 0, \quad \forall v \in H : g(v) \in K, \tag{3}$$

which is called the general variational inequality introduced and studied by Noor [29] in connection with nonconvex functions. See also Noor and Noor [31,32] for more details.

If $g \equiv I$, the identity operator, then problem (3) is equivalent to finding $u \in K$ such that

$$\langle Tu, v-u\rangle \geq 0, \quad \forall v \in K, \tag{4}$$

which is known as the classical variational inequality introduced and studied by Stampacchia [44] in 1964. For the recent trends and developments in variational inclusions and inequalities, see [2-45] and the references therein.

We also need the following well known concepts and results.

Definition 2.1 [5]. If A is a maximal monotone operator on H, then, for a constant $\rho > 0$, the resolvent operator associated with A is defined by

$$J_A(u) = (I + \rho A)^{-1}(u), \quad \text{for all } u \in H,$$

where I is the identity operator. It is well known that a monotone operator is maximal if and only if its resolvent operator is defined everywhere. In addition, the resolvent operator is a single-valued and nonexpansive, that is, for all $u, v \in H$,

$$\|J_A(u) - J_A(v)\| \leq \|u - v\|.$$

Remark 2.1. It is well known that the subdifferential $\partial\varphi$ of a proper, convex and lower semicontinuous function $\varphi : H \to R \cup \{+\infty\}$ is a maximal monotone operator, we denote by

$$J_\varphi(u) = (I + \rho\partial\varphi)^{-1}(u), \quad \text{for all } u \in H,$$

the resolvent operator associated with $\partial\varphi$, which is defined everywhere on H. In particular, the resolvent operator J_φ has the following interesting characterization.

Lemma 2.1 [5]. For a given $z \in H$, $u \in H$ satisfies the inequality

$$\langle u - z, v - u\rangle + \rho\varphi(v) - \rho\varphi(u) \geq 0, \quad \text{for all } v \in H,$$

if and only if

$$u = J_\varphi z,$$

where $J_\varphi = (I + \rho\partial\varphi)^{-1}$ is the resolvent operator.

This property of the resolvent operator J_φ plays an important part in developing the numerical methods for solving the mixed variational inequalities.

If the function $\varphi(.)$ is the indicator function of a closed convex set K in H, then it is well known that $J_\varphi = P_K$, the projection operator of H onto the closed convex set K.

Related to the variational inclusions, we consider the problem of solving the resolvent equations. To be more precise, let $R_A = I - gJ_A$, where J_A is the resolvent operator associated with the maximal monotone operator A, and I is the identity operator. For a given operator T, we consider the problem of finding $z \in H$ such that

$$TJ_A z + \rho^{-1} R_A z = 0, \tag{5}$$

which is called the general resolvent equation. If φ is the indicator function of a closed convex set K, then $J_\varphi = P_K$, the projection of H onto the closed convex set K. and $Q_K = I - gP_K$. In this case, resolvent equations (5) are equivalent to find $z \in H$ such that

$$TP_K z + \rho^{-1} Q_K z = 0,$$

which are called the Wiener-Hopf equations which were introduced and considered by Noor [29]. If $g \equiv I$, the identity operator, then obtain the original Wiener-Hopf equations introduced and studied by Shi [43]. It is well known that the Wiener-Hopf equations are equivalent to the variational inequalities. This equivalence alternative formulation is more general and flexible that the projection fixed point problem. For the formulation, numerical methods and applications of the Wiener-Hopf equations, see [14,25,28,33,37,41,43] and the references therein.

Using the definition of the resolvent operator J_A, one can easily prove the following well known result. For the sake of completeness and to convey an idea, we include its proof.

Lemma 2.2. The function $u \in H$ is a solution of the variational inclusion (1) if and only if $u \in H$ satisfies the relation

$$u = J_A[g(u) - \rho Tu],$$

where $\rho > 0$ is a constant and $J_A = (I + \rho A)^{-1}$ is the resolvent operator associated with the maximal monotone operator.

Proof. Let $u \in H$ be a solution of (1). Then

$$\begin{aligned} 0 \quad &\in \quad \rho Tu + u - g(u) + \rho A(u) \\ &\iff \quad -(g(u) - \rho Tu) + (I + \rho A)(u) \\ &\iff \quad u = (I + \rho A)^{-1}[g(u) - \rho Tu] = J_A[g(u) - \rho Tu], \end{aligned}$$

the required result.

□

It is clear from Lemma 2.2 that variational inclusion (1) and the fixed point problems are equivalent. This alternative equivalent formulation has played a significant role in the studies of the variational inequalities and related optimization problems.

Algorithm 2.1. For a given $x_0 \in H$, compute the approximate solution x_{n+1} by the iterative schemes:

$$x_{n+1} = (1 - a_n)x_n + a_n J_A[g(x_n) - \rho Tx_n].$$

where $a_n \in [0, 1]$ for all $n \geq 0$. Algorithm 2.1 is also known as Mann iteration.

We now discuss some special cases of Algorithm 2.1 for solving the mixed variational inequalities (2).

I. If $A(.) \equiv \varphi(.)$, the subdifferential of a proper lower-semicontinuous and convex function φ, then $J_A = J_\varphi = (I + \rho\partial\varphi)^{-1}$ and consequently Algorithm 2.1 collapses to:

Algorithm 2.2. For a given $x_0 \in H$, compute the approximate solution x_n by the iterative schemes

$$x_{n+1} = (1 - a_n)x_n + a_n J_\varphi[g(x_n) - \rho Tx_n],$$

where $a_n \in [0, 1]$ for all $n \geq 0$. Algorithm 2.2 is called one-step method for solving the general mixed variational inequalities (2) and appears to be a new one.

II. If φ is the indicator function of a closed convex set K in H, then $J_\varphi \equiv P_K$, the projection of H onto the closed convex set K. In this case Algorithm 2.1 reduces to the following method.

Algorithm 2.3. For a given $x_0 \in H$, compute the approximate solution x_n by the iterative schemes

$$x_{n+1} = (1 - a_n)x_n + a_n P_K[g(x_n) - \rho T x_n],$$

where $a_n \in [0, 1]$ for all $n \geq 0$. Algorithm 2.3 is a one-step method for solving the general variational inequalities (3). Noor [29] has studied the convergence analysis of Algorithm 2.3 and its various special cases.

From the above discussion, it is clear that Algorithm 2.1 is quite general and it includes several new and previously known algorithms for solving variational inequalities and related optimization problems.

We now recall some well known concepts and notions.

Definition 2.2. A mapping $T : H \to H$ is called μ-Lipschitz if for all $x, y \in H$, there exists a constant $\beta > 0$, such that

$$||Tx - Ty|| \leq \beta ||x - y||.$$

Definition 2.4. A mapping $T : H \to H$ is called $\in K$, there exists a constant $\alpha > 0$, such that

$$\langle Tx - Ty, x - y \rangle \geq \alpha ||x - y||^2.$$

Lemma 2.3 [46]. Suppose $\{\delta_k\}_{k=0}^{\infty}$ is a nonnegative sequence satisfying the following inequality:

$$\delta_{k+1} \leq (1 - \lambda_k)\delta_k + \sigma_k, \ k \geq 0$$

with $\lambda_k \in [0, 1]$, $\sum_{k=0}^{\infty} \lambda_k = \infty$, and $\sigma_k = o(\lambda_k)$. Then $\lim_{k\to\infty} \delta_k = 0$.

3. Main Results

In this section, we use the general resolvent equation technique to suggest and analyze some iterative methods for solving the general variational inclusion (1). For this purpose, we need the following result, which can be proved by using Lemma 2.2. However, for the sake of completeness and to convey an idea, we include its proof.

Lemma 3.1. The element $u \in H$ is a solution of (1), if and only if, $z \in H$ satisfies the resolvent equations (5), where

$$\begin{aligned} u &= J_A z, \\ z &= g(u) - \rho T u. \end{aligned}$$

Proof. Let $u \in H$ be a solution of (1). Then, from Lemma 2.3, we have

$$u = J_A[g(u) - \rho T u]. \tag{6}$$

$$z = g(u) - \rho T u. \tag{7}$$

Form (6) and (7), we have

$$\begin{aligned} u &= J_A z, \\ z &= g(u) - \rho T u, \end{aligned}$$

from which, we have

$$z = g J_A z - \rho T J_A z,$$

which is exactly the resolvent equation (5), the required result.

□

From Lemma 3.1, it follows that the variational inclusion (1) and the resolvent equation (5) are equivalent. This alternative equivalent formulation has been used to suggest and analyze a wide class of efficient and robust iterative methods for solving variational inclusions and related optimization problems, see [3-16] and the references therein.

Using Lemma 3.1, we now suggest and analyze a new iterative algorithm for solving the general variational inclusion (1) and this is the main motivation of this paper.

Algorithm 3.1. For a given $z_0 \in H$, compute the approximate solution z_{n+1} by the iterative schemes

$$u_n = (1-a_n)z_n + a_n J_A z_n \tag{8}$$

$$z_{n+1} = (1-a_n)z_n + a_n\{g(u_n) - \rho T u_n\} \tag{9}$$

where $a_n \in [0,1]$ for all $n \geq 0$.

If $g \equiv I$, the identity operator, then Algorithm 3.1 reduces to:

Algorithm 3.2. For a given $z_0 \in H$, compute the approximate solution z_{n+1} by the iterative schemes

$$\begin{aligned} u_n &= (1-a_n)z_n + a_n J_A z_n \\ z_{n+1} &= (1-a_n)z_n + a_n\{u_n - \rho T u_n\}. \end{aligned}$$

For $a_n = 1$, Algorithm 3.1 collapses to the following iterative method for solving variational inclusions (1).

Algorithm 3.3. For a given $z_0 \in H$, compute the approximate solution z_{n+1} by the iterative schemes

$$\begin{aligned} u_n &= J_A z_n \\ z_{n+1} &= g(u_n) - \rho T u_n. \end{aligned}$$

If φ is the indicator function of a closed convex set K in H, then $J_\varphi \equiv P_K$, the projection of H onto the closed convex set K. In this case Algorithm 2.1 reduces to the following method for solving general variational inequalities (3). These iterative methods are mainly due to Noor [29].

Algorithm 3.4. For a given $z_0 \in H$, compute the approximate solution z_{n+1} by the iterative schemes

$$\begin{aligned} u_n &= (1-a_n)z_n + a_n P_K z_n \\ z_{n+1} &= (1-a_n)z_n + a_n\{g(u_n) - \rho T u_n\} \end{aligned}$$

where $a_n \in [0,1]$ for all $n \geq 0$.

In brief, Algorithm 3.1 is quite general and includes several iterative methods for solving mixed variational inequalities and related optimization problems as special cases.

We now study those conditions under which the approximate solution obtained from Algorithm 3.1 to a solution of the variational inclusion (1).

Theorem 3.1. Let T be a strongly monotone with constant $\alpha > 0$ and Lipschitz continuous with constant $\beta > 0$ and let g be a strongly monotone with constant

$\sigma > 0$ and Lipschitz continuous with constant $\delta > 0$. If

$$\left|\rho - \frac{\alpha}{\beta^2}\right| < \frac{\sqrt{\alpha^2 - \mu^2(2k - k^2)}}{\beta^2}, \tag{10}$$

$$\alpha > \beta\sqrt{k(2-k)}, \quad k < 1, \tag{11}$$

where

$$k = \sqrt{1 - 2\sigma + \delta^2},$$

and $a_n \in [0,1]$, $\sum_{n=0}^{\infty} a_n = \infty$, then the approximate solution z_{n+1} obtained from Algorithm 3.1 converges to a solution z of the general resolvent equation (5).

Proof. Let $z^* \in H$ be a solution of (5). Then, from Lemma 3.1, we have

$$u^* = (1 - a_n)z^* + a_n J_A z^* \tag{12}$$

$$z^* = (1 - a_n)z^* + a_n\{g(u^*) - \rho T u^*\} \tag{13}$$

where $a_n \in [0,1]$ and $u^* \in H$ is a solution of (1). To prove the result, we need first to evaluate $||z_{n+1} - z^*||$ for all $n \geq 0$. From (9) and (14), we have

$$\begin{aligned} ||z_{n+1} - z^*|| &= ||(1 - a_n)z_n + a_n\{g(u_n) - \rho T u_n\} - (1 - a_n)z^* - a_n\{g(u^*) - \rho T u^*\}|| \\ &\leq (1 - a_n)||z_n - z^*|| + a_n||g(u_n) - g(u^*) - \rho(Tu_n - Tu^*)|| \\ &\leq (1 - a_n)\|z_n - z^*\| + a_n\|u_n - u^* - (g(u_n) - g(u^*))\| \\ &\quad a_n\|u_n - u^* - \rho(Tu_n - Tu^*)\|. \end{aligned} \tag{14}$$

From the strongly monotonicity and Lipschitz continuity of the operator T, we have

$$\begin{aligned} & ||u_n - u^* - \rho(Tu_n - Tu^*)||^2 \\ = \; & ||u_n - u^*||^2 - 2\rho\langle Tu_n - Tu^*, u_n - u^*\rangle + \rho^2||Tu_n - Tu^*||^2 \\ \leq \; & ||u_n - u^*||^2 - 2\rho\|u_n - u^*\|^2 + \beta^2\rho^2||u_n - u^*||^2] \\ = \; & \theta_1^2\|u_n - u^*\|^2, \end{aligned} \tag{15}$$

where

$$\theta_1 = \sqrt{1 - 2\rho\alpha + \rho^2\beta^2}. \tag{16}$$

In a similar way, we have

$$\begin{aligned} \|u_n - u^* - (g(u_n) - g(u^*))\| &\leq [1 - 2\sigma + \delta^2]\|u_n - u^*\|^2 \\ &= k^2\|u_n - u^*\|^2, \end{aligned} \tag{17}$$

where k is defined by (12).

Combining (15), (16) and (18), we have

$$\|z_{n+1} - z^*\| \leq (1 - a_n)\|z_n - z^*\| + a_n\theta\|u_n - u^*\|, \tag{18}$$

where $\theta = \theta_1 + k$.

From (8), (13) and the nonexpansivity of the operators J_A, we have

$$\begin{aligned} \|u_n - u^*\| &\leq (1 - a_n)\|z_n - z^*\| + a_n\|J_A z_n - J_A z^*\| \\ &\leq (1 - a_n)\|z_n - z^*\| + a_n\|z_n - z^*\| \\ &= \|z_n - z^*\|. \end{aligned} \tag{19}$$

From (19) and (20), we obtain that

$$\begin{aligned} ||z_{n+1} - z^*|| &\leq (1 - a_n)||z_n - z^*|| + a_n\theta\|z_n - z^*\| \\ &= [1 - a_n(1 - \theta)]||z_n - z^*||, \end{aligned}$$

and hence by Lemma 2.3, $\lim_{n\to\infty} ||z_n - z^*|| = 0$, completing the proof.

□

4. Computational Aspects

In this paper, we have shown that the general variational inclusions are equivalent to a new class of resolvent equations . This equivalence is used to suggest and analyze an iterative method for solving the general variational inclusions. It is worth mentioning that a special case of Algorithm 3.1 has been used by Pitonyak, Shi and Schiller [41] to find the numerical solutions of the obstacle problems. The results are encouraging and perform better than other methods. Noor, Wang and Xiu [39] has developed a very efficient and robust method using the technique of the Wiener-Hopf equations for solving the variational inequalities. It is interesting to use the technique and idea of this paper to develop other new iterative methods for solving the variational inequalities involving the nonexpansive operators. This is another direction for future work.

References

(1) W. F. Ames, Numerical Methods for Partial Differential Equations, Third Edition, Academic Press, New York, 1992.
(2) C. Baiocchi and A. Capelo, Variational and Quasi-Variational Inequalities, J. Wiley and Sons, New York, London, 1984.
(3) A. Bnouhachem, M. Aslam Noor and T. M. Rassias, Three-step iterative algorithms for mixed variational inequalities. Appl. Math. Comput. **183**(2006), 436-446.
(4) A. Bnouhachem and M. Aslam Noor, Numerical comparison between prediction-correction methods for general variational inequalities, Appl. Math. Comput. **186**(2007), 496-505.
(5) H. Brezis, Operateurs Maximaux Monotone et Semigroups de Contractions dan Espaces de Hilbert, North-Holland, Amsterdam, 1973.
(6) R.W. Cottle, F. Giannessi and J.L. Lions, Variational Inequalities and Complementarity Problems: Theory and Applications, J. Wiley and Sons, New York, 1980.
(7) J. Eckstein and B. P. Bertsekas, On the Douglas-Rachford splitting method and the proximal point algorithm for maximal monotone operators, Math. Prog. 55 (1992) 293-318.
(8) M. Fukushima, The primal Douglas-Rachford splitting algorithm for a class of monotone operators with applications to the traffic equilibrium problem, Math. Prog. 72 (1996) 1-15.
(9) F. Giannessi and A. Maugeri, Variational Inequalities and Network Equilibrium Problems, Plenum Press, New York, 1995.
(10) R. Glowinski, J.L. Lions and R. Trémolières, Numerical Analysis of Variational Inequalities, North-Holland, Amsterdam, 1981.
(11) S. Haubruge, V. H. Nguyen and J. J. Strodiot, Convergence analysis and applications of the Glowinski-Le Tallec splitting method for finding a zero of the sum of two maximal monotone operators, J. Optim. Theory Appl. 97 (1998) 645-673.
(12) P. L. Lions and B. Mercier, Splitting algorithms for the sum of two nonlinear operators, SIAM J. Numer. Anal. 16 (1979) 69-76.

(13) A. Moudafi and M. Thera, Finding a zero of the sum of two maximal monotone operators, J. Optim. Theory Appl. 97 (1997) 425-448.
(14) A. Moudafi and M. Aslam Noor, Sensitivity analysis of variational inclusions by the Wiener-Hopf equations technique, J. Appl. Math. Stochastic Anal. 12 (1999) 223-232.
(15) M. Aslam Noor, Some algorithms for general monotone mixed variational inequalities, Math. Computer Modelling 29(7)(1999) 1-9.
(16) M. Aslam Noor, Algorithms for general monotone mixed variational inequalities, J. Math. Anal. Appl. 229(1999) 330-343.
(17) M. Aslam Noor, An extraresolvent method for monotone mixed variational inequalities, Math. Computer Modelling 29(1999) 95-100.
(18) M. Aslam Noor, Some recent advances in variational inequalities, Part I, basic concepts, New Zealand J. Math. 26 (1997) 53-80.
(19) M. Aslam Noor, Some recent advances in variational inequalities, Part II, other concepts, New Zealand J. Math. 26 (1997) 229-255.
(20) M. Aslam Noor, Generalized set-valued variational inclusions and resolvent equations, J. Math. Anal. Appl. 228 (1998) 206-220.
(21) M. Aslam Noor, Set-valued mixed quasi variational inequalities and implicit resolvent equations, Math. Computer Modelling, 29(1999), 1-11.
(22) M.A. Noor, New approximation schemes for general variational inequalities, J. Math. Anal. Appl. 251 (2000) 217-229.
(23) M. Aslam Noor, Equivalence of variational inclusions with resolvent equations, Nonl. Anal., **42**(2000), 963-970.
(24) M. Aslam Noor, Three-step iterative algorithms for multivalued quasi variational inclusions, J. Math. Anal. Appl. 255(2001), 589-604.
(25) M. Aslam Noor, A Wiener-Hopf dynamical system for variational inequalities, New Zealand J. Math. **31**(2002), 173-182.
(26) M. Aslam Noor, Resolvent dynamical systems for mixed variational inequalities, Korean J. Comput. Appl. Math., **9**(2002), 15-26.
(27) M. Aslam Noor, Fundamentals of mixed quasi variational inequalities, Inter. J. Pure Appl. Math. 15(2004), 137-258.
(28) M.Aslam Noor, Some developments in general variational inequalities, Appl. Math. Comput. 152 (2004) 199-277.
(29) M. Aslam Noor, Differentiable nonconvex functions and general variational inequalities, Appl. Math. Comput., **199**(2008), 623-630.
(30) M. Aslam Noor and A. Bnouhachem, On an iterative algorithm for general variational inequalities, Appl. Math. Comput., **185**(2007), 155-168.
(31) M. Aslam Noor and K. Inayat Noor, On sensitivity analysis of general variational inequalities, Math. Comm. **13**(2008), 75-83.
(32) M. Aslam Noor and K. Inayat Noor, Projection algorithms for solving a system of general variational inequalities, Nonl. Anal. (2008).
(33) M. Aslam Noor and K. Inayat Noor, Three-step iterative methods for general variational inclusions in L^p-spaces, J. Appl. Math. Computing, **27**(2008), 281-291.
(34) M. Aslam Noor and K. Inayat Noor, Multivalued variational inequalities and resolvent equations, Math. Computer Modelling, **26**
(35) M. Aslam Noor and K. Inayat Noor, Sensitivity analysis for quasi variational inclusions, J. Math. Anal. Appl. 236(1999) 290-299.

(36) M. Aslam Noor and Th. M. Rassias, Resolvent equations for set-valued variational inequalities, Nonl. Anal., **42**(2000), 71-83.
(37) M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Some aspects of variational inequalities, J. Comput. Appl. Math. 47 (1993) 285-312.
(38) M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Set-valued resolvent equations and mixed variational inequalities, J. Math. Anal. Appl., 220 (1998) 741- 759.
(39) M. Aslam Noor, Y. J. Wang and N. Xiu, Some new projection methods for variational inequalities, Appl. Math. Computation, **137** (2003), 423-435.
(40) M. Patriksson, Nonlinear Programming and Variational Inequalities: A Unified Approach, Kluwer Academic Publishers, Dordrecht, 1998.
(41) A. Pitonyok, P. Shi and M. Shillor, On an iterative method for variational inequalities, Numer. Math. , **58**(1990), 231-242.
(42) R. T. Rockafellar, Monotone operators and the proximal point algorithms, SIAM J. Control Optim. 14 (1976) 877-898.
(43) P. Shi, Equivalence of Wiener-Hopf equations with variational inequalities, Proc. Amer. Math. Soc. , **111**(1991), 339- 346.
(44) G. Stampacchia, Formes bilineaires coercivities sur les ensembles convexes, C.R. Acad. Sci. Paris, 258 (1964) 4413-4416.
(45) W. Takahashi and M. Toyoda, Weak convergence theorems for nonexpansive mappings and monotone mappings, J. Optim. Theory Appl. 118 (2) (2003) 417-428.
(46) X.L. Weng, Fixed point iteration for local strictly pseudocontractive mappings, Proc. Amer. Math. Soc. 113 (1991) 727-731.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 117–127
ISSN 1930-1235: (2009)

ITERATIVE METHODS FOR GENERAL NONCONVEX VARIATIONAL INEQUALITIES

MUHAMMAD ASLAM NOOR

Abstract. In this paper, we introduce and consider some new classes of variational inequalities and the Wiener-Hopf equations. Using the projection technique, we establish the equivalence between the general nonconvex variational inequalities and the fixed point problems as well as the Wiener-Hopf equations. This alternative equivalent formulation is used to study the existence of a solution of the general convex variational inequalities. This equivalence is used to suggest and analyzed several projection iterative methods for solving the general nonconvex variational inequalities. Convergence criteria of these new iterative is also discussed under suitable conditions. Our method of proofs is very simple as compared with other techniques.

1. Introduction

Variational inequalities theory, which was introduced in early sixties, has emerged as an interesting and fascinating field of mathematical and engineering sciences. It is tool of great power that can be applied to a wide variety of problems, which arise in almost all branches of pure, applied, physical, regional and engineering sciences. It have been shown that the variational inequalities provide the most natural, direct, simple and efficient framework for the general treatment of wide range of problems, see [1-35] and the references therein.

In recent years, variational inequalities have been generalized in several directions using novel and innovative techniques. Noor [25,26,28] has introduced and considered some classes of variational inequalities in the setting of uniformly prox-regular sets. It is known [6,7,33] that the uniformly prox-regular sets are nonconvex and include the convex sets as special cases. Inspired and motivated by ongoing research in this direction, we introduce and consider a new class of general nonconvex variational inequalities involving two (nonlinear) operators. This work is continuation of our earlier work. Using the idea and technique of Noor [25,26,28], we show that the projection technique can be extended for the general nonconvex variational inequalities. We establish the equivalence between the general nonconvex variational inequalities and fixed point problems using essentially the projection technique. This equivalent alternative formulation is used to discuss the existence of a solution of the nonconvex variational inequalities, which is Theorem 3.1. We use this alternative equivalent formulation to suggest and analyze an implicit type

Received by the editors April 2, 2009 .
2000 *Mathematics Subject Classification.* Primary 49J40; Secondary 90C33.
Key words and phrases. Variational inequalities; nonconvex functions; fixed-point problem, Wiener-Hopf equations, convergence.

iterative methods for solving the nonconvex variational inequalities. In order to implement this new implicit method, we use the predictor-corrector technique to suggest a two-step method for solving the nonconvex variational inequalities, which is Algorithm 3.4. We also consider the convergence (Theorem 3.2) of the new iterative method under some suitable conditions. We have also suggested three-step iterative methods for solving nonconvex variational inequalities. Some special cases are also discussed.

We also introduce and consider the problem of solving the nonlinear Wiener-Hopf equations. Using essentially the projection technique, we establish the equivalence between the general nonconvex variational inequalities and the Wiener-Hopf equations. This alternative equivalent formulation is more general and flexible than the projection operator technique. This alternative equivalent formulation is used to suggest and analyze a number of iterative methods for solving the nonconvex variational inequalities. These iterative methods is the subject of Section 4. We also consider the convergence criteria of the proposed iterative methods under some suitable conditions. Several special cases are also discussed. Results obtained in this paper can be viewed as refinement and improvement of the previously known results for the variational inequalities and related optimization problems. We would like to point out that our method of proofs is very simple as compared with other techniques.

2. Preliminaries

Let H be a real Hilbert space whose inner product and norm are denoted by $\langle \cdot, \cdot \rangle$ and $\|.\|$ respectively. Let K be a nonempty and convex set in H.

We, first of all, recall the following well-known concepts from nonlinear convex analysis and nonsmooth analysis [7,33].

Definition 2.1. The proximal normal cone of K at $u \in H$ is given by

$$N_K^P(u) := \{\xi \in H : u \in P_K[u + \alpha\xi]\},$$

where $\alpha > 0$ is a constant and

$$P_K[u] = \{u^* \in K : d_K(u) = \|u - u^*\|\}.$$

Here $d_K(.)$ is the usual distance function to the subset K, that is

$$d_K(u) = \inf_{v \in K} \|v - u\|.$$

The proximal normal cone $N_K^P(u)$ has the following characterization.

Lemma 2.1. Let K be a nonempty, closed and convex subset in H. Then $\zeta \in N_K^P(u)$,
if and only if, there exists a constant $\alpha > 0$ such that

$$\langle \zeta, v - u \rangle \leq \alpha \|v - u\|^2, \quad \forall v \in K.$$

Definition 2.2. The Clarke normal cone, denoted by $N_K^C(u)$, is defined as

$$N_K^C(u) = \overline{co}[N_K^P(u)],$$

where $\overline{co}$ means the closure of the convex hull. Clearly $N_K^P(u) \subset N_K^C(u)$, but the converse is not true. Note that $N_K^P(u)$ is always closed and convex, whereas $N_K^C(u)$ is convex, but may not be closed (Ref. 24).

Poliquin et al. [33] and Clarke et al [7] have introduced and studied a new class of nonconvex sets, which are called uniformly prox-regular sets. This class

of uniformly prox-regular sets has played an important part in many nonconvex applications such as optimization, dynamic systems and differential inclusions.

Definition 2.3. For a given $r \in (0, \infty]$, a subset K_r is said to be normalized uniformly r-prox-regular if and only if every nonzero proximal normal to K_r can be realized by an r-ball, that is, $\forall u \in K_r$ and $0 \neq \xi \in N_{K_r}^P(u)$, one has

$$\langle (\xi)/\|\xi\|, v - u\rangle \leq (1/2r)\|v - u\|^2, \quad \forall v \in K.$$

It is clear that the class of normalized uniformly prox-regular sets is sufficiently large to include the class of convex sets, p-convex sets, $C^{1,1}$submanifolds (possibly with boundary) of H, the images under a $C^{1,1}$ diffeomorphism of convex sets and many other nonconvex sets; see [7,33]. It is clear that if $r = \infty$, then uniformly prox-regularity of K_r is equivalent to the convexity of K. It is known that if K_r is a uniformly prox-regular set, then the proximal normal cone $N_{K_r}^P(u)$ is closed as a set-valued mapping. Thus, we have $N_{K_r}^P(u) = N_{K_r}^C(u)$.

For a given nonlinear operator T, h, we consider the problem of finding $u \in K_r$ such that

$$\langle \rho Tu + u - h(u), h(v) - u\rangle \geq 0, \quad \forall v \in H : h(v) \in K_r, \tag{1}$$

which is called the *general nonconvex variational inequality.*

If $h \equiv I$, the identity operator, then problem (1) is equivalent to finding $u \in K_r$ such that

$$\langle \rho Tu, v - u\rangle \geq 0, \quad \forall v \in K_r, \tag{2}$$

which is known as the nonconvex variational inequality, studied and introduced by Noor [26].

We note that, if $K_r \equiv K$, the convex set in H, then problem (1) is equivalent to finding $u \in K$ such that

$$\langle \rho Tu + u - h(u), h(v) - u\rangle \geq 0, \qquad \forall v \in H : h(u) \in K. \tag{3}$$

Inequality of type (3) is called the *general variational inequality*, which was introduced and studied by Noor [28].

If $h(u) = u$, then problem (1) is equivalent to finding $u \in H : h(u) \in K_r$ such that

$$\langle T(h(u)), h(v) - h(u)\rangle \geq 0, \quad \forall v \in H : h(v) \in K_r, \tag{4}$$

which is also called the general nonconvex variational inequality.

If $K_r \equiv K$, the convex set in H, then problem (4) is equivalent to finding $u \in H : h(u) \in K$ such that

$$\langle T(h(u)), h(v) - h(u)\langle \geq 0, \forall v \in H; h(v) \in K, \tag{5}$$

which was introduced and studied by Noor [12] in 1988. It has been shown that the minimum of a differentiable nonconvex function can be characterized by the general variational inequality (5). See also [19] for its applications in applied sciences.

If $h \equiv I$, the identity operator, then problem (5) is equivalent to finding $u \in K$ such that

$$\langle Tu, v - u\rangle \geq 0, \quad v \in K, \tag{6}$$

which is known as the classical variational inequality, introduced and studied by Stampacchia [35] in 1964. It turned out that a number of unrelated obstacle, free, moving, unilateral and equilibrium problems arising in various branches of pure

and applied sciences can be studied via variational inequalities, see [1-35] and the references therein.

It is well-known that problem (6) is equivalent to finding $u \in K$ such that

$$0 \in Tu + N_K(u), \tag{7}$$

where $N_K(u)$ denotes the normal cone of K at u in the sense of convex analysis. Problem (7) is called the variational inclusion associated with variational inequality (6).

Similarly, if K_r is a nonconvex (uniformly prox-regular) set, then problem (1) is equivalent to finding $u \in K_r$ such that

$$0 \in \rho Tu - h(u) + u + \rho N_{K_r}^P(u), \tag{8}$$

where $N_{K_r}^P(u)$ denotes the normal cone of K_r at u in the sense of nonconvex analysis. Problem (8) is called the nonconvex variational inclusion problem associated with nonconvex variational inequality (1). This implies that the general nonconvex variational inequality (1) is equivalent to finding a zero of the sum of two monotone operators (8). This equivalent formulation plays a crucial and basic part in this paper. We would like to point out this equivalent formulation allows us to use the projection operator technique for solving the general nonconvex variational inequality (1).

We now recall the well known proposition which summarizes some important properties of the uniform prox-regular sets.

Lemma 2.2. Let K be a nonempty closed subset of H, $r \in (0, \infty]$ and set $K_r = \{u \in H : d(u, K) < r\}$. If K_r is uniformly prox-regular, then

i. $\forall u \in K_r, P_{K_r}(u) \neq \emptyset$.

ii. $\forall r^{'} \in (0, r)$, P_{K_r} is Lipschitz continuous with constant $\frac{r}{r-r^{'}}$ on $K_{r^{'}}$.

iii. The proximal normal cone is closed as a set-valued mapping.

We now consider the problem of solving the nonlinear Wiener-Hopf equations. To be more precise, let $Q_{K_r} = I - hP_{K_r}$, where P_{K_r} is the projection operator, h is the nonlinear operator and I is the identity operator. For given nonlinear operators T, h, consider the problem of finding $z \in H$ such that

$$TP_{K_r}z + \rho^{-1}Q_{K_r}z = 0. \tag{9}$$

Equations of the type (9) are called the general nonconvex Wiener-Hopf equations. Note that, if $r = \infty$ and $h =\equiv I$, the identity operator, then the nonlinear Wiener-Hopf equations are exactly the same Wiener-Hopf equations associated with the variational inequalities (6), which were introduced and studied by Shi [34]. This shows that the original Wiener-Hopf equations are the special case of the nonlinear Wiener-Hopf equations (9). The Wiener-Hopf equations technique has been used to study and develop several iterative methods for solving variational inequalities and related optimization problems, see [9-26].

Definition 2.4. An operator $T : H \to H$ is said to be:

(i) *strongly monotone*, if and only if, there exists a constant $\alpha > 0$ such that

$$\langle Tu - Tv, u - v\rangle \geq \alpha||u - v||^2, \quad \forall u, v \in H.$$

(ii) *Lipschitz continuous*, if and only if, there exists a constant $\beta > 0$ such that

$$||Tu - Tv|| \leq \beta||u - v||, \quad \forall u, v \in H.$$

3. Projection Methods

In this section, we establish the equivalence between the nonconvex variational inequality (1) and the fixed point problem using the projection operator technique. This alternative formulation is used to discuss the existence of a solution of the problem (1) and to suggest some new iterative methods for solving the general nonconvex variational inequality (1).

Lemma 3.1. $u \in K_r$ is a solution of the general nonconvex variational inequality (1) if and only if $u \in K_r$ satisfies the relation

$$u = P_{K_r}[h(u) - \rho Tu], \tag{10}$$

where P_{K_r} is the projection of H onto the uniformly prox-regular set K_r.

Proof. Let $u \in K_r$ be a solution of (1). Then, for a constant $\rho > 0$,

$$\begin{aligned} 0 &\in u + \rho N^P_{K_r}(u) - (h(u) - \rho Tu) = (I + \rho N^P_{K_r})(u) - (h(u) - \rho Tu) \\ &\iff \\ u &= (I + \rho N^P_{K_r})^{-1}[h(u) - \rho Tu] = P_{K_r}[h(u) - \rho Tu], \end{aligned}$$

where we have used the well-known fact that $P_{K_r} \equiv (I + N^P_{K_r})^{-1}$. □

Lemma 3.1 implies that the general nonconvex variational inequality (1) is equivalent to the fixed point problem (10). This alternative equivalent formulation is very useful from the numerical and theoretical point of views.

We rewrite the the relation (10) in the following form

$$F(u) = P_{K_r}[h(u) - \rho Tu], \tag{11}$$

which is used to study the existence of a solution of the general nonconvex variational inequality (1).

We now study those conditions under which the general nonconvex variational inequality (1) has a solution and this is the main motivation of our next result.

Theorem 3.1. Let P_{K_r} be the Lipschitz continuous operator with constant $\delta = \frac{r}{r-r'}$. Let T, h be strongly monotone with constants $\alpha > 0, \sigma > 0$ and Lipschitz continuous with constants $\beta > 0, \delta > 0$, respectively. If there exists a constant $\rho > 0$ such that

$$\begin{aligned} |\rho - \frac{\alpha}{\beta^2}| &< \frac{\sqrt{\delta^2\alpha^2 - \beta^2(\delta^2 - (1-\delta k)^2))}}{\delta\beta^2}, \\ \delta\alpha &> \beta\sqrt{\delta^2 - (1-\delta k)^2}, \quad < \delta(1+k), \end{aligned} \tag{12}$$

then there exists a solution of the problem (1).

Proof. From Lemma 3.1, it follows that problems (10) and (1) are equivalent. Thus it is enough to show that the map $F(u)$, defined by (11), has a fixed point. For all $u \neq v \in K_r$, we have

$$\begin{aligned} ||F(u) - F(v)|| &= \|P_{K_r}[h(u) - \rho Tu] - P_{K_r}[h(v) - \rho Tv]\| \\ &\leq \delta\|h(u) - h(v) - \rho(Tu - Tv)\| \\ &\leq \delta\left\{\|u - v - (h(u) - h(v)) + \|u - v - \rho(Tu - Tv)\|\right\}, \end{aligned} \tag{13}$$

where we have used the fact that the operator P_{K_r} is a Lipschitz continuous operator with constant δ.

Since the operator T is strongly monotone with constant $\alpha > 0$ and Lipschitz continuous with constant $\beta > 0$, it follows that

$$\begin{aligned} ||u - v - \rho(Tu - Tv)||^2 &\leq ||u - v||^2 - 2\rho\langle Tu - Tv, u - v\rangle + \rho^2||Tu - Tv||^2 \\ &\leq (1 - 2\rho\alpha + \rho^2\beta^2)||u - v||^2. \end{aligned} \tag{14}$$

In a similar way, we have

$$\|u - v - (h(u) - h(v))\| \leq \sqrt{1 - 2\sigma + \delta^2}\|u - v|, \tag{15}$$

where $\sigma > 0$ is the strongly monotonicity constant and $\delta > 0$ is the Lipschitz continuity constant of the operator h respectively.

From (13), (14) and (15), we have

$$\begin{aligned} ||F(u) - F(v)|| &\leq \delta\left\{k + \sqrt{1 - 2\alpha\rho + \beta^2\rho^2)}\right\}||u - v|| \\ &= \theta||u - v||, \end{aligned}$$

where

$$\theta = \delta\{\sqrt{1 - 2\alpha\rho + \beta^2\rho^2} + k\} \tag{16}$$

$$k = \sqrt{1 - 2\sigma + \delta^2}. \tag{17}$$

From (12), it follows that $\theta < 1$, which implies that the map $F(u)$ defined by (11), has a fixed point, which is the unique solution of (1). □

This fixed point formulation (10) is used to suggest the following iterative method for solving the nonconvex variational inequality (1).

Algorithm 3.1. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative scheme

$$u_{n+1} = (1 - \alpha_n)u_n + \alpha_n\{P_{K_r}[h(u_n) - \rho Tu_n]\}, \quad n = 0, 1, 2, \ldots, \tag{18}$$

where $\alpha_n \in [0, 1], \forall n \geq 0$ is a constant. Algorithm 3.1 is also called the Mann iteration process.

For $\alpha_n = 1$, Algorithm 3.1 collapse to:

Algorithm 3.2. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative scheme

$$h(u_{n+1}) = P_{K_r}[h(u_n) - \rho Tu_n], \quad n = 0, 1, 2, \ldots$$

We again use the fixed formulation to suggest and analyze an iterative method for solving the nonconvex variational inequalities (1) as:

Algorithm 3.3. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative scheme

$$h(u_{n+1}) = P_{K_r}[h(u_{n+1}) - \rho Tu_{n+1}], \quad n = 0, 1, 2, \ldots$$

Algorithm 3.3 is an implicit type iterative method, which is difficult to implement. To implement Algorithm 3.3, we use the predictor-corrector technique. Here we use the Algorithm 3.1 as a predictor and Algorithm 3.3 as a corrector. Consequently, we have the following iterative method

Algorithm 3.4. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative schemes

$$\begin{aligned} y_n &= P_{K_r}[h(u_n) - \rho Tu_n] \\ u_{n+1} &= P_{K_r}[h(y_n) - \rho Ty_n], \quad n = 0, 1, 2, \ldots \end{aligned}$$

which is called the two-step or splitting type iterative method for solving the general nonconvex variational inequalities (1). It is worth mentioning that Algorithm 3.4 can be suggested by using the updating the technique of the solution.

In this paper, we suggest and analyze the following two-step iterative method for solving the general nonconvex variational inequalities (1).

Algorithm 3.5. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative schemes

$$\begin{aligned} y_n &= (1-\beta_n)u_n + \beta_n\{P_{K_r}[h(u_n) - \rho T u_n]\} \\ u_{n+1} &= (1-\alpha_n)u_n + \alpha_n\{P_{K_r}[h(y_n) - \rho T y_n]\}, \quad n = 0, 1, 2, \ldots, \end{aligned}$$

where $\alpha_n, \beta_n \in [0,1], \quad \forall n \geq 0$.

Clearly for $\alpha_n = \beta_n = 1$, Algorithm 3.5 reduces to Algorithm 3.4. It is worth mentioning that, if $r = \infty$, then the nonconvex set K_r reduces to a convex set K. Consequently Algorithms 3.1- 3.5 collapse to the following algorithms for solving the classical variational inequalities (6). We would like to point that Algorithm 3.4 appears to be a new one for solving the variational inequalities (3)

We now consider the convergence analysis of Algorithm 3.1 and this is the main motivation of our next result. In a similar way, one can consider the convergence criteria of other Algorithms.

Theorem 3.2. Let P_{K_r} be the Lipschitz continuous operator with constant $\delta = \frac{r}{r-r'}$. Let the operators $T, h : H \longrightarrow H$ be strongly monotone with constants $\alpha > 0, \sigma > 0$ and Lipschitz continuous with constants with $\beta > 0, \delta > 0$, respectively. If (12) holds, $\alpha_n, \in [0,1], \quad \forall n \geq 0$ and $\sum_{n=0}^{\infty} \alpha_n = \infty$, then the approximate solution u_n obtained from Algorithm 3.1 converges to a solution $u \in K_r$ satisfying the nonconvex variational inequality (1).

Proof. Let $u \in K_r$ be a solution of the nonconvex variational inequality (1). Then, using Lemma 3.1, we have

$$u = (1-\alpha_n)u + \alpha_n\{P_{K_r}[h(u) - \rho T u]\}, \tag{19}$$

where $0 \leq \alpha_n \leq 1$ is a constant.

From (14)-(19) and using the Lipschitz continuity of the projection P_{K_r} with constant δ, we have

$$\begin{aligned} ||u_{n+1} - u|| &= ||(1-\alpha_n)(u_n - u) + \alpha_n\{P_{K_r}[h(u_n) - \rho T u_n] - P_{K_r}[h(u) - \rho T u]\}|| \\ &\leq (1-\alpha_n)\|u_n - u\| + \alpha_n\|P_{K_r}[h(u_n) - \rho T u_n] - P_{K_r}[h(u) - \rho T u]\| \\ &\leq (1-\alpha_n)\|u_n - u\| + \alpha_n\delta\left\{\|u_n - u + \rho(Tu_n - Tu)\|\right\} \\ &\quad + \alpha_n\|u_n - u - (h(u_n) - h(u))\| \\ &\leq (1-\alpha_n)\|u_n - u\| + \alpha_n\delta\{k + \sqrt{1 - 2\alpha\rho + \beta^2\rho^2}\}\|u_n - u\| \\ &= \left[1 - \alpha_n(1-\theta)\right]\|u_n - u\| \\ &\leq \prod_{i=0}^{n}\left[1 - \alpha_i(1-\theta)\right]\|u_0 - u\|, \end{aligned}$$

where, using (12), we have

$$\theta = \delta\left\{k + \delta\sqrt{1 - 2\rho\alpha + \beta^2\rho^2}\right\} < 1.$$

Since $\sum_{n=0}^{\infty}\alpha_n$ diverges and $1-\theta>0$, we have $\lim_{n\to\infty}\{\prod_{i=0}^{n}[1-(1-\theta)\alpha_i]\}=0$. Consequently the sequence $\{u_n\}$ convergences strongly to u. This completes the proof. □

4. Wiener-Hopf Equations Technique

In this section, we first establish the equivalence between the nonconvex variational inequality (1) and the Wiener-Hopf equations (9) using essentially the projection method. This equivalence is used to suggest and analyze some iterative methods for solving the variational inclusions.

Using Lemma 3.1, we show that the general nonconvex variational inequality (1) are equivalent to the Wiener-Hopf equations (9).

Lemma 4.1. The nonconvex variational inequality (1) has a solution $u\in K_r$ if and only if the Wiener-Hopf equations (9) have a solution $z\in H$, provided

$$u = P_{K_r}z \tag{20}$$

$$z = h(u)-\rho Tu, \tag{21}$$

where $\rho>0$ is a constant.

Proof. Let $u\in K_r$ be a solution of (1). Then, from Lemma 3.1, we have

$$u=P_{K_r}[h(u)-\rho Tu]. \tag{22}$$

Taking $z=h(u)-\rho Tu$ in (22), we have

$$u=P_{K_r}z. \tag{23}$$

From (22) and (23), we have

$$z=h(u)-\rho Tu=hP_{K_r}z-\rho TP_{K_r}z,$$

which shows that $z\in H$ is a solution of the Wiener-Hopf equations (9). This completes the proof. □

From Lemma 4.1, we conclude that the general nonconvex variational inequality (1) and the Wiener-Hopf equations (9) are equivalent. This alternative formulation plays an important and crucial part in suggesting and analyzing various iterative methods for solving variational inequalities and related optimization problems. In this paper, by suitable and appropriate rearrangement, we suggest a number of new iterative methods for solving the general nonconvex variational inequality (1).

I. The Wiener-Hopf equations (9) can be written as

$$Q_{K_r}z=-\rho TP_{K_r}z,$$

which implies that, using(4.2)

$$z=hP_{K_r}z-\rho TP_{K_r}z=h(u)-\rho Tu.$$

This fixed point formulation enables us to suggest the following iterative method for solving the nonconvex variational inequality (1).

Algorithm 4.1. For a given $z_0\in H$, compute z_{n+1} by the iterative schemes

$$u_n = P_{K_r}z_n \tag{24}$$

$$z_{n+1} = (1-\alpha_n)z_n+\alpha_n\{h(u_n)-\rho Tu_n,\}\quad n=0,1,2,\ldots\ldots, \tag{25}$$

where $0\le\alpha_n\le 1$, for all $n\ge 0$ and $\sum_{n=0}^{\infty}\alpha_n=\infty$.

II. The Wiener-Hopf equations (9) may be written as

$$\begin{aligned} z &= hP_{K_r}z - \rho TP_{K_r}z + (1-\rho^{-1})Q_{K_r}z \\ &= h(u) - \rho Tu + (1-\rho^{-1})Q_{K_r}z. \end{aligned}$$

Using this fixed point formulation, we suggest the following iterative method.

Algorithm 4.2. For a given $z_0 \in H$, compute z_{n+1} by the iterative schemes

$$\begin{aligned} u_n &= P_{K_r}z_n \\ z_{n+1} &= (1-\alpha_n)z_n + \alpha_n\{h(u_n) - \rho Tu_n + (1-\rho^{-1})Q_{K_r}z_n,\} \quad n = 0,1,2,\ldots, \end{aligned}$$

where $0 \leq \alpha_n \leq 1$, for all $n \geq 0$ and $\sum_{n=0}^{\infty}\alpha_n = \infty$.

III. If the operator T is linear and T^{-1} exists, then the Wiener-Hopf equations (9) can be written as

$$z = (I - \rho^{-1}T^{-1})Q_{K_r}z,$$

which allows us to suggest the iterative method.

Algorithm 4.3. For a given $z_0 \in H$, compute z_{n+1} by the iterative scheme

$$z_{n+1} = (1-\alpha_n)z_n + \alpha_n\{(I - \rho^{-1}T^{-1})Q_{K_r}z_n,\} \quad n = 0,1,2\ldots,$$

where $0 \leq \alpha_n \leq 1$, for all $n \geq 0$ and $\sum_{n=0}^{\infty}\alpha_n = \infty$.

We would like to point out that one can obtain a number of iterative methods for solving the general nonconvex variational inequality (1) for suitable and appropriate choices of the operators T, h and the space H. This shows that iterative methods suggested in this paper are more general and unifying ones.

We now study the convergence analysis of Algorithm 4.1. In a similar way, one can analyze the convergence analysis of other iterative methods.

Theorem 4.1. Let the operators T, A satisfy all the assumptions of Theorem 3.1. If the condition (12) holds, $\alpha_n \in [0,1]$, $\forall n \geq 0$, and $\sum_{n=0}^{\infty}\alpha_n = \infty$, then the approximate solution $\{z_n\}$ obtained from Algorithm 4.1 converges to a solution $z \in H$ satisfying the Wiener-Hopf equation (9) strongly.

Proof. Let $u \in H$ be a solution of (1). Then, using Lemma 4.1, we have

$$z = (1-\alpha_n)z + \alpha_n\{h(u) - \rho Tu\}, \tag{26}$$

where $0 \leq \alpha_n \leq 1$, and $\sum_{n=0}^{\infty}a_n = \infty$.

From(25), (26), (14) and (15), we have

$$\begin{aligned} \|z_{n+1} - z\| &\leq (1-\alpha_n)\|z_n - z\| + \alpha_n\|h(u_n) - h(u) - \rho(Tu_n - Tu)\| \\ &\leq (1-\alpha_n)\|z_n - z\| + \alpha_n\left\{k + \sqrt{1 - 2\rho\alpha + \beta^2\rho^2}\right\}\|u_n - u\|. \end{aligned} \tag{27}$$

Also from (24), (20) and the Lipschitz continuity of the projection operator P_{K_r} with constant δ, we have

$$\|u_n - u\| = \|P_{K_r}z_n - P_{K_r}z\| \leq \delta\|z_n - z\|. \tag{28}$$

Combining (27), and (28), we have

$$\|z_{n+1} - z\| \leq (1-\alpha_n)\|z_n - z\| + \alpha_n\theta\|z_n - z\|. \tag{29}$$

From (12), we see that $\theta < 1$ and consequently

$$\begin{aligned} \|z_{n+1} - z\| &\leq (1-\alpha_n)\|z_n - z\| + \alpha_n\theta\|z_n - z\| \\ &= [1-(1-\theta)\alpha_n]\|z_n - z\| \\ &\leq \prod_{i=0}^{n}[1-(1-\theta)\alpha_i]\|z_0 - z\|. \end{aligned}$$

Since $\sum_{n=0}^{\infty}\alpha_n$ diverges and $1-\theta > 0$, we have $\lim_{n\to\infty}\prod_{i=0}^{n}[1-(1-\theta)\alpha_i] = 0$. Consequently the sequence $\{z_n\}$ convergences strongly to z in H, the required result. □

Acknowledgement. The author would like to express his gratitude to Dr. M. Junaid Zaidi, Rector, CIIT, for providing excellent research facilities.

References

[1] H. Brezis, Operateurs maximaux monotone, Mathematical Studies, No. 5, North-Holland, 1973.
[2] A. Bnouhachem and M. Aslam Noor, Numerical methods for general mixed variational inequalities, Appl. Math. Comput. **204**(2008), 27-36.
[3] A. Bnouhachem, M. Aslam Noor and M. Khalfaoui, Modified descent-projection method for solving variational inequalities, Appl. Math. Comput. **190**(2008), 1691-1700.
[4] A. Bnouhachem and M. Aslam Noor, Numerical comparison between prediction-correction methods for general variational inequalities, Appl. Math. Comput. **186**(2007), 496-505.
[5] A. Bnouhachem and M. Aslam Noor, Inexact proximal point method for general variational inequalities, J. Math. Anal. Appl. **324**(2006), 1195-1212.
[6] M. Bounkhel, L. Tadj and A. Hamdi, Iterative schemes to solve nonconvex variational problems, J. Inequal. Pure Appl. Math.,**4**(2003), 1-14.
[7] F. H. Clarke, Y. S. Ledyaev and P. R. Wolenski, Nonsmooth Analysis and Control Theory, Springer-Verlag, Berlin, 1998.
[8] D. Kinderlehrer and G. Stampacchia, An Introduction to Variational Inequalities and Their Applications, SIAM, Philadelphia, 2000.
[9] J. L. Lions and G. Stampacchia, Variational inequalities, Comm. Pure Appl. Math. **20**(1967), 493-512.
[10] P. L. Lions and B. Mercier, Splitting algorithms for the sum of two nonlinear operators, SIAM J. Numer. Anal. **16**(1979), 964-979.
[11] M. Aslam Noor, General variational inequalities, Appl. Math. Letters, **1**(1988), 119-121.
[12] M. Aslam Noor, Quasi variational inequalities, Appl. Math. Letters, **1**(1988), 367-370.
[13] M. Aslam Noor, Wiener-Hopf equations and variational inequalities, J. Optim. Theory Appl. **79**(1993), 197-206.
[14] M. Aslam Noor, Some recent advances in variational inequalities, Part II, other concepts, New Zealand J. Math. **26**(1997), 229-255.
[15] M. Aslam Noor, New approximation schemes for general variational inequalities, J. Math. Anal. Appl. , **251**(2000), 217-229.
[16] M. Aslam Noor, A Wiener-Hopf dynamical system for variational inequalities, New Zealand J. Math. **31**(2002), 173-182.
[17] M. Aslam Noor, New extragradient-type methods for general variational inequalities. J. Math. Anal. Appl. **277**(2003), 379-395.
[18] M. Aslam Noor, Mixed quasi variational inequalities, Appl. Math. Computation, **146**(2003), 553-578.
[19] M. Aslam Noor, Some developments in general variational inequalities, Appl. Math. Computation, **152**(2004), 199-277.
[20] M. Aslam Noor, Iterative schemes for nonconvex variational inequalities, J. Optim. Theory Appl. **121**(2004), 385-395.
[21] M. Aslam Noor, Fundamentals of mixed quasi variational inequalities, Inter. J. Pure Appl. Math. **15**(2004), 137-258.

[22] M. Aslam Noor, Fundamentals of equilibrium problems, Math. Inequal. Appl. **9**(2006), 529-566.
[23] M. Aslam Noor, Merit functions for general variational inequalities, J. Math. Anal. Appl. **316**(2006), 736-752.
[24] M. Aslam Noor, Differentiable nonconvex functions and general variational inequalities, Appl. Math. Computation, **199** (2008), 623-630
[25] M. Aslam Noor, Some iterative methods for general nonconvex variational inequalities, Comput. Math. Modeling, **21**(2010).
[26] M. Aslam Noor, Projection methods for nonconvex variational inequalities, Optim. Letters(2009), DOI: 10.1007/s11590-009-0121.1.
[27] M. Aslam Noor, Extended general variational inequalities, Appl. Math. Letters, **22**(2009), 182-186.
[28] M. Aslam Noor, Variational Inequalities and Applications, Lecture Notes, Mathematics Department, COMSATS Institute of Information Technology, Islamabad, Pakistan, 2007-2009.
[29] M. Aslam Noor and K. Inayat Noor, Projection algorithms for solving system of general variational inequalities, Nonl. Anal. **70**(2009), 2700-2706.
[30] M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Some aspects of variational inequalities, J. Comput. Appl. Math. **47**(1993), 285-312.
[31] M. Aslam Noor, K. Inayat Noor and H. Yaqoob, On general mixed variational inequalities, Acta Appl. Math. (2008), DOI 10.1007/s10440-008-9402.4
[32] L. P. Pang, J. Shen and H. S. Song, A modified predictor-corrector algorithm for solving nonconvex generalized variational inequalities, Computers Math. Appl. **54**(2007), 319-325.
[33] R. A. Poliquin, R. T. Rockafellar and L. Thibault, Local differentiability of distance functions, Trans. Amer. Math. Soc., **352**(2000), 5231-5249.
[34] P. Shi, Equivalence of variational inequalities with Wiener-Hopf equations, Proc. Amer. Math. Soc., **111**(1991), 339-346.
[35] G. Stampacchia, Formes bilineaires coercitives sur les ensembles convexes, C. R. Acad. Sci, Paris, **258**(1964), 4413-4416

COMSATS Institute of Information Technology, Mathematics Department, Islamabad, Pakistan
E-mail address: noormaslam@gmail.com and noormaslam@hotmail.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 4, Pages 131–160
ISSN 1930-1235: (2009)

AUTOMORPHISM GROUPS OF CYCLIC CURVES DEFINED OVER FINITE FIELDS OF ANY CHARACTERISTICS

R. Sanjeewa

Dept. of Mathematics
Oakland University
Rochester, MI. USA.
rsanjeew@oakland.edu

Abstract. In this paper we determine automorphism groups of cyclic algebraic curves defined over finite fields of any characteristic.

1. Introduction

Let $g \geq 2$ be a fixed integer and k an algebraically closed field of characteristic $p \geq 0$ and let $\mathcal{X}_g$ is an irreducible algebraic curve defined over k. Determining the list of group which occur as automorphism groups of $\mathcal{X}_g$ is very old problem in mathematics. Mathematicians are working on this problem more than a century now. In 1893 Hurwitz proved that the order of such group is $\leq 84(g-1)$ when $p = 0$; see [5]. After 80 years, Stichtenoth et al. proved that the bound is $16g^4$ for $p > 0$; see [23]. In any case, the group of automorphisms is a finite group. There are hundreds of papers on the structure of such groups, determining the equation of the curve when the group is given, determining the group when the curve is given, etc. T. Shaska determines the list of groups for hyperelliptic curves when $p = 0$, see [20] and K. Magaard et. al. determine the list of groups for any given $g \geq 2$ when $p = 0$. Such results are based on an exhaustive computer search of all possible ramification structures for a given g and a deep understanding of Hurwitz spaces for a given genus g, a group G, and the ramification structure for the covering $\mathcal{X}_g \to \mathcal{X}_g^G$. The case of positive characteristic is still an open problem.

In most cases there is a cyclic subgroup $C_n \lhd G$ such that $g(\mathcal{X}^{C_n}) = 0$. Such curves are called *cyclic curves*. In this paper we determine groups G which occur as automorphism groups of cyclic curves in any characteristic and for any genus $g \geq 2$.

In section 2, we cover basic facts on automorphism groups of cyclic curves. Let $G = \mathrm{Aut}(\mathcal{X}_g)$ automorphism group of cyclic curve $\mathcal{X}_g$, $C_n = \langle w \rangle$ such that $g(\mathcal{X}^{C_n}) = 0$. The group $\bar{G} := \mathrm{Aut}(\mathcal{X}_g)/\langle w \rangle$ is called the reduced automorphism group. This group $\bar{G}$ is embedded in $PGL_2(k)$ and therefore is isomorphic to one of C_m, D_m, A_4, S_4, A_5, *a semidirect product of elementary Abelian group with cyclic group*, $PSL(2,q)$ and $PGL(2,q)$ cf. Lemma 1. We determine a rational functions $\phi(x)$ that generates the fixed field $k(x)^{\bar{G}}$.

Key words and phrases. algebraic curves; automorphism groups.

In the section 3, we determine ramification signature of each cover $\Phi(x) : \mathcal{X} \to \mathcal{X}^G$ by using the ramification of $\bar{G}$. By considering the lifting of ramified points of the cover Φ, we divide each $\bar{G}$ into sub cases. Then we are able to find automorphism group G for each sub cases. For some cases, we give presentation for G. The moduli space of covers Φ with fixed group G and ramification signature $\mathbf{C}$ is a Hurwitz space $\mathcal{H}$. There is a map from $\mathcal{H}$ to the moduli space of genus g algebraic curves $\mathcal{H}_g$. The image of this map is a subvariety of $\mathcal{H}_g$ and denoted by $\mathcal{H}(G, \mathbf{C})$. Since we know the signature of the curve, we use Hurwitz genus formula to calculate dimension of $\mathcal{H}(G, \mathbf{C})$. We list all possible signatures $\mathbf{C}$ and dimension of the locus $\mathcal{H}(G, \mathbf{C})$. Then we list automorphism groups as theorems for each $\bar{G}$.

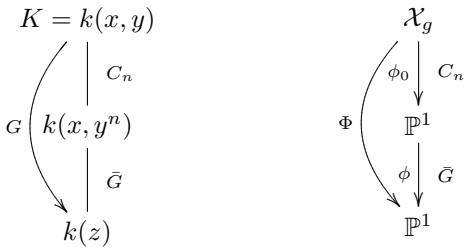
In section 4, we combine Theorems 3.2 - 3.12 altogether to make main theorem. In our main theorem, we list all possible automorphism groups of genus $g \geq 2$ cyclic curves define over the finite field of characteristic $p \neq 2$. We are able to give presentations for some of automorphism groups.

Notation : Through this paper k denotes an algebraically closed field of characteristic $\neq 2$, g an integer ≥ 2, and $\mathcal{X}_g$ a cyclic curve of genus g defined over k. For a given curve $\mathcal{X}$, $g(\mathcal{X})$ denotes its genus.

2. Preliminaries

Let k be an algebraically closed field of characteristic p and $\mathcal{X}_g$ be a genus g cyclic curve given by the equation $y^n = f(x)$ for some $f \in k[x]$. Let $K := k(x, y)$ be the function field of $\mathcal{X}_g$. Then $k(x)$ is degree n genus zero subfield of K. Let $G = \mathrm{Aut}(K/k)$. Since $C_n := Gal(K/k(x)) = \langle w \rangle$, with $w^n = 1$ such that $\langle w \rangle \lhd G$, then group $\bar{G} := G/C_n$ and $\bar{G} \leq PGL_2(k)$. Hence $\bar{G}$ is isomorphic to one of the following: C_m, D_m, A_4, S_4, A_5, *semidirect product of elementary Abelian group with cyclic group*, $PSL(2, q)$ and $PGL(2, q)$, see [16].

The group $\bar{G}$ acts on $k(x)$ via the natural way. The fixed field is a genus 0 field, say $k(z)$. Thus z is a degree $|\bar{G}|$ rational function in x, say $z = \phi(x)$. We illustrate with the following diagram:



Let $\phi_0 : \mathcal{X}_g \to \mathbb{P}^1$ be the cover which corresponds to the degree n extension $K/k(x)$. Then $\Phi := \phi \circ \phi_0$ has monodromy group $G := \mathrm{Aut}(\mathcal{X}_g)$. From the basic covering theory, the group G is embedded in the group S_l where $l = deg\ \Phi$. There is an r-tuple $\overline{\sigma} := (\sigma_1, ..., \sigma_r)$, where $\sigma_i \in S_l$ such that $\sigma_1, ..., \sigma_r$ generate G and $\sigma_1 ... \sigma_r = 1$. The signature of Φ is an r-tuple of conjugacy classes $\mathbf{C} := (C_1, ..., C_r)$ in S_l such that C_i is the conjugacy class of σ_i. We use the notation n to denote the conjugacy class of permutations which is cycle of length n. Using the signature of $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ one finds out the signature of $\Phi : \mathcal{X}_g \to \mathbb{P}^1$ for any given g and G.

Let E be the fixed field of G, the Hurwitz genus formula states that

$$2(g_K - 1) = 2(g_E - 1)|G| + deg(\mathfrak{D}_{K/E}) \tag{1}$$

with g_K and g_E the genera of K and E respectively and $\mathfrak{D}_{K/E}$ the different of K/E. Let $\overline{P}_1, \overline{P}_2, ..., \overline{P}_r$ be ramified primes of E. If we set $d_i = deg(\overline{P}_i)$ and let e_i be the ramification index of the $\overline{P}_i$ and let β_i be the exponent of $\overline{P}_i$ in $\mathfrak{D}_{K/E}$. Hence, (1) may be written as

$$2(g_K - 1) = 2(g_E - 1)|G| + |G| \sum_{i=1}^{r} \frac{\beta_i}{e_i} d_i \tag{2}$$

If $\overline{P}_i$ is tamely ramified then $\beta_i = e_i - 1$ or if $\overline{P}_i$ is wildly ramified then $\beta_i = e_i^* q_i + q_i - 2$ with $e_i = e_i^* q_i$, e_i^* relatively prime to p, q_i a power of p and $e_i^* | q_i - 1$. For fixed G, $\mathbf{C}$ the family of covers $\Phi : \mathcal{X}_g \to \mathbb{P}^1$ is a Hurwitz space $\mathcal{H}(G, \mathbf{C})$. $\mathcal{H}(G, \mathbf{C})$ is an irreducible algebraic variety of dimension $\delta(G, \mathbf{C})$. Using equation (2) and signature $\mathbf{C}$ one can find out the dimension for each G.

Next we want to determine the cover $z = \phi(x) : \mathbb{P}^1 \to \mathbb{P}^1$ for all characteristics. Notice that the case of $char(k) = 0$ is known, see [20].

We define a semidirect product of elementary Abelian group with cyclic group as follows.

$$K_m := \langle \{\sigma_a, t | a \in \mathcal{U}_m\} \rangle$$

where $t(x) = \xi^2 x, \quad \sigma_a(x) = x + a$, for each $a \in \mathcal{U}_m$,

$$\mathcal{U}_m := \{a \in k | (a \prod_{j=0}^{\frac{p^t-1}{m}-1} (a^m - b_j)) = 0\}$$

$b_j \in \mathbb{F}_q^*$, $m | p^t - 1$ and ξ is a primitive $2m$-th root of unity. Obviously $\mathcal{U}_m$ is a subgroup of the additive group of k.

Lemma 1. *Let k be an algebraically closed field of characteristic p, $\bar{G}$ be a finite subgroup of $PGL_2(k)$ acting on the field $k(x)$. Then, $\bar{G}$ is isomorphic to one of the following groups C_m, D_m, A_4, S_4, A_5, $U = C_p^t$, K_m, $PSL_2(q)$ and $PGL_2(q)$, where $q = p^f$ and $(m, p) = 1$. Moreover, the fixed subfield $k(x)^{\bar{G}} = k(z)$ is given by Table 1, where $\alpha = \frac{q(q-1)}{2}$, $\beta = \frac{q+1}{2}$. H_t is a subgroup of the additive group of k with $|H_t| = p^t$ and $b_j \in k^*$.*

Proof. It is well known that $\bar{G}$ is isomorphic to $C_n, D_n, A_4, S_4, A_5, U, K_m, PSL(2, q)$ and $PGL(2, q)$; see [16]. Cases 1) .. 5) are the same as in characteristic zero; see [21]. We briefly display the generators of $\bar{G}$ is such cases. The reader can check that z is fixed by such generators.

Case 1: If $\bar{G} \cong C_m$ then $C_m = \langle \sigma \rangle$, where $\sigma(x) = \zeta x$, ζ is a primitive m^{th} root of unity. So $\sigma(z) = (\zeta x)^m = \zeta^m x^m = x^m = z$.

Case 2: If $\bar{G} \cong D_{2m}$ then $D_{2m} = \langle \sigma, t \rangle$, where $\sigma(x) = \xi x$, $t(x) = \frac{1}{x}$, ξ is primitive $(2m)^{th}$ root of unity. Hence, σ and t fix z.

Case 3: If $\bar{G} \cong A_4$ then $A_4 = \langle \sigma, \mu \rangle$, where $\sigma(x) = -x$, $\mu(x) = i\frac{x+1}{x-1}$, $i^2 = -1$. Therefore, $\sigma(z) = z$ and $\mu(z) = z$.

Case 4: If $\bar{G} \cong S_4$ then $S_4 = \langle \sigma, \mu \rangle$, where $\sigma(x) = ix$, $\mu(x) = i\frac{x+1}{x-1}$, $i^2 = -1$. Therefore, σ, μ fix z.

Case 5: If $\bar{G} \cong A_5$ then $A_5 = \langle \sigma, \rho \rangle$, where $\sigma(x) = \xi x$, $\rho(x) = -\frac{x+b}{bx-1}$, ξ is primitive fifth root of unity and $b = -i(\xi + \xi^4)$, $i^2 = -1$. One can check that σ, ρ fix z.

$Case$	$\bar{G}$	z	$Ramification$
1	C_m, $(m,p)=1$	x^m	(m,m)
2	D_{2m}, $(m,p)=1$	$x^m+\frac{1}{x^m}$	$(2,2,m)$
3	A_4, $p\neq 2,3$	$\frac{x^{12}-33x^8-33x^4+1}{x^2(x^4-1)^2}$	$(2,3,3)$
4	S_4, $p\neq 2,3$	$\frac{(x^8+14x^4+1)^3}{108(x(x^4-1))^4}$	$(2,3,4)$
5	A_5, $p\neq 2,3,5$	$\frac{(-x^{20}+228x^{15}-494x^{10}-228x^5-1)^3}{(x(x^{10}+11x^5-1))^5}$	$(2,3,5)$
	A_5, $p=3$	$\frac{(x^{10}-1)^6}{(x(x^{10}+2ix^5+1))^5}$	$(6,5)$
6	U	$\prod_{a\in H_t}(x+a)$	(p^t)
7	K_m	$(x\prod_{j=0}^{\frac{p^t-1}{m}-1}(x^m-b_j))^m$	(mp^t,m)
8	$PSL(2,q)$, $p\neq 2$	$\frac{((x^q-x)^{q-1}+1)^{\frac{q+1}{2}}}{(x^q-x)^{\frac{q(q-1)}{2}}}$	(α,β)
9	$PGL(2,q)$	$\frac{((x^q-x)^{q-1}+1)^{q+1}}{(x^q-x)^{q(q-1)}}$	$(2\alpha,2\beta)$

TABLE 1. Rational functions correspond to each $\bar{G}$

Case 6: If $\bar{G}\cong U$ then $U=\langle\{\sigma_a|a\in H_t\}\rangle$, where $\sigma_a(x)=x+a$ with $a\in H_t$. Therefore,

$$\sigma_a(z)=\prod_{a_1\in H_t}(x+a_1+a)=\prod_{a_2\in H_t}(x+a_2)=\prod_{a\in H_t}(x+a)=z.$$

and $a_2=a+a_1\in H_t$.

Case 7: If $\bar{G}\cong K_m$ then $K_m=\langle\{\sigma_a,t|a\in\mathcal{U}_m\}\rangle$, where $t(x)=\xi^2x$, $\sigma_a(x)=x+a$ for each $a\in\mathcal{U}_m:=\{a\in k|(a\prod_{j=0}^{\frac{p^t-1}{m}-1}(a^m-b_j))=0\}\leq H_t$, ξ is a primitive $2m$-th root of unity. So,

$$t(z)=((\xi^2x)\prod_{j=0}^{\frac{p^t-1}{m}-1}((\xi^2x)^m-b_j))^m=(x\prod_{j=0}^{\frac{p^t-1}{m}-1}(x^m-b_j))^m=z.$$

$$\sigma_a(z)=((x+a)\prod_{j=0}^{\frac{p^t-1}{m}-1}((x+a)^m-b_j))^m=(x\prod_{j=0}^{\frac{p^t-1}{m}-1}(x^m-b_j))^m=z.$$

Case 8: If $\bar{G} \cong PSL(2,q)$ then $PSL(2,q) = \langle \sigma, t, \phi \rangle$, where $\sigma(x) = \xi^2 x$, $t(x) = -\frac{1}{x}$, $\phi(x) = x+1$ and ξ is a primitive $(q-1)$-th root of unity. So,

$$\sigma(z) = \frac{(((\xi^2x)^q - (\xi^2x))^{q-1}+1)^{\frac{q+1}{2}}}{((\xi^2x)^q - (\xi^2x))^{\frac{q(q-1)}{2}}} = \frac{((x^q-x)^{q-1}+1)^{\frac{q+1}{2}}}{(x^q-x)^{\frac{q(q-1)}{2}}} = z.$$

$$t(z) = \frac{(((-\frac{1}{x})^q - (-\frac{1}{x}))^{q-1}+1)^{\frac{q+1}{2}}}{((-\frac{1}{x})^q - (-\frac{1}{x}))^{\frac{q(q-1)}{2}}} = \frac{((x^q-x)^{q-1}+1)^{\frac{q+1}{2}}}{(x^q-x)^{\frac{q(q-1)}{2}}} = z.$$

$$\phi(z) = \frac{(((x+1)^q - (x+1))^{q-1}+1)^{\frac{q+1}{2}}}{((x+1)^q - (x+1))^{\frac{q(q-1)}{2}}} = \frac{((x^q-x)^{q-1}+1)^{\frac{q+1}{2}}}{(x^q-x)^{\frac{q(q-1)}{2}}} = z.$$

Case 9: If $\bar{G} \cong PGL(2,q)$ then $PGL(2,q) = \langle \sigma, t, \phi \rangle$, where $\sigma(x) = \xi x$, $t(x) = \frac{1}{x}$, $\phi(x) = x+1$ and ξ is a primitive $(q-1)$-th root of unity. Hence,

$$\sigma(z) = \frac{(((\xi x)^q - (\xi x))^{q-1}+1)^{q+1}}{((\xi x)^q - (\xi x))^{q(q-1)}} = \frac{((x^q-x)^{q-1}+1)^{q+1}}{(x^q-x)^{q(q-1)}} = z.$$

$$t(z) = \frac{(((\frac{1}{x})^q - (\frac{1}{x}))^{q-1}+1)^{q+1}}{((\frac{1}{x})^q - (\frac{1}{x}))^{q(q-1)}} = \frac{((x^q-x)^{q-1}+1)^{q+1}}{(x^q-x)^{q(q-1)}} = z.$$

$$\phi(z) = \frac{(((x+1)^q - (x+1))^{q-1}+1)^{q+1}}{((x+1)^q - (x+1))^{q(q-1)}} = \frac{((x^q-x)^{q-1}+1)^{q+1}}{(x^q-x)^{q(q-1)}} = z$$

This completes the proof. □

3. Automorphism groups of a cyclic curves

In this section we determine groups which occur as automorphism group G of genus $g \geq 2$ cyclic curves, their signatures and the dimension of the locus $\mathcal{H}(G, \mathbf{C})$. We know that $\bar{G} := G/G_0$, where $G_0 := Gal(k(x,y)/k(x))$ and $\bar{G}$ is isomorphic to C_m, D_m, A_4, S_4, A_5, U, K_m, $PSL(2,q)$, $PGL(2,q)$. By considering the lifting of ramified points in each $\bar{G}$, we divide each $\bar{G}$ into sub cases. We determine signature of each sub case by looking the behavior of lifting and ramification of $\bar{G}$. Using that signature and Equation 2 we calculate δ for each case. We list all possible automorphism groups G as separate theorems for each $\bar{G}$.

3.1. The case 2g+1≥ p> 5.

Throughout this subsection we assume that $2g+1 \geq p > 5$.

Remark 1. *The case $p > 2g+1$ is same as char $= 0$; see [20]*

Theorem 3.1. *Let $g \geq 2$ be a fixed integer, $\mathcal{X}$ a genus g cyclic curve, $G = Aut(\mathcal{X})$ and $C_n \triangleleft G$ such that $g(\mathcal{X}^{C_n}) = 0$. The signature of cover $\Phi(x) : \mathcal{X} \to \mathcal{X}^G$ and dimension δ is given in Table 2. In Table 2, $m = |PSL_2(q)|$ for cases 38-41 and $m = |PGL_2(q)|$ for cases 42-45.*

#	$\bar{G}$	$\delta(G, \mathbf{C})$	$\mathbf{C} = (C_1, ..., C_r)$
1	$(p, m) = 1$	$\frac{2(g+n-1)}{m(n-1)} - 1$	$(m, m, n, ..., n)$

continued on the next page

#	$\bar{G}$	$\delta(G,\mathbf{C})$	$\mathbf{C}=(C_1,...,C_r)$
2	C_m	$\frac{2g+n-1}{m(n-1)}-1$	$(m,mn,n,...,n)$
3		$\frac{2g}{m(n-1)}-1$	$(mn,mn,n,...,n)$
4	$(p,m)=1$	$\frac{g+n-1}{m(n-1)}$	$(2,2,m,n,...,n)$
5		$\frac{2g+m+2n-nm-2}{2m(n-1)}$	$(2n,2,m,n,...,n)$
6	D_{2m}	$\frac{g}{m(n-1)}$	$(2,2,mn,n,...,n)$
7		$\frac{g+m+n-mn-1}{m(n-1)}$	$(2n,2n,m,n,...,n)$
8		$\frac{2g+m-mn}{2m(n-1)}$	$(2n,2,mn,n,...,n)$
9		$\frac{g+m-mn}{m(n-1)}$	$(2n,2n,mn,n,...,n)$
10		$\frac{n+g-1}{6(n-1)}$	$(2,3,3,n,...,n)$
11	A_4	$\frac{g-n+1}{6(n-1)}$	$(2,3n,3,n,...,n)$
12		$\frac{g-3n+3}{6(n-1)}$	$(2,3n,3n,n,...,n)$
13		$\frac{g-2n+2}{6(n-1)}$	$(2n,3,3,n,...,n)$
14		$\frac{g-4n+4}{6(n-1)}$	$(2n,3n,3,n,...,n)$
15		$\frac{g-6n+6}{6(n-1)}$	$(2n,3n,3n,n,...,n)$
16		$\frac{g+n-1}{12(n-1)}$	$(2,3,4,n,...,n)$
17		$\frac{g-3n+3}{12(n-1)}$	$(2,3n,4,n,...,n)$
18		$\frac{g-2n+2}{12(n-1)}$	$(2,3,4n,n,...,n)$
19		$\frac{g-6n+6}{12(n-1)}$	$(2,3n,4n,n,...,n)$
20	S_4	$\frac{g-5n+5}{12(n-1)}$	$(2n,3,4,n,...,n)$
21		$\frac{g-9n+9}{12(n-1)}$	$(2n,3n,4,n,...,n)$
22		$\frac{g-8n+8}{12(n-1)}$	$(2n,3,4n,n,...,n)$
23		$\frac{g-12n+12}{12(n-1)}$	$(2n,3n,4n,n,...,n)$

continued on the next page

#	$\bar{G}$	$\delta(G,\mathbf{C})$	$\mathbf{C}=(C_1,...,C_r)$
24		$\frac{g+n-1}{30(n-1)}$	$(2,3,5,n,...,n)$
25		$\frac{g-5n+5}{30(n-1)}$	$(2,3,5n,n,...,n)$
26		$\frac{g-15n+15}{30(n-1)}$	$(2,3n,5n,n,...,n)$
27		$\frac{g-9n+9}{30(n-1)}$	$(2,3n,5,n,...,n)$
28	A_5	$\frac{g-14n+14}{30(n-1)}$	$(2n,3,5,n,...,n)$
29		$\frac{g-20n+20}{30(n-1)}$	$(2n,3,5n,n,...,n)$
30		$\frac{g-24n+24}{30(n-1)}$	$(2n,3n,5,n,...,n)$
31		$\frac{g-30n+30}{30(n-1)}$	$(2n,3n,5n,n,...,n)$
32		$\frac{2g+2n-2}{p^t(n-1)}-2$	$(p^t,n,...,n)$
33	U	$\frac{2g+np^t-p^t}{p^t(n-1)}-2$	$(np^t,n,...,n)$
34		$\frac{2(g+n-1)}{mp^t(n-1)}-1$	$(mp^t,m,n,...,n)$
35		$\frac{2g+2n+p^t-np^t-2}{mp^t(n-1)}-1$	$(mp^t,nm,n,...,n)$
36	K_m	$\frac{2g+np^t-p^t}{mp^t(n-1)}-1$	$(nmp^t,m,n,...,n)$
37		$\frac{2g}{mp^t(n-1)}-1$	$(nmp^t,nm,n,...,n)$
38		$\frac{2(g+n-1)}{m(n-1)}-1$	$(\alpha,\beta,n,...,n)$
39	$PSL_2(q)$	$\frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)}-1$	$(\alpha,n\beta,n,...,n)$
40		$\frac{2g+nq(q-1)+q-q^2}{m(n-1)}-1$	$(n\alpha,\beta,n,...,n)$
41		$\frac{2g}{m(n-1)}-1$	$(n\alpha,n\beta,n,...,n)$
42		$\frac{2(g+n-1)}{m(n-1)}-1$	$(2\alpha,2\beta,n,...,n)$
43	$PGL_2(q)$	$\frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)}-1$	$(2\alpha,2n\beta,n,...,n)$
44		$\frac{2g+nq(q-1)+q-q^2}{m(n-1)}-1$	$(2n\alpha,2\beta,n,...,n)$

continued on the next page

#	$\bar{G}$	$\delta(G, \mathbf{C})$	$\mathbf{C} = (C_1, ..., C_r)$
45		$\frac{2g}{m(n-1)} - 1$	$(2n\alpha, 2n\beta, n, ..., n)$

Table 2: The signature $\mathbf{C}$ and dimension δ for char > 5

Proof. Let n be the number of branch points of Φ. Then $\delta = n - 3$; see [11]. We know that $\phi_0 : \mathcal{X}_g \to \mathbb{P}^1$ corresponds to degree n extension $K/k(x)$.

Case $\bar{G} \cong C_m$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is (m, m). i.e. $C_m = \langle \sigma, \tau | \sigma^m = \tau^m = \sigma\tau = 1 \rangle$. where $\tau = \sigma^{-1}$.

(1) If σ and τ both lift to elements of order m in G, then conjugacy classes $\mathbf{C} = (m, m, n, ..., n)$. By Riemann Hurwitz formula, we have

$$2(g-1) = 2(0-1)mn + mn\left(\left(\frac{m-1}{m}\right)\cdot 2 + \left(\frac{n-1}{n}\right)(\delta+1)\right)$$

Then $\delta = \frac{2(g+n-1)}{m(n-1)} - 1$.

(2) If either σ or τ lifts to an element of order mn in G, then ramification $\mathbf{C} = (mn, m, n, ..., n)$. By Riemann Hurwitz formula, we have

$$2(g-1) = 2(0-1)mn + mn\left(\left(\frac{m-1}{m}\right) + \left(\frac{nm-1}{nm}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right)$$

Then $\delta = \frac{2g+n-1}{m(n-1)} - 1$.

(3) If σ and τ both lift to elements of order mn in G, then ramification, $\mathbf{C} = (mn, mn, n, ..., n)$. By Riemann Hurwitz formula, we have

$$2(g-1) = 2(0-1)mn + mn\left(\left(\frac{mn-1}{mn}\right)\cdot 2 + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g)}{m(n-1)} - 1$.

Case $\bar{G} \cong D_{2m}$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is $(2, 2, m)$. i.e. $D_m = \langle \sigma, \tau, \mu | \sigma^2 = \tau^2 = \mu^m = 1 \rangle$, where $\mu = \sigma\tau$. Since the branching corresponding to first two ramification points is the same then there are basically six distinct sub cases which could arise.

(4) If σ, τ and μ lift in G to elements of orders $|\sigma|$, $|\tau|$ and $|\mu|$ respectively, then the ramification is $\mathbf{C} = (2, 2, m, n, ..., n)$. The dimension δ can be found using Riemann Hurwitz formula as follows.

$$2(g-1) = 2(0-1)2mn + 2mn\left(\left(\frac{2-1}{2}\right)\cdot 2 + \left(\frac{m-1}{m}\right) + \left(\frac{n-1}{n}\right)\delta\right).$$

Then, $\delta = \frac{g+n-1}{m(n-1)}$.

(5) If either τ or μ lifts in G to element of order $n|\tau|$ or $n|\mu|$ then ramification $\mathbf{C} = (2n, 2, m, n, ..., n)$. The dimension δ is as follows.

$$2(g-1) = 2(0-1)2mn+ \\ 2mn\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{2-1}{2}\right)+\left(\frac{m-1}{m}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{2g+m+2n-mn-2}{2m(n-1)}$.

(6) If μ lifts to an element of order $n|\mu|$ in G, then the ramification $\mathbf{C} = (2, 2, mn, n, ..., n)$. By Riemann Hurwitz formula, we have

$$2(g-1) = 2(0-1)2mn + 2mn\left(\left(\frac{2-1}{2}\right)\cdot 2+\left(\frac{mn-1}{mn}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g}{m(n-1)}$.

(7) If both σ and τ lift to elements of order $n|\sigma|$ and $n|\tau|$ in G, then ramification $\mathbf{C} = (2n, 2n, m, n, ..., n)$. By Riemann Hurwitz formula, we have

$$2(g-1) = 2(0-1)2mn + 2mn\left(\left(\frac{2n-1}{2n}\right)\cdot 2+\left(\frac{m-1}{m}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g+m+n-nm-1}{m(n-1)}$.

(8) If both σ and μ lift to elements of order $n|\sigma|$ and $n|\mu|$, then ramification $\mathbf{C} = (2n, 2, mn, n, ..., n)$. By Riemann Hurwitz formula, we have

$$2(g-1) = 2(0-1)2mn+ \\ 2mn\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{2-1}{2}\right)+\left(\frac{mn-1}{mn}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{2g+m-mn}{2m(n-1)}$.

(9) If σ, τ and μ lift to elements of orders $n|\sigma|$, $n|\tau|$ and $n|\mu|$ respectively in G, then the ramification $\mathbf{C} = (2n, 2n, mn, n, ..., n)$. Riemann Hurwitz formula gives us

$$2(g-1) = 2(0-1)2mn + 2mn\left(\left(\frac{2n-1}{2n}\right)\cdot 2+\left(\frac{mn-1}{mn}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g+m-mn}{m(n-1)}$.

Case $\bar{G} \cong A_4$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is $(2, 3, 3)$. i.e. $A_4 = \langle \sigma, \tau, \mu | \sigma^2 = \tau^3 = \mu^3 = 1 \rangle$, where $\mu = \sigma\tau$. Since the branching corresponding to last two ramification points is the same then there are basically six distinct sub cases which could arise.

(10) If σ, τ and μ lift in G to elements of orders $|\sigma|$, $|\tau|$ and $|\mu|$ respectively, then the ramification $\mathbf{C} = (2, 3, 3, n, ..., n)$. The dimension δ can be found using Riemann Hurwitz formula as follows.

$$2(g-1) = 2(0-1)12n + 12n\left(\left(\frac{2-1}{2}\right)+\left(\frac{3-1}{3}\right)\cdot 2+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g+n-1}{6(n-1)}$.

(11) If τ lifts in G to element of order $n|\tau|$ then ramification, $\mathbf{C} = (2, 3n, 3, n, ..., n)$. The dimension δ is as follows.

$$2(g-1) = 2(0-1)12n + 12n\left(\left(\frac{2n-1}{2n}\right) + \left(\frac{3-1}{3}\right)\cdot 2 + \left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-n+1}{6(n-1)}$.

(12) If τ and μ lift in G to element of order $n|\tau|$ and $n|\mu|$ then ramification $\mathbf{C} = (2, 3n, 3n, n, ..., n)$. The dimension δ is as follows.

$$2(g-1) = 2(0-1)12n + 12n\left(\left(\frac{2-1}{2}\right) + \left(\frac{3n-1}{3n}\right)\cdot 2 + \left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-3n+3}{6(n-1)}$.

(13) If σ lifts in G to element of order $n|\sigma|$ then ramification $\mathbf{C} = (2n, 3, 3, n, ..., n)$. The dimension δ can be found using Riemann-Hurwitz formula as follows.

$$2(g-1) = 2(0-1)12n + 12n\left(\left(\frac{2n-1}{2n}\right) + \left(\frac{3-1}{3}\right)\cdot 2 + \left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-2n+2}{6(n-1)}$.

(14) If σ and τ lift in G to element of order $n|\sigma|$ and $n|\tau|$ then ramification $\mathbf{C} = (2n, 3n, 3, n, ..., n)$. The dimension δ is as follows.

$$2(g-1) = 2(0-1)12n + 12n\left(\left(\frac{2n-1}{2n}\right) + \left(\frac{3n-1}{3n}\right) + \left(\frac{3-1}{3}\right) + \left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-4n+4}{6(n-1)}$.

(15) If σ, τ and μ lift to elements of orders $n|\sigma|$, $n|\tau|$ and $n|\mu$ respectively in G, then ramification $\mathbf{C} = (2n, 3n, 3n, n, ..., n)$. The dimension δ is as follows.

$$2(g-1) = 2(0-1)12n + 12n\left(\left(\frac{2n-1}{2n}\right) + \left(\frac{3n-1}{3n}\right)\cdot 2 + \left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-6n+6}{6(n-1)}$.

Case $\bar{G} \cong S_4$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is $(2, 3, 4)$. i.e. $S_4 = \langle \sigma, \tau, \mu | \sigma^2 = \tau^3 = \mu^4 = 1 \rangle$, where $\mu = \sigma\tau$. Let s and t be the lifting of σ and $\tau \in G$ respectively.

(16) If σ, τ and μ lift in G to elements of orders $|\sigma|$, $|\tau|$ and $|\mu|$ respectively, then ramification $\mathbf{C} = (2, 3, 4, n, ..., n)$. The dimension δ can find using Riemann Hurwitz formula as follows.

$$2(g-1) = 2(0-1)24n + 24n\left(\left(\frac{2-1}{2}\right) + \left(\frac{3-1}{3}\right) + \left(\frac{4-1}{4}\right) + \left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g+n-1}{12(n-1)}$.

(17) If τ lifts to an element of order $n|\tau|$ then ramification $(2, 3n, 4, n, .. ., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)24n+ \\ 24n\left(\left(\frac{2-1}{2}\right)+\left(\frac{3n-1}{3n}\right)+\left(\frac{4-1}{4}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-3n+3}{12(n-1)}$.

(18) If μ lifts to an element of order $n|\mu|$, then ramification $(2, 3, 4n, n, .. ., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)24n+ \\ 24n\left(\left(\frac{2-1}{2}\right)+\left(\frac{3-1}{3}\right)+\left(\frac{4n-1}{4n}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-2n+2}{12(n-1)}$.

(19) If τ and μ lift to elements of orders $n|\tau|$ and $n|\mu|$ respectively, then ramification $(2, 3n, 4n, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)24n+ \\ 24n\left(\left(\frac{2-1}{2}\right)+\left(\frac{3n-1}{3n}\right)+\left(\frac{4n-1}{4n}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-6n+6}{12(n-1)}$.

(20) If σ lifts to an element of order $n|\sigma|$, then ramification $(2n, 3, 4, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)24n+ \\ 24n\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{3-1}{3}\right)+\left(\frac{4-1}{4}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-5n+5}{12(n-1)}$.

(21) If σ and τ lift to elements of orders $n|\sigma|$ and $n|\tau|$ respectively, then ramification $(2n, 3n, 4, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)24n+ \\ 24n\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{3n-1}{3n}\right)+\left(\frac{4-1}{4}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-9n+9}{12(n-1)}$.

(22) If σ and μ lift to elements of orders $n|\sigma|$ and $n|\mu|$ respectively, then ramification $(2n, 3, 4n, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)24n+ \\ 24n\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{3-1}{3}\right)+\left(\frac{4n-1}{4n}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-8n+8}{12(n-1)}$.

(23) If σ, τ and μ lift to elements of orders $n|\sigma|$, $n|\tau|$ and $n|\mu|$ respectively, then ramification $(2n, 3n, 4n, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)24n+ \\ 24n\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{3n-1}{3n}\right)+\left(\frac{4n-1}{4n}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-12n+12}{12(n-1)}$.

Case $\bar{G} \cong A_5$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is $(2, 3, 5)$. i.e. $A_5 = \langle \sigma, \tau, \mu | \sigma^2 = \tau^3 = \mu^5 = 1 \rangle$, where $\mu = \sigma\tau$. Let s and t be the lifting of σ and $\tau \in G$ respectively.

(24) If σ, τ and μ lift to elements of orders $|\sigma|$, $|\tau|$ and $|\mu|$ respectively, then ramification $\mathbf{C} = (2, 3, 5, n, ..., n)$. The dimension δ can be found using Riemann Hurwitz formula as follows.

$$2(g-1) = 2(0-1)60n+ \\ 60n\left(\left(\frac{2-1}{2}\right)+\left(\frac{3-1}{3}\right)+\left(\frac{5-1}{5}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g+n-1}{30(n-1)}$.

(25) If μ lifts to an element of order $n|\mu|$, then ramification $(2, 3, 5n, n, .. ., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)60n+ \\ 60n\left(\left(\frac{2-1}{2}\right)+\left(\frac{3-1}{3}\right)+\left(\frac{5n-1}{5n}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-5n+5}{30(n-1)}$.

(26) If τ and μ lift to elements of orders $n|\tau|$ and $n|\mu|$ respectively, the ramification $(2, 3n, 5n, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)60n+ \\ 60n\left(\left(\frac{2-1}{2}\right)+\left(\frac{3n-1}{3n}\right)+\left(\frac{5n-1}{5n}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-15n+15}{30(n-1)}$.

(27) If τ lifts to an element of order $n|\tau|$, then ramification $(2, 3n, 5, n, .. ., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)60n+ \\ 60n\left(\left(\frac{2-1}{2}\right)+\left(\frac{3n-1}{3n}\right)+\left(\frac{5-1}{5}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-9n+9}{30(n-1)}$.

(28) If σ lifts to an element of order $n|\sigma|$, then ramification $(2n, 3, 5, n, .. ., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)60n+ \\ 60n\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{3-1}{3}\right)+\left(\frac{5-1}{5}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-14n+14}{30(n-1)}$.

(29) If σ and μ lift to elements of orders $n|\sigma|$ and $n|\mu|$ respectively, then ramification $(2n, 3, 5n, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)60n+ \\ 60n\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{3-1}{3}\right)+\left(\frac{5n-1}{5n}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-20n+20}{30(n-1)}$.

(30) If σ and τ lift to elements of orders $n|\sigma|$ and $n|\tau|$ respectively, then ramification $(2n, 3n, 5, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)60n+ \\ 60n\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{3n-1}{3n}\right)+\left(\frac{5-1}{5}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-24n+24}{30(n-1)}$.

(31) If σ, τ and μ lift to elements of orders $n|\sigma|$, $n|\tau|$ and $n|\mu|$ respectively, then ramification $(2n, 3n, 5n, n, ..., n)$. By Riemann Hurwitz formula

$$2(g-1) = 2(0-1)60n+ \\ 60n\left(\left(\frac{2n-1}{2n}\right)+\left(\frac{3n-1}{3n}\right)+\left(\frac{5n-1}{5n}\right)+\left(\frac{n-1}{n}\right)\delta\right).$$

Then $\delta = \frac{g-30n+30}{30(n-1)}$.

Case $\bar{G} \cong U$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is (p^t). We know that (p^t) is wildly ramified place; see[16],Theorem 1. Hence $\beta = e^*q + q - 2$ in equation 2. Also we know $q = p^t$; see [16],Theorem 1.

(32) If element of order p^t lifts to an element of order p^t, then ramification $\mathbf{C} = (p^t, n, ..., n)$. We know $e^* = 1$; see [16],Theorem 1. The dimension δ can be

found using Riemann Hurwitz formula as follows.

$$2(g-1) = 2(0-1)np^t + np^t\left(\left(\frac{p^t+p^t-2}{p^t}\right) + \left(\frac{n-1}{n}\right)(\delta+2)\right).$$

Then $\delta = \frac{2g+2n-2}{p^t(n-1)} - 2$.

(33) If element of order p^t lifts to an element of order np^t, then ramification $\mathbf{C} = (np^t, n, ..., n)$. In this case $e^* = n$. Also $(n,p) = 1$ and $n|p^t - 1$. The dimension δ can be found using Riemann Hurwitz formula as follows.

$$2(g-1) = 2(0-1)np^t + np^t\left(\left(\frac{np^t+p^t-2}{np^t}\right) + \left(\frac{n-1}{n}\right)(\delta+2)\right).$$

Then $\delta = \frac{2g+np^t-p^t}{p^t(n-1)} - 2$.

Case $\bar{G} \cong K_m$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is (mp^t, m). We know that the first place is wildly ramified; see [16],Theorem 1. Hence $\beta_1 = e_1^* q_1 + q_1 - 2$ in equation 2. We know $q_1 = p^t$; see [16],Theorem 1.

(34) If both elements of orders mp^t and m lift to elements of orders mp^t and m respectively, then ramification $\mathbf{C} = (mp^t, m, n, ..., n)$. We know $e_1^* = m$, $m|p^t - 1$ and $(m,p) = 1$; see [16],Theorem 1. Riemann Hurwitz formula gives us,

$$2(g-1) = 2(0-1)nmp^t + nmp^t\left(\left(\frac{mp^t+p^t-2}{mp^t}\right) + \left(\frac{m-1}{m}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+2n-2}{mp^t(n-1)} - 1$.

(35) If element of order m lifts to an element of order nm, then ramification $\mathbf{C} = (mp^t, nm, n, ..., n)$. As in previous case $e_1^* = m$, $m|p^t - 1$ and $(m,p) = 1$. The dimension δ can be found using Riemann Hurwitz formula as follows.

$$2(g-1) = 2(0-1)nmp^t + nmp^t\left(\left(\frac{mp^t+p^t-2}{mp^t}\right) + \left(\frac{nm-1}{nm}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+2n+p^t-np^t-2}{mp^t(n-1)} - 1$.

(36) If element of order mp^t lifts to an element of order nmp^t, then ramification $\mathbf{C} = (nmp^t, m, n, ..., n)$. In this case $e_1^* = nm$. Also $(nm,p) = 1$ and $nm|p^t - 1$. The dimension δ can be found using Riemann Hurwitz formula as follows.

$$2(g-1) = 2(0-1)nmp^t + nmp^t\left(\left(\frac{nmp^t+p^t-2}{nmp^t}\right) + \left(\frac{m-1}{m}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+np^t-p^t}{mp^t(n-1)} - 1$.

(37) If both elements of orders mp^t and m lift to elements of orders nmp^t and nm respectively, then ramification $\mathbf{C} = (nmp^t, nm, n, ..., n)$. As in previous case

$e_1^* = nm$, $(nm, p) = 1$ and $nm|p^t - 1$. Riemann Hurwitz formula gives us,

$$2(g-1) = 2(0-1)nmp^t + nmp^t\left(\left(\frac{nmp^t + p^t - 2}{nmp^t}\right) + \left(\frac{nm-1}{nm}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g}{mp^t(n-1)} - 1$.

Case $\bar{G} \cong PSL_2(q)$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is (α, β), where $\alpha = \frac{q(q-1)}{2}$ and $\beta = \frac{q+1}{2}$. We know that the first place is wildly ramified; see [16],Theorem 1. Hence $\beta_1 = e_1^* q_1 + q_1 - 2$ in equation 2. We know $q_1 = q$; see [16],Theorem 1. Let m be the size of $PSL_2(q)$. i.e. $m = \frac{q(q-1)(q+1)}{2}$.

(38) If both elements of orders α and β lift to elements of orders α and β respectively, then ramification $\mathbf{C} = (\alpha, \beta, n, ..., n)$. We know $e_1^* = \frac{q-1}{2}$ and $\left(\frac{q-1}{2}, p\right) = 1$; see [16],Theorem 1. Riemann Hurwitz formula gives us,

$$2(g-1) = 2(0-1)nm + nm\left(\left(\frac{\frac{q(q-1)}{2} + q - 2}{\frac{q(q-1)}{2}}\right) + \left(\frac{\frac{q+1}{2} - 1}{\frac{q+1}{2}}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+2n-2}{m(n-1)} - 1$.

(39) If an element of order β lifts to element of order $n\beta$, then ramification $\mathbf{C} = (\alpha, n\beta, n, ..., n)$. As in previous case $e_1^* = \frac{q-1}{2}$ and $\left(\frac{q-1}{2}, p\right) = 1$. By using Riemann Hurwitz formula we can find δ as follows.

$$2(g-1) = 2(0-1)nm + nm\left(\left(\frac{\frac{q(q-1)}{2} + q - 2}{\frac{q(q-1)}{2}}\right) + \left(\frac{\frac{n(q+1)}{2} - 1}{\frac{n(q+1)}{2}}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)} - 1$.

(40) If an element of order α lifts to element of order $n\alpha$, then ramification $\mathbf{C} = (n\alpha, \beta, n, ..., n)$. In this case $e_1^* = \frac{n(q-1)}{2}$, $\frac{n(q-1)}{2} | q-1$ and $\left(\frac{n(q-1)}{2}, p\right) = 1$. So only possible values for n are 1 and 2. By using Riemann Hurwitz formula we can find δ as follows.

$$2(g-1) = 2(0-1)nm + nm\left(\left(\frac{\frac{nq(q-1)}{2} + q - 2}{\frac{nq(q-1)}{2}}\right) + \left(\frac{\frac{q+1}{2} - 1}{\frac{q+1}{2}}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+nq(q-1)+q-q^2}{m(n-1)} - 1$.

(41) If both elements of orders α and β lift to elements of orders $n\alpha$ and $n\beta$ respectively, then ramification $\mathbf{C} = (n\alpha, n\beta, n, ..., n)$. As in previous case $e_1^* = \frac{n(q-1)}{2}$, $\left(\frac{n(q-1)}{2}, p\right) = 1$ and n can be either 1 or 2. Riemann Hurwitz formula gives

us,

$$2(g-1) = 2(0-1)nm+ \\ nm\left(\left(\frac{\frac{nq(q-1)}{2}+q-2}{\frac{nq(q-1)}{2}}\right)+\left(\frac{\frac{n(q+1)}{2}-1}{\frac{n(q+1)}{2}}\right)+\left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g}{m(n-1)} - 1$.

Case $\bar{G} \cong PGL_2(q)$ **:** The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is $(2\alpha, 2\beta)$, where α and β as in the case $PSL_2(q)$. We know that the first place is wildly ramified; see [16],Theorem 1. Hence $\beta_1 = e_1^* q_1 + q_1 - 2$ in equation 2. Also we know $q_1 = q$; see [16],Theorem 1. Let m be the size of $PGL_2(q)$. i.e. $m = q(q-1)(q+1)$.

(42) If both elements of orders 2α and 2β lift to elements of orders 2α and 2β respectively, then ramification $\mathbf{C} = (2\alpha, 2\beta, n, ..., n)$. We know $e_1^* = q-1$ and $(q-1, p) = 1$; see [16],Theorem 1. Riemann Hurwitz formula gives us,

$$2(g-1) = 2(0-1)nm+ \\ nm\left(\left(\frac{q(q-1)+q-2}{q(q-1)}\right)+\left(\frac{q+1-1}{q+1}\right)+\left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+2n-2}{m(n-1)} - 1$.

(43) If an element of order 2β lifts to element of order $2n\beta$, then ramification $\mathbf{C} = (2\alpha, 2n\beta, n, ..., n)$. As in previous case $e_1^* = q-1$ and $(q-1, p) = 1$. By using Riemann Hurwitz formula we can find δ as follows.

$$2(g-1) = 2(0-1)nm+ \\ nm\left(\left(\frac{q(q-1)+q-2}{q(q-1)}\right)+\left(\frac{n(q+1)-1}{n(q+1)}\right)+\left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)} - 1$.

(44) If an element of order 2α lifts to element of order $2n\alpha$, then ramification $\mathbf{C} = (2n\alpha, 2\beta, n, ..., n)$. In this case $e_1^* = n(q-1)$, $(n(q-1), p) = 1$ and $n(q-1)|q-1$. So only possible value for n is 1. By using Riemann Hurwitz formula we can find δ as follows.

$$2(g-1) = 2(0-1)nm+ \\ nm\left(\left(\frac{nq(q-1)+q-2}{nq(q-1)}\right)+\left(\frac{q+1-1}{q+1}\right)+\left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g+nq(q-1)+q-q^2}{m(n-1)} - 1$.

(45) If both elements of orders 2α and 2β lift to elements of orders $2n\alpha$ and $2n\beta$ respectively, then ramification $\mathbf{C} = (2n\alpha, 2n\beta, n, ..., n)$. As in previous case

$e_1^* = n(q-1)$, $(n(q-1), p) = 1$ and $n = 1$. Riemann Hurwitz formula gives us,

$$2(g-1) = 2(0-1)nm + nm\left(\left(\frac{nq(q-1)+q-2}{nq(q-1)}\right) + \left(\frac{n(q+1)-1}{n(q+1)}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{2g}{m(n-1)} - 1$.

This completes the proof. □

Now we determine the automorphism group G for each $\bar{G}$ as separate theorems. We know that each $\bar{G}$ has sub cases. So we list G for each sub cases under the appropriate theorem. In some cases we give a presentation for G.

Remark 2. *Let $\bar{G}$ be a group such that $s \in \bar{G}$ and $s^m = 1$. Let C_n be the cyclic group of order n and r be the generator of it. Let G be a extension of $\bar{G}$ by C_n such that $C_n \triangleleft G$. Then $srs^{-1} = r^l$, where $(l, n) = 1$ and $l^m \equiv 1$ (mod n).*

Proof. Since $C_n \triangleleft G$, $srs^{-1} = r^l$ for some $1 \leq l \leq n$. But $(srs^{-1})^n = 1$. Hence $(l, n) = 1$. Since $s^m r s^{-m} = r$ and $s^m r s^{-m} = r^{l^m}$, $l^m \equiv 1$ (mod n). □

3.1.1. $\bar{G} \cong C_m$.

Theorem 3.2. *The automorphism group G of a cyclic curve of genus $g \geq 2$ with $\bar{G} \cong C_m$ is as follows.*

(1) If G has ramification as in case 1, then there are two sub-cases. If $m = 1$ then $G \cong C_n$, otherwise G has a presentation:

$$\langle r, s \,|\, r^n = 1, s^m = 1, srs^{-1} = r^l \rangle$$

where (l,n)=1 and $l^m \equiv 1$ (mod n). But if $(m, n) = 1$, then $l = n - 1$.

(2) If G has ramification as in cases 2-3 in Table 2 then $G \cong C_{mn}$.

Proof. We know that the second cohomology group is as follows; see Table 1 in [15].

$$H^2(C_m, C_n) \cong C_{(n,m)}$$

(1) If $m = 1$, then G is a cyclic extension of C_n by C_1. C_n is the only one possible extension. Now we consider the sub case $m > 1$. Let $C_n = \langle r | r^n = 1 \rangle$ and let $C_m = \langle \sigma | \sigma^m = 1 \rangle$. Let s be the lifting σ in G. In the case 1, an element of order m lifts to an element of order m in G. Hence $s^m = 1$. Since $C_n \triangleleft G$, $srs^{-1} = r^l$ for some $l \in \{1, ..., n\}$. By Remark 2, $(l, n) = 1$ and $l^m \equiv 1$ (mod n). Hence G has a presentation:

$$\langle r, s \,|\, r^n = 1, s^m = 1, srs^{-1} = r^l \rangle$$

If $(m, n) = 1$, then $\left|H^2(C_m, C_n)\right| = 1$. Hence there is only one extension. If $l = 1$, $G \cong C_m \times C_n = C_{mn}$. Since this case G does not have an element of order mn, $l \neq 1$. So if $(m, n) = 1$ then $l = n - 1$.

(2) If G has ramification as in cases 2-3 in Table 2 then G has an element of order mn. Among the extensions C_m by C_n, C_{mn} is the only one extension for which has an element of order mn. Hence, for those cases $G \cong C_{mn}$. □

3.1.2. $\bar{G} \cong D_{2m}$.

Theorem 3.3. *Let $\bar{G} = G/C_n \cong D_{2m}$. The automorphism group G is as follows.*

(1) If n is odd then $G \cong D_{2m} \times C_n$.

(2) If n is even and m is odd then $G \cong D_{2m} \times C_n$ for the cases 4,6 and $G \cong G_9$ for the cases 7,9 in Table 2 respectively, where G_9 is as follows.

$$G_9 = \langle r, s, t |\, r^n = 1, s^2 = r, t^2 = r^{n-1}, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle$$

There are no possible group extensions for the cases 5 and 8 in Table 2.

(3) If n is even and m is even then $G \cong G_4, G_5, G_6, G_7, G_8, G_9$ for the cases 4-9 in Table 2 respectively, where $G_4 - G_9$ are as follows.

$$\begin{aligned}
G_4 =& D_{2m} \times C_n \\
G_5 =& \langle r, s, t |\, r^n = 1, s^2 = r, t^2 = 1, (st)^m = 1, srs^{-1} = r, trt^{-1} = r^{n-1} \rangle \\
G_6 =& D_{2mn} \\
G_7 =& \langle r, s, t |\, r^n = 1, s^2 = r, t^2 = r^{n-1}, (st)^m = 1, srs^{-1} = r, trt^{-1} = r \rangle \\
G_8 =& \langle r, s, t |\, r^n = 1, s^2 = r, t^2 = 1, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r^{n-1} \rangle \\
G_9 =& \langle r, s, t |\, r^n = 1, s^2 = r, t^2 = r^{n-1}, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle
\end{aligned}$$

Proof. We know that the second cohomology group is as follows; see Table 1 in [15].

$$H^2(D_{2m}, C_n) \cong \begin{cases} 1 & \text{if } (n,2) = 1 \\ C_2 & \text{if } (n,2) = 2 \text{ and } (m,2) = 1 \\ C_2 \times C_2 \times C_2 & \text{if } (n,2) = 2 \text{ and } (m,2) = 2 \end{cases}$$

(1) If n is odd then $\left|H^2(D_{2m}, C_n)\right| = 1$. Hence $G \cong D_{2m} \times C_n$.

(2) If n is even and m is odd then $|H^2(D_{2m}, C_n)| = 2$. So there are at most 2 extensions which could occur. For cases 4 and 6 $G \cong D_{2m} \times C_n$ because in those cases two elements of order 2 of G lift to elements of same order. In cases 7 and 9, two elements of order 2 left to elements of order $2n$. Let $C_n = \langle r | r^n = 1 \rangle$. The group D_{2m} has a presentation, $\langle \sigma, \tau, \mu | \sigma^2 = \tau^2 = \mu^m = 1 \rangle$, where $\mu = \sigma\tau$. Let s and t be the lifting of σ and τ in G respectively and we know that $C_n \triangleleft D_{2m}$. Hence $srs^{-1} = r^l$ and $trt^{-1} = r^k$. By Remark 2, $(l, n) = 1$, $l^2 \equiv 1 \pmod{n}$ and $(k, n) = 1$, $k^2 \equiv 1 \pmod{n}$. We choose $k = l = 1$. Since both σ and τ lift to elements of order $n|\sigma|$ and $n|\tau|$ in G, then we choose $s^2 = r$ and $t^2 = r^{n-1}$, because both r and r^{n-1} have order n in C_n. In case 9, μ lifts to element of order $n|\mu|$. Thus we choose $(st)^m = r^{\frac{n}{2}}$, because $r^{\frac{n}{2}}$ has order 2 in C_n. Hence $G \cong G_9$, where G_9 is as follows.

$$G_9 = \langle r, s, t |\, r^n = 1, s^2 = r, t^2 = r^{n-1}, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle$$

we know that the dimension δ is an integer. But δ's of cases 5 and 8 cannot be an integer when n is even and m is odd. So there are no possible automorphism groups for these cases.

(3) If n and m both even then $|H^2(D_{2m}, C_n)| = 6$. So there are at most 6 extensions which could occur. As in proof of part (2), $D_{2m} = \langle \sigma, \tau, \mu | \sigma^2 = \tau^2 = \mu^m = 1 \rangle$, where $\mu = \sigma\tau$, $C_n = \langle r | r^n = 1 \rangle$ and s and t be the lifting of σ and τ in G respectively. Also, $srs^{-1} = r^l$ and $trt^{-1} = r^k$. By Remark 2, $(l, n) = 1$, $l^2 \equiv 1 \pmod{n}$ and $(k, n) = 1$, $k^2 \equiv 1 \pmod{n}$. We choose $k = 1$.

In case 4, σ, τ and μ lift in G to elements of orders $|\sigma|$, $|\tau|$ and $|\mu|$ respectively. Hence $G \cong D_{2m} \times C_n$.

If τ lifts to element of order $n|\tau|$ like in case 5, then we choose s such that $s^2 = r$, because order of r is n in c_n. Since other two generators lift to elements of same orders that they had before, $t^2 = 1$ and $(st)^m = 1$. Further we choose $l = n - 1$. So G is isomorphic to G_5.

In case 6, μ lifts to an element of order $n|\mu|$ in G. Hence $G \cong D_{2mn}$.

In case 7, both σ and τ lift to elements of orders $n|\sigma|$ and $n|\tau|$ in G, then we choose $s^2 = r$ and $t^2 = r^{n-1}$, because both r and r^{n-1} have order n in C_n. Since other generator lifts to an element of same order that it has before, $(st)^m = 1$. Also we choose $l = 1$. So G is isomorphic to G_7.

If both σ and μ lift to elements of orders $n|\sigma|$ and $n|\mu|$ like in case 8, then we choose $s^2 = r$ and $(st)^m = r^{\frac{n}{2}}$. Since the order of τ is remaining the same, $t^2 = 1$. Further we choose $l = n - 1$. Hence $G \cong G_8$.

In case 9, σ, τ and μ lift to elements of orders $n|\sigma|$, $n|\tau|$ and $n|\mu|$ respectively, then we choose s and t such that $s^2 = r$, $t^2 = r^{n-1}$ and $(st)^m = r^{\frac{n}{2}}$. Also we choose $l = 1$. Hence $G \cong G_9$.

□

3.1.3. $\bar{G} \cong A_4$.

Lemma 2. *Let G be a group extension of A_4 by C_n and let $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$. If $3 \nmid (p_i - 1)$ for all $1 \leq i \leq r$, then G is a central extension.*

Proof. Let's consider the conjugation action of A_4 on C_n and the homomorphism $\gamma : A_4 \longrightarrow Aut(C_n)$. Then $im(\gamma) \in 1, C_3, A_4$. If $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ and $3 \nmid (p_i - 1)$ for all $1 \leq i \leq r$, then $3 \nmid |Aut(C_n)|$. So $3 \nmid |im(\gamma)|$. i.e. $|im(\gamma)|$=1. Hence G is central extension of A_4 by C_n. □

Theorem 3.4. *Let $\mathcal{X}_g$ be a genus $g \geq 2$ cyclic curve with $\bar{G} \cong A_4$. Then $G := Aut(\mathcal{X}_g)$ as follows.*

(1) If n is odd and not a multiple of 3 then $G \cong A_4 \times C_n$.

(2) If n is odd and a multiple of 3 then $G \cong G'_{10}, G'_{12}, G'_{13}, G'_{15}$ for the cases 10,12,13,15 in Table 2 respectively, where $G'_{10}, G'_{12}, G'_{13}, G'_{15}$ are as follows.

$$G'_{10} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = 1, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^l \rangle$$
$$G'_{12} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = r^{\frac{n}{3}}, (st)^3 = r^{\frac{n}{3}}, srs^{-1} = r, trt^{-1} = r^l \rangle$$
$$G'_{13} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{3}}, t^3 = 1, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^l \rangle$$
$$G'_{15} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{3}}, t^3 = r^{\frac{n}{3}}, (st)^3 = r^{\frac{n}{3}}, srs^{-1} = r, trt^{-1} = r^l \rangle$$

where $(l, n) = 1$ and $l^3 \equiv 1$ (mod n). Furthermore $G'_{10} \cong G'_{13}$, $G'_{12} \cong G'_{15}$ and there are no possible group extensions for the cases 11, 14 in Table 2.

(3) If n is even, not a multiple of 3, then if n satisfies the condition in Lemma 2 then $G \cong A_4 \times C_n$ when G has ramification as in cases 10 and G has ramification as in cases 11-15 in Table 2 then G has a presentation:

$$\langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^3 = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle$$

If n does not satisfy the condition in Lemma 2, then $G \cong G_{10}, G_{11}, G_{12}, G_{13}, G_{14}, G_{15}$ for the cases 10-15 in Table 2 respectively, where $G_{10} - G_{15}$ are as in (4).

(4) If n is even and multiple of 3 then $G \cong G_{10}, G_{11}, G_{12}, G_{13}, G_{14}, G_{15}$ for the cases 10-15 in Table 2 respectively, where $G_{10} - G_{15}$ are as follows.

$$G_{10} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = 1, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^k \rangle$$
$$G_{11} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = r^{\frac{n}{2}}, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^k \rangle$$
$$G_{12} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = r^{\frac{n}{2}}, (st)^3 = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r^k \rangle$$
$$G_{13} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = 1, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^k \rangle$$
$$G_{14} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^k \rangle$$
$$G_{15} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^3 = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r^k \rangle$$

where $(k, n) = 1$ and $k^3 \equiv 1$ (mod n). Furthermore $G_{10} \cong G_{11} \cong G_{12}$ and $G_{13} \cong G_{14} \cong G_{15}$.

Proof. We know that the second cohomology group is as follows; see Table 1 in [15].

$$H^2(A_4, C_n) \cong C_{(n,2)} \times C_{(n,3)}$$

(1) If n is not a multiple of 3 then $H^2(A_4, C_n) = C_{(n,2)} \times C_1$. If we consider the case that n is odd under the condition n is not a multiple of 3, then $\left|H^2(A_4, C_n)\right| = 1$. Hence $G \cong A_4 \times C_n$.

(2) If n is odd and a multiple of 3 then $\left|H^2(A_4, C_n)\right| = 3$. So there are at most 3 extensions which could occur. Let $C_n = \langle r | r^n = 1 \rangle$. The group A_4 has a presentation, $\langle \sigma, \tau, \mu | \sigma^2 = \tau^3 = \mu^3 = 1 \rangle$, where $\mu = \sigma\tau$. Let s and t be the lifting of σ and τ in G respectively and we know that $C_n \triangleleft A_4$. Hence $srs^{-1} = r^k$ and $trt^{-1} = r^l$. We choose $k = 1$. By Remark 2, $(l, n) = 1$ and $l^3 \equiv 1$ (mod n).

The case 10 in Table 2 is lifting of σ, τ and μ to elements of orders $|\sigma|$, $|\tau|$ and $|\mu|$ respectively, then $s^2 = 1$, $t^3 = 1$ and $(st)^3 = 1$. Hence G has a presentation as in G'_{10}.

If τ and μ lift to elements of orders $n|\tau|$ and $n|\mu|$ respectively, then we choose s and t such that $t^3 = r^{\frac{n}{2}}$ and $(st)^3 = r^{\frac{n}{2}}$. In case 12, we have such a situation. Since the order of σ is remaining the same, $s^2 = 1$. So G has presentation as in G'_{12}.

In case 13, σ lifts to an element of order $n|\sigma|$, then we choose s such that $s^2 = r^{\frac{n}{2}}$. Since the orders of τ and μ are remaining the same, $t^3 = 1$ and $(st)^3 = 1$. So $G \cong G'_{13}$.

In case 15, σ, τ and μ lift to elements of orders $n|\sigma|$, $n|\tau|$ and $n|\mu|$ respectively, then we choose s and t such that $s^2 = r^{\frac{n}{2}}$, $t^3 = r^{\frac{n}{2}}$ and $(st)^3 = r^{\frac{n}{2}}$. Hence $G \cong G'_{15}$.

(3) If n is even and not a multiple of 3 then $\left|H^2(A_4, C_n)\right| = 2$. By Lemma 2, if $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ and $3 \nmid (p_i - 1)$ for all $1 \leq i \leq r$ then G is a central extension. Hence there are two extensions. So $G \cong A_4 \times C_n$ for the cases 10 in Table 2, because $A_4 \times C_n$ does not have element of order $2n$. By using GAP algebra package we found out that $G := \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^3 = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle$ for the cases 11-15 in table 2. If n does not satisfy the condition in Lemma 2 then G isomorphic to $G_{10} - G_{15}$ in (4) and proof is exactly similar to proof in (4).

(4) If n is even then $\left|H^2(A_4, C_n)\right| = 2$ or 6. So there are at most 6 extensions which could occur. Let $C_n = \langle r | r^n = 1 \rangle$. As proof of part (2), A_4 has a presentation, $\langle \sigma, \tau, \mu | \sigma^2 = \tau^3 = \mu^3 = 1 \rangle$, where $\mu = \sigma\tau$. Let s and t be the lifting of σ and τ in G respectively and we know that $C_n \triangleleft A_4$. Hence $srs^{-1} = r^l$ and $trt^{-1} = r^k$. We choose $l = 1$. By Remark 2, $(k, n) = 1$ and $k^3 \equiv 1$ (mod n).

The case 10 in Table 2 is lifting of σ, τ and μ to elements of orders $|\sigma|$, $|\tau|$ and $|\mu|$ respectively, then $s^2 = 1$, $t^3 = 1$ and $(st)^3 = 1$. Hence G has a presentation as in G_{10}.

In case 11, τ lifts to an element of order $n|\tau|$, we choose t such that $t^3 = r^{\frac{n}{2}}$. Since the orders of σ and μ are remaining the same, $s^2 = 1$ and $(st)^3 = 1$. Hence $G \cong G_{11}$.

If τ and μ lift to elements of orders $n|\tau|$ and $n|\mu|$ respectively, then we choose s and t such that $t^3 = r^{\frac{n}{2}}$ and $(st)^3 = r^{\frac{n}{2}}$. In case 12, we have such a situation. Since the order of σ is remaining the same, $s^2 = 1$. So G has presentation as in G_{12}.

In case 13, σ lifts to an element of order $n|\sigma|$, then we choose s such that $s^2 = r^{\frac{n}{2}}$. Since the orders of τ and μ are remaining the same, $t^3 = 1$ and $(st)^3 = 1$. So $G \cong G_{13}$.

If σ and τ lift to elements of orders $n|\sigma|$ and $n|\tau|$ respectively like in case 14, then we choose s and t such that $s^2 = r^{\frac{n}{2}}$ and $t^3 = r^{\frac{n}{2}}$. Since the order of μ does not change $(st)^3 = 1$. Hence $G \cong G_{14}$.

In case 15, σ, τ and μ lift to elements of orders $n|\sigma|$, $n|\tau|$ and $n|\mu|$ respectively, then we choose s and t such that $s^2 = r^{\frac{n}{2}}$, $t^3 = r^{\frac{n}{2}}$ and $(st)^3 = r^{\frac{n}{2}}$. Hence $G \cong G_{15}$. □

3.1.4. $\bar{G} \cong S_4$.

Theorem 3.5. *The full automorphism groups for the cases 16-23 in Table 2 as follows.*

(1) If n is odd then $G \cong S_4 \times C_n$.

(2) If n is even then $G \cong G_{16}, G_{17}, G_{18}, G_{19}, G_{20}, G_{21}, G_{22}, G_{23}$ for the cases 16-23 in Table 2 respectively, where $G_{16} - G_{23}$ are as follows.

$$G_{16} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = 1, (st)^4 = 1, srs^{-1} = r^l, trt^{-1} = r \rangle$$
$$G_{17} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = r^{\frac{n}{2}}, (st)^4 = 1, srs^{-1} = r^l, trt^{-1} = r \rangle$$
$$G_{18} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = 1, (st)^4 = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r \rangle$$
$$G_{19} = \langle r, s, t \,|\, r^n = 1, s^2 = 1, t^3 = r^{\frac{n}{2}}, (st)^4 = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r \rangle$$
$$G_{20} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = 1, (st)^4 = 1, srs^{-1} = r^l, trt^{-1} = r \rangle$$
$$G_{21} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^4 = 1, srs^{-1} = r^l, trt^{-1} = r \rangle$$

$$G_{22} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = 1, (st)^4 = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r \rangle$$
$$G_{23} = \langle r, s, t \,|\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^4 = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r \rangle$$

where $(l, n) = 1$ and $l^2 \equiv 1$ (mod n). Furthermore $G_{16} \cong G_{17}$, $G_{18} \cong G_{19}$, $G_{20} \cong G_{21}$ and $G_{22} \cong G_{23}$.

Proof. We know that the second cohomology group is as follows; see Table 1 in [15].

$$H^2(S_4, C_n) \cong C_{(n,2)} \times C_{(n,2)}$$

(1) If n is odd then $\left|H^2(S_4, C_n)\right| = 1$. So $G \cong S_4 \times C_n$.

(2) If n is even then $\left|H^2(S_4, C_n)\right| = 4$. So there are at most 4 extensions which could occur. Let $C_n = \langle r | r^n = 1 \rangle$. The group S_4 has a presentation: $\langle \sigma, \tau, \mu | \sigma^2 = \tau^3 = \mu^4 = 1 \rangle$, where $\mu = \sigma\tau$. Let s and t be the lifting of σ and

τ in G respectively and we know that $C_n \triangleleft S_4$. Hence $srs^{-1} = r^l$ and $trt^{-1} = r^k$. We choose $k = 1$. By Remark 2, $(l, n) = 1$ and $l^2 \equiv 1 \pmod{n}$.

The case 16 in Table 2 is lifting of σ, τ and μ to elements of orders $|\sigma|$, $|\tau|$ and $|\mu|$ respectively, then $s^2 = 1$, $t^3 = 1$ and $(st)^4 = 1$. Hence G has a presentation as in G_{16}.

In case 17, τ lifts to an element of order $n|\tau|$, we choose t such that $t^3 = r^{\frac{n}{2}}$. Since the orders of σ and μ are remaining the same, $s^2 = 1$ and $(st)^4 = 1$. Hence $G \cong G_{17}$.

If μ lifts to an element of order $n|\mu|$ like in case 18, then we choose s and t such that $(st)^4 = r^{\frac{n}{2}}$. Since the orders of σ and τ don't change, $s^2 = 1$ and $st^3 = 1$. Hence $G \cong G_{18}$.

If τ and μ lift to elements of orders $n|\tau|$ and $n|\mu|$ respectively, then we choose s and t such that $t^3 = r^{\frac{n}{2}}$ and $(st)^4 = r^{\frac{n}{2}}$. In case 19, we have such a situation. Since the order of σ is remaining the same, $s^2 = 1$. So G has presentation as in G_{19}.

In case 20, σ lifts to an element of order $n|\sigma|$, then we choose s such that $s^2 = r^{\frac{n}{2}}$. Since the orders of τ and μ are remaining the same, $t^3 = 1$ and $(st)^4 = 1$. So $G \cong G_{20}$.

If σ and τ lift to elements of orders $n|\sigma|$ and $n|\tau|$ respectively like in case 21, then we choose s and t such that $s^2 = r^{\frac{n}{2}}$ and $t^3 = r^{\frac{n}{2}}$. Since the order of μ does not change $(st)^4 = 1$. Hence $G \cong G_{21}$.

In case 22, σ and μ lift to elements of orders $n|\sigma|$ and $n|\mu|$ respectively, then we choose s and t such that $s^2 = r^{\frac{n}{2}}$ and $(st)^4 = r^{\frac{n}{2}}$. Since the order of μ does not change $(st)^4 = 1$. Hence G has a presentation as in G_{22}.

In case 23, σ, τ and μ lift to elements of orders $n|\sigma|$, $n|\tau|$ and $n|\mu|$ respectively, then we choose s and t such that $s^2 = r^{\frac{n}{2}}$, $t^3 = r^{\frac{n}{2}}$ and $(st)^4 = r^{\frac{n}{2}}$. Hence $G \cong G_{23}$. □

3.1.5. $\bar{G} \cong A_5$.

Lemma 3. *Let $\bar{G}$ be either A_5 or $PSL_2(q)$. Then an extension of $\bar{G}$ by C_n is central.*

Proof. Let us consider the conjugation action of A_5 on C_n. The image of the induce homomorphism $\pi : A_5 \longrightarrow Aut(C_n)$ is a quotient of A_5. Since $Aut(C_n)$ is abelian group, $im(\pi)$ is abelian group. $\bar{G}$ is non abelian simple group. Hence $\bar{G}$ is perfect group and $\frac{\bar{G}}{[\bar{G},\bar{G}]} = 1$. So $\bar{G}$ has only trivial abelian quotient. Therefore $im(\pi)$=1. Hence the action of A_5 on C_n is trivial. Therefore extension of A_5 by C_n is central. □

Theorem 3.6. *The automorphism groups for the cases 24-31 in Table 2 are as follows. If n is odd or G has a ramification as in cases 24-27 in Table 2 then $G \cong A_5 \times C_n$. Otherwise G admits group has presentation as:*

$$\langle r, s, t |\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^5 = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle$$

Proof. By Lemma 3, we know that extension is central and We know that the second cohomology group is as follows; see Table 1 in [15].

$$H^2(A_5, C_n) \cong \begin{cases} 1 & \text{if } n \text{ is odd} \\ C_2 & \text{if } n \text{ is even} \end{cases}$$

Hence if n is odd there is only one central extension. Since C_n is abelian $G \cong A_5 \times C_n$. If n is even there are two central extensions. The one possibility is $A_5 \times C_n$.

According to the ramification of the cases 28-31 in Table 2, G has element of order $2n$. But $A_5 \times C_n$ does not have element of order $2n$. Hence if G has a ramification of the cases 24-27 in Table 2 then $G \cong A_5 \times C_n$. Since $A_5 = \langle s,t|\, s^2 = t^3 = (st)^5 = 1\rangle$, all possible central extensions are of the form $\langle r,s,t|\, r^n = 1, s^2 = r^a, t^3 = r^b, (st)^5 = r^c, srs^{-1} = r, trt^{-1} = r\rangle$ where $a,b,c \in \{1,...,n\}$. If $a = b = c = 1$ then the above presentation gives $A_5 \times C_n$. We use GAP algebra package to calculate suitable a, b and c for the cases 24-27 in Table 2 and we found out that $a = b = c = \frac{n}{2}$. □

3.1.6. $\bar{G} \cong U$. We defined $U = C_P^t$.

Theorem 3.7. *Let $\mathcal{X}_g$ be a genus $g \geq 2$ cyclic curve with $\bar{G} \cong U$. Then $G := Aut(\mathcal{X}_g)$ as follows.*

(1) If G has ramification as in case 32 in Table 2 then G has presentation:

$$< r, s_1, s_2, ..., s_t | r^n = s_1^p = s_2^p = ... = s_t^p = 1, \quad s_i s_j = s_j s_i, s_i r s_i^{-1} = r^l, 1 \leq i,j \leq t >$$

where $(l,n) = 1$ and $l^p \equiv 1$ (mod n).

(2) If G has ramification as in case 33 in Table 2 then $G \cong U \times C_n$.

Proof. (1) Let $U =< \sigma_1, \sigma_2, ..., \sigma_t | \sigma_1^p = \sigma_2^p = ... = \sigma_t^p = 1, \sigma_i\sigma_j = \sigma_j\sigma_i, 1 \leq i,j \leq t >$. Let $C_n = \langle r|r^n = 1\rangle$. Let $s_1, s_2, ..., s_t$ be the lifting of $\sigma_1, \sigma_2, ..., \sigma_t$ in G respectively. In case 32, $\sigma_1...\sigma_t$ lifts to an element of order $|\sigma_1...\sigma_t|$, then $s_1^p = s_2^p = ... = s_t^p = 1, s_i s_j = s_j s_i, 1 \leq i,j \leq t$. Since $C_n \triangleleft U$, $s_i r s_i^{-1} = r^{l_i}, 1 \leq i \leq t$. By Remark 2, $(l_i, n) = 1$ and $l_i^p \equiv 1$ (mod n), for $1 \leq i \leq t$. We choose $l = l_i$ for $1 \leq i \leq t$. Hence G has presentation,

$$< r, s_1, s_2, ..., s_t | r^n = s_1^p = s_2^p = ... = s_t^p = 1, s_i s_j = s_j s_i, s_i r s_i^{-1} = r^l, 1 \leq i,j \leq t > .$$

(2) In case 33, G has an element of order np^t. We know that $(n,p) = 1$ and $n|p^t - 1$. Hence $(n,p^t) = 1$. So among the extensions of U by C_n, $U \times C_n$ is the only one extension for which has an element of order np^t. So in this case $G \cong U \times C_n$. □

3.1.7. $\bar{G} \cong K_m$. We know that $K_m = C_p^t \rtimes C_m$ and $m|p^t - 1$.

Theorem 3.8. *Let $\mathcal{X}_g$ be a genus $g \geq 2$ cyclic curve with $\bar{G} \cong K_m$. Then $G := Aut(\mathcal{X}_g)$ as follows.*

(1) If G has ramification as in case 34 in Table 2 then G has presentation:

$$< r, s_1, ..., s_t, v | r^n = s_1^p = ... = s_t^p = v^m = 1, s_i s_j = s_j s_i, \quad v r v^{-1} = r, s_i r s_i^{-1} = r^l, s_i v s_i^{-1} = v^k, 1 \leq i,j \leq t >$$

where $(l,n) = 1$ and $l^p \equiv 1$ (mod n), $(k,m) = 1$ and $k^p \equiv 1$ (mod m).

(2) If G has ramification as in case 35,36 and 37 in Table 2 then G has presentation:

$$G_{35} = \langle r, s_1, ..., s_t | r^{nm} = s_1^p = ... = s_t^p = 1, s_i s_j = s_j s_i, s_i r s_i^{-1} = r^l, 1 \leq i,j \leq t\rangle$$

where $(l, nm) = 1$ and $l^p \equiv 1$ (mod nm).

Proof. (1) Let $K =< \sigma_1, \sigma_2, ..., \sigma_t, u | \sigma_1^p = \sigma_2^p = ... = \sigma_t^p = u^m = 1, \sigma_i\sigma_j = \sigma_j\sigma_i, \sigma_i u \sigma_i^{-1} = u^{k_i}, 1 \leq i,j \leq t >$, $(k_i, m) = 1$ and $k_i^p \equiv 1$ (mod m). Let $C_n = \langle r|r^n = 1\rangle$. Let $s_1, s_2, ..., s_t, v$ be the lifting of $\sigma_1, \sigma_2, ..., \sigma_t, u$ in G respectively. In case 34, $u\sigma_1...\sigma_t$ lifts to an element of order $|u\sigma_1...\sigma_t|$, then $s_1^p = s_2^p =$

$... = s_t^p = v^m = 1, s_i s_j = s_j s_i, svs^{-1} = v^{k_i}, 1 \leq i, j \leq t$. We choose $k = k_i$ for $1 \leq i \leq t$. Since $C_n \triangleleft U$, $s_i r s_i^{-1} = r^{l_i}, 1 \leq i \leq t$. By Remark 2, $(l_i, n) = 1$ and $l_i^p \equiv 1 \pmod{n}$, for $1 \leq i \leq t$. We choose $l = l_i$ for $1 \leq i \leq t$. Also $vrv^{-1} = r^a$. By Remark 2, $(a, n) = 1$ and $a^m \equiv 1 \pmod{n}$. we choose $a = 1$. Hence G has presentation,

$$< r, s_1, ..., s_t, v | r^n = s_1^p = ... = s_t^p = v^m = 1, s_i s_j = s_j s_i, \\ vrv^{-1} = r, s_i r s_i^{-1} = r^l, s_i v s_i^{-1} = v^k, 1 \leq i, j \leq t >$$

(2) In case 35, 36 and 37, G has elements of orders nmp^t and nm. Among the extension of K_m by C_n, G_{35} is the only one extension so that it has elements of orders nmp^t and nm. Non of other extensions have either elements of orders nm or nmp^t. Note that if $(n, m) = 1$, then G_{35} is isomorphic to the group G of case 34. □

3.1.8. $\bar{G} \cong PSL_2(q)$. We know that $q = p^f$ where p is the characteristic of field k.

Theorem 3.9. *Let G be a Aut($\mathcal{X}_g$) where $\mathcal{X}_g$ is a cyclic curve of genus $g \geq 2$ with $\bar{G} \cong PSL_2(q)$, $q \neq 9$ then G is as follows.*

(1) If G has ramification as in cases 38 and 39 then $G \cong PSL_2(q) \times C_n$.

(2) If G has ramification as in cases 40 and 41 and $q = 3$ then $G \cong SL_2(3)$. There are no possible groups for $q \neq 3$.

Proof. By Lemma 3, we know that extension is central and the second cohomology group is as follows; see Table 1 in [15].

$$H^2(PSL_2(q), C_n) \cong \begin{cases} 1 & \text{if } p = 2,\ p^f \neq 4 \\ C_{(2,n)} & \text{if } p > 2,\ p^f \neq 9 \text{ or } p^f = 4 \\ C_{(6,n)} & \text{if } p^f = 9 \end{cases}$$

(1) If n is odd then there is only one extension. Since C_n is abelian $G \cong PSL_2(q) \times C_n$. If n is even, there are two extensions. According to ramification structure of cases 38 and 39 $G \cong PSL_2(q) \times C_n$. So for any n $G \cong PSL_2(q) \times C_n$ for cases 38 and 39.

(2) By cases 40 and 41 of Theorem 3.1, $n = 2$. We know that $SL_2(q)$ is the only degree two central extension of $PSL_2(q)$; see [8]. If $q \neq 3$ then $SL_2(q)$ does not have elements of $n\alpha$ or $n\beta$. Therefore there are no possible groups for $q \neq 3$. But if $q = 3$, $G \cong SL_2(3)$.

□

3.1.9. $\bar{G} \cong PGL_2(q)$. As previous subsection we know that $q = p^f$.

Theorem 3.10. *The automorphism group G such that $\bar{G} = G/C_n \cong PGL(2, q)$ is as follows. If G has ramification as in cases 42 and 43 in Table 2 then $G \cong PGL(2, q) \times C_n$. There are no possible group extensions for the cases 44 and 45 in same table.*

Proof. We know that the second cohomology group is as follows; see Table 1 in [15].

$$H^2(PGL(2, q), C_n) \cong C_{(n,2)} \times C_{(n,2)}$$

According to the ramifications structure of the cases 42 and 43 and the second homology group, for any n, $G \cong PGL(2, q) \times C_n$. By Theorem 3.1, only possible

value for n is one for the cases 44 and 45. Hence there are no possible groups for those cases.

□

3.2. **The case p=5.** In this case $\bar{G}$ is isomorphic to one of the C_m, D_m, A_4, S_4, U, K_m, $PSL(2,q)$ or $PGL(2,q)$. Since the ramifications of covers $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ are similar to the ramifications in Theorem 3.1, then signatures of covers $\Phi : \mathcal{X} \to \mathcal{X}^G$ and dimensions are same as corresponding cases in Table 2.

Theorem 3.11. *Let $g \geq 2$ be a fixed integer. Then the automorphism group G of a cyclic curve of genus g defined over a algebraically closed field k such that char(k)=5 is one of the group in the Theorem 3.2, 3.3, 3.4, 3.5, 3.7, 3.8, 3.9, 3.10. Furthermore, signatures of covers $\Phi : \mathcal{X} \to \mathcal{X}^G$ and dimensions are same as corresponding cases in the Table 2.*

Proof. Since the ramification of the cases under $\bar{G} \cong C_m, D_m, A_4, S_4, U, K_m, PSL(2,q)$ and $PGL(2,q)$ are same as in Theorem 3.1, the proofs of those cases are the same as proof of Theorem 3.1. But the case $G \cong A_5$ does not appear when $p = 5$. □

3.3. **The case p=3.** In this case $\bar{G} \cong C_m$, D_m, A_5, U, K_m, $PSL(2,q)$ or $PGL(2,q)$. The cases $\bar{G} \cong C_m$, D_m, U, K_m, $PSL(2,q)$ and $PGL(2,q)$ have the same ramifications as in Theorem 3.1. Hence those cases have signatures as in Table 2. However the case $\bar{G} \cong A_5$ has different ramification.

Theorem 3.12. *Let $g \geq 2$ be a fixed integer. Then the automorphism group G of a cyclic curve of genus g defined over a algebraically closed field k such that char(k)=3 is one of the group in the Theorems 3.2, 3.3, 3.7, 3.8, 3.9, 3.10 or if G has ramification as in cases a, b in Table 3 then $G \cong A_5 \times C_n$. There are no possible group for cases c, d in Table 3. Furthermore, signatures of covers $\Phi : \mathcal{X} \to \mathcal{X}^G$ and dimensions are same as corresponding cases in the Table 2 or Table 3.*

#	$\bar{G}$	$\delta(G, \mathbf{C})$	$\mathbf{C} = (C_1, ..., C_r)$
a		$\frac{g+n-1}{30(n-1)} - 1$	$(6, 5, n, ..., n)$
b		$\frac{g+5n-5}{30(n-1)} - 1$	$(6, 5n, n, ..., n)$
c	A_5	$\frac{g+6n-6}{30(n-1)} - 1$	$(6n, 5, n, ..., n)$
d		$\frac{g}{30(n-1)} - 1$	$(6n, 5n, n, ..., n)$

Table 3: The signature $\mathbf{C}$ and dimension δ for $\bar{G} \cong A_5$ and $p = 3$

Proof. The proof of the cases under $\bar{G} \cong C_m, D_m, A_4, S_4, U, K_m, PSL(2,q)$ and $PGL(2,q)$ are the same as in proof in Theorem 3.1.

Case $\bar{G} \cong A_5$: The ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is $(6, 5)$. By Theorem 1 in [16], the first point is wildly ramified and second one is tamely ramified. Hence in equation 2, $\beta_1 = e_1^* q_1 + q_1 - 2$ for the first ramified place. By Theorem 1 in [16], $q_1 = 3$.

(a) If both elements of orders 6 and 5 lift to elements of orders 5 and 6 then ramification is $\mathbf{C} = (6, 5, n, ..., n)$. In this case $e_1^* = 2$. Hence by Riemann Hurwitz formula,

$$2(g-1) = 2(0-1)60n + 60n\left(\left(\frac{6+3-2}{6}\right) + \left(\frac{5-1}{5}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{g+n-1}{30(n-1)} - 1$.

(b) If element of order 5 lifts an element of order $5n$, then ramification is $\mathbf{C} = (6, 5n, n, ..., n)$. As previous case $e_1^* = 2$. Hence by Riemann Hurwitz formula,

$$2(g-1) = 2(0-1)60n + 60n\left(\left(\frac{6+3-2}{6}\right) + \left(\frac{5n-1}{5n}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{g-5n+5}{30(n-1)} - 1$.

(c) If element of order 6 lifts an element of order $6n$, then ramification is $\mathbf{C} = (6, 5n, n, ..., n)$. In this case $e_1^* = 2n$. Furthermore $(2n, 3) = 1$ and $2n|(3-1)$. Hence only possible value for n is one. So Riemann Hurwitz gives,

$$2(g-1) = 2(0-1)60n + 60n\left(\left(\frac{6n+3-2}{6n}\right) + \left(\frac{5-1}{5}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{g-6n+6}{30(n-1)} - 1$.

(d) If both elements of orders 6 and 5 lift to elements of orders 5 and 6 then ramification is $\mathbf{C} = (6n, 5n, n, ..., n)$. As in previous case $e_1^* = 2n$ and only possible value for n is one.

$$2(g-1) = 2(0-1)60n + 60n\left(\left(\frac{6n+3-2}{6n}\right) + \left(\frac{5n-1}{5n}\right) + \left(\frac{n-1}{n}\right)(\delta+1)\right).$$

Then $\delta = \frac{g}{30(n-1)} - 1$.

By Lemma 3, we know that extensions A_5 by C_n is central. By Table 1 in [15] $H^2(A_5, C_n) = C_{(n,2)}$. So if G has ramification as in cases a and b then $G \cong A_5 \times C_n$. According to cases c and d, only possible value for n is one. So there are no possible group extensions for those two cases. □

4. The Main Theorem

We combine Theorems 3.2 - 3.12 altogether to make main theorem. This main theorem gives us all possible automorphism groups of genus $g \geq 2$ cyclic curves defined over the finite field of characteristic p.

Theorem 4.1. *Let $\mathcal{X}_g$ be a genus $g \geq 2$ irreducible cyclic curve defined over an algebraically closed field k, $char(k) = p \neq 2$, $G = Aut(\mathcal{X}_g)$, $\bar{G}$ its reduced automorphism group.*

(1) *If $\bar{G} \cong C_m$ then $G \cong C_{mn}$ or*

$$\langle r, s | \, r^n = 1, s^m = 1, srs^{-1} = r^l \rangle$$

where (l,n)=1 and $l^m \equiv 1$ (mod n).

(2) *If $\bar{G} \cong D_{2m}$ then $G \cong D_{2m} \times C_n$ or*

$$G_5 = \langle r, s, t | \, r^n = 1, s^2 = r, t^2 = 1, (st)^m = 1, srs^{-1} = r, trt^{-1} = r^{n-1} \rangle$$

$$G_6 = D_{2mn}$$

$$G_7 = \langle r, s, t | \, r^n = 1, s^2 = r, t^2 = r^{n-1}, (st)^m = 1, srs^{-1} = r, trt^{-1} = r \rangle$$

$$G_8 = \langle r, s, t | \, r^n = 1, s^2 = r, t^2 = 1, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r^{n-1} \rangle$$

$$G_9 = \langle r, s, t | \, r^n = 1, s^2 = r, t^2 = r^{n-1}, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle$$

(3) *If $\bar{G} \cong A_4$ and $p \neq 3$ then $G \cong A_4 \times C_n$ or*

$$G'_{10} = \langle r, s, t | \, r^n = 1, s^2 = 1, t^3 = 1, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^l \rangle$$

$$G'_{12} = \langle r, s, t | \, r^n = 1, s^2 = 1, t^3 = r^{\frac{n}{3}}, (st)^3 = r^{\frac{n}{3}}, srs^{-1} = r, trt^{-1} = r^l \rangle$$

where $(l, n) = 1$ and $l^3 \equiv 1$ (mod n) or

$$\langle r, s, t | \, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^5 = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle$$

or

$$G_{10} = \langle r, s, t | \, r^n = 1, s^2 = 1, t^3 = 1, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^k \rangle$$

$$G_{13} = \langle r, s, t | \, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = 1, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^k \rangle$$

where $(k, n) = 1$ and $k^3 \equiv 1$ (mod n).

(4) *If $\bar{G} \cong S_4$ and $p \neq 3$ then $G \cong S_4 \times C_n$ or*

$$G_{16} = \langle r, s, t | \, r^n = 1, s^2 = 1, t^3 = 1, (st)^4 = 1, srs^{-1} = r^l, trt^{-1} = r \rangle$$

$$G_{18} = \langle r, s, t | \, r^n = 1, s^2 = 1, t^3 = 1, (st)^4 = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r \rangle$$

$$G_{20} = \langle r, s, t | \, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = 1, (st)^4 = 1, srs^{-1} = r^l, trt^{-1} = r \rangle$$

$$G_{22} = \langle r, s, t | \, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = 1, (st)^4 = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r \rangle$$

where $(l, n) = 1$ and $l^2 \equiv 1$ (mod n).

(5) *If $\bar{G} \cong A_5$ and $p \neq 5$ then $G \cong A_5 \times C_n$ or*

$$\langle r, s, t | \, r^n = 1, s^2 = r^{\frac{n}{2}}, t^3 = r^{\frac{n}{2}}, (st)^5 = r^{\frac{n}{2}}, srs^{-1} = r, trt^{-1} = r \rangle$$

(6) *If $\bar{G} \cong U$ then $G \cong U \times C_n$ or*

$$< r, s_1, s_2, ..., s_t | r^n = s_1^p = s_2^p = ... = s_t^p = 1,$$
$$s_i s_j = s_j s_i, s_i r s_i^{-1} = r^l, 1 \leq i, j \leq t >$$

where $(l, n) = 1$ and $l^p \equiv 1$ (mod n).

(7) *If $\bar{G} \cong K_m$ then $G \cong$*

$$< r, s_1, ..., s_t, v | r^n = s_1^p = ... = s_t^p = v^m = 1, s_i s_j = s_j s_i,$$
$$vrv^{-1} = r, s_i r s_i^{-1} = r^l, s_i v s_i^{-1} = v^k, 1 \leq i, j \leq t >$$

where $(l,n)=1$ *and* $l^p \equiv 1$ *(mod* n*),* $(k,m)=1$ *and* $k^p \equiv 1$ *(mod* m*) or*

$$\langle r, s_1, ..., s_t | r^{nm} = s_1^p = ... = s_t^p = 1, s_i s_j = s_j s_i, s_i r s_i^{-1} = r^l, 1 \leq i,j \leq t \rangle$$

where $(l,nm)=1$ *and* $l^p \equiv 1$ *(mod* nm*).*

(8) *If* $\bar{G} \cong PSL_2(q)$ *then* $G \cong PSL_2(q) \times C_n$ *or* $SL_2(3)$.

(9) *If* $\bar{G} \cong PGL(2,q)$ *then* $G \cong PGL(2,q) \times C_n$.

4.1. **Automorphism groups of genus 3 cyclic curves.** Applying Theorem 3.1 through Theorem 3.12, we obtain the automorphism groups of a genus 3 cyclic curve defined over algebraically closed field of characteristic 0,3,5,7 and bigger than 7. We listed GAP group ID of those groups in following theorem.

Theorem 4.2. *Let* $\mathcal{X}_g$ *be a genus 3 cyclic curve defined over a field of characteristic* p*. Then the automorphism groups of* $\mathcal{X}_g$ *are as follows.*

i): $p = 0$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(8,3)$, $(7,1)$, $(21,1)$, $(14,2)$, $(6,2)$, $(12,2)$, $(9,1)$, $(8,1)$, $(8,5)$, $(16,11)$, $(16,10)$, $(32,9)$, $(30,2)$, $(42,3)$, $(12,4)$, $(16,7)$, $(24,5)$, $(18,3)$, $(16,8)$, $(48,33)$, $(48,48)$.

ii): $p = 3$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(8,3)$, $(7,1)$, $(14,2)$, $(6,2)$, $(8,1)$, $(8,5)$, $(16,11)$, $(16,10)$, $(32,9)$, $(30,2)$, $(16,7)$, $(16,8)$, $(6,2)$.

iii): $p = 5$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(8,3)$, $(7,1)$, $(21,1)$, $(14,2)$, $(6,2)$, $(12,2)$, $(9,1)$, $(8,1)$, $(8,5)$, $(16,11)$, $(16,10)$, $(32,9)$, $(42,3)$, $(12,4)$, $(16,7)$, $(24,5)$, $(18,3)$, $(16,8)$, $(48,33)$, $(48,48)$.

iv): $p = 7$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(8,3)$, $(7,1)$, $(21,1)$, $(6,2)$, $(12,2)$, $(9,1)$, $(8,1)$, $(8,5)$, $(16,11)$, $(16,10)$, $(32,9)$, $(30,2)$, $(42,3)$, $(12,4)$, $(16,7)$, $(24,5)$, $(18,3)$, $(16,8)$, $(48,33)$, $(48,48)$.

v): $p > 7$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(8,3)$, $(7,1)$, $(21,1)$, $(14,2)$, $(6,2)$, $(12,2)$, $(9,1)$, $(8,1)$, $(8,5)$, $(16,11)$, $(16,10)$, $(32,9)$, $(30,2)$, $(42,3)$, $(12,4)$, $(16,7)$, $(24,5)$, $(18,3)$, $(16,8)$, $(48,33)$, $(48,48)$.

4.2. **Automorphism groups of genus 4 cyclic curves.** Again applying Theorem 3.1 through Theorem 3.12, we obtain the following groups as automorphism groups of a genus 4 cyclic curve defined over algebraically closed field of characteristic 0,3,5,7 and bigger than 7. We listed GAP group ID of those groups in following theorem.

Theorem 4.3. *Let* $\mathcal{X}_g$ *be a genus 4 cyclic curve defined over a field of characteristic* p*. Then the automorphism groups of* $\mathcal{X}_g$ *are as follows.*

i): $p = 0$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(6,2)$, $(9,2)$, $(5,1)$, $(10,2)$, $(20,1)$, $(9,1)$, $(27,4)$, $(18,2)$, $(15,1)$, $(4,1)$, $(20,4)$, $(18,3)$, $(8,3)$, $(40,8)$, $(12,5)$, $(36,12)$, $(54,4)$, $(16,7)$, $(20,5)$, $(32,19)$, $(24,10)$, $(8,4)$, $(60,9)$, $(36,11)$, $(24,3)$, $(72,42)$.

ii): $p = 3$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(6,2)$, $(5,1)$, $(10,2)$, $(20,1)$, $(9,1)$, $(18,2)$, $(15,1)$, $(4,1)$, $(20,4)$, $(8,3)$, $(40,8)$, $(12,5)$, $(16,7)$, $(20,5)$, $(32,19)$, $(24,10)$, $(8,4)$, $(9,2)$, $(18,5)$.

iii): $p = 5$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(6,2)$, $(9,2)$, $(5,1)$, $(10,2)$, $(20,1)$, $(9,1)$, $(27,4)$, $(18,2)$, $(4,1)$, $(18,3)$, $(8,3)$, $(12,5)$, $(36,12)$, $(54,4)$, $(16,7)$, $(20,5)$, $(32,19)$, $(24,10)$, $(8,4)$, $(60,9)$, $(36,11)$, $(24,3)$, $(72,42)$, $(10,2)$, $(18,5)$.

iv): $p = 7$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(6,2)$, $(9,2)$, $(5,1)$, $(10,2)$, $(20,1)$, $(9,1)$, $(27,4)$, $(18,2)$, $(15,1)$, $(4,1)$, $(20,4)$, $(18,3)$, $(8,3)$, $(40,8)$, $(12,5)$, $(36,12)$, $(54,4)$, $(16,7)$, $(20,5)$, $(32,19)$, $(24,10)$, $(8,4)$, $(60,9)$, $(36,11)$, $(24,3)$, $(72,42)$.

v): $p > 7$ *:* $(2,1)$, $(4,2)$, $(3,1)$, $(6,2)$, $(9,2)$, $(5,1)$, $(10,2)$, $(20,1)$, $(9,1)$, $(27,4)$, $(18,2)$, $(15,1)$, $(4,1)$, $(20,4)$, $(18,3)$, $(8,3)$, $(40,8)$, $(12,5)$, $(36,12)$, $(54,4)$, $(16,7)$, $(20,5)$, $(32,19)$, $(24,10)$, $(8,4)$, $(60,9)$, $(36,11)$, $(24,3)$, $(72,42)$.

References

[1] Rolf Brandt, *Ü*ber die automorphismengruppen von algebraischen funkionenkörpern. Ph.D. thesis, Universität-Gesamthochschule Essen, 1988.

[2] R. Brandt, H. Stichtenoth, Die Automorphismengruppen hyperelliptischer Kurven, Man. Math 55 (1986), 83–92.

[3] E. Bujalance, J. Gamboa, G. Gromadzki, The full automorphism groups of hyperelliptic Riemann surfaces, Manuscripta Math. 79 (1993), no. 3-4, 267–282.

[4] E. Nart, D Sadornil, Hyperelliptic curves of genus three over finite fields of even characteristic. Finite Fields Appl. 10 (2004), no. 2, 198–220.

[5] A. Hurwitz, *Ü*ber algebraische Gebilde mit eindeutigen Transformationen in sich, Math. Ann. 41 (1893), 403-442.

[6] W. Baily, On the automorphism group of a generic curve of genus > 2. J. Math. Kyoto Univ. 1 1961/1962 101–108; correction, 325.

[7] Y. Demirbas, Automorphism groups of hyperelliptic curves of genus 3 in characteristic 2, Computational aspects of algebraic curves, T. Shaska (Edt), Lect. Notes in Comp., World Scientific, 2005.

[8] I. Schur, Utersuchen *ü*ber die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, J. Reine. Angew. Math., 132 (1907), 85-137.

[9] Gutierrez, J.; Shaska, T. Hyperelliptic curves with extra involutions. LMS J. Comput. Math. 8 (2005), 102–115.

[10] Magaard, Kay; Shaska, Tanush; Vlklein, Helmut Genus 2 curves that admit a degree 5 map to an elliptic curve. Forum Math. 21 (2009), no. 3, 547–566.

[11] K. Magaard, T. Shaska, S. Shpectorov, H. Völklein, The locus of curves with prescribed automorphism group. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). Sürikaisekikenkyüsho Kökyüroku No. 1267 (2002), 112–141.

[12] G. A. Miller, H. F. Blichfeldt, L. E. Dickson, Theory and applications of finite groups. (English) 2. ed. XVII + 390 p. New York, Stechert. Published: 1938

[13] P. G. Henn, Die Automorphismengruppen der algebraischen Funktionenkörper vom Geschlecht 3, PhD thesis, University of Heidelberg, (1976).

[14] P. Roquette, Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik. Math. Z. 117 1970 157–163.

[15] A. Kontogeorgis, The Group of Automorphisms of Cyclic Extensions of Rational Function Fields, J. Algebra 216(2) (1999), 665-706.

[16] C. R. Valentini, L. M. Madan, A Hauptsatz of L. E. Dickson and Artin-Scheier extension, J. Reine Angew. Math. 318 (1980), 156-177.

[17] Sanjeewa, R.; Shaska, T. Determining equations of families of cyclic curves. Albanian J. Math. 2 (2008), no. 3, 199–213.

[18] Sevilla, David; Shaska, Tanush Hyperelliptic curves with reduced automorphism group A_5. Appl. Algebra Engrg. Comm. Comput. 18 (2007), no. 1-2, 3–20.

[19] Shaska, Tanush Some special families of hyperelliptic curves. J. Algebra Appl. 3 (2004), no. 1, 75–89.

[20] T. Shaska, Subvarieties of the Hyperelliptic Moduli Determined by Group Actions, Serdica Math. J. 32 (2006), 355-374.

[21] T. Shaska, J. Thompson, On the generic curve of genus 3. Affine algebraic geometry, 233–243, Contemp. Math., 369, Amer. Math. Soc., Providence, RI, 2005.

[22] T. Shaska, H. Völklein, Elliptic subfields and automorphisms of genus 2 function fields. Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 703–723, Springer, Berlin, 2004.

[23] H. Stichtenoth, *Ü*ber die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe. Arch. Math. (Basel) 24 (1973) 527–544.

[24] S. Tufféry, Les automorphismes des courbes de genre 3 de caractristique 2. C. R. Acad. Sci. Paris Sér. I Math. 321 (1995), no. 2, 205–210.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 4, Pages 161–174
ISSN 1930-1235: (2009)

MEAN STAIRCASES OF THE RIEMANN ZEROS: A COMMENT ON THE LAMBERT W-FUNCTION AND AN ALGEBRAIC ASPECT

DAVIDE A MARCA, STEFANO BELTRAMINELLI, AND DANILO MERLINI

Abstract. In this note we discuss explicitly the structure of some simple sets of values on the critical line (the "trivial critical values") which are associated with the mean staircases emerging from the Zeta function. They are given as solutions of an equation involving the Lambert W-function. The argument of the latter function may then be set equal to a special $N \times N$ (classical) matrix (for every N) related to the Hamiltonian of the Mehta-Dyson model. In this way we specify a function of an hermitean operator whose eigenvalues are exactly these values. In the general case, the sets of such trivial critical values (zeros) are special solutions of a parametric equation involving a linear combination of $\mathrm{Re}\,\zeta(s)$ and $\mathrm{Im}\,\zeta(s)$ on the critical line.

This research note is dedicated to the international Swiss-Italian mathematician and physicist Professor Dr. Sergio Albeverio on the occasion of his seventieth birthday; a friend and long-standing scientific director of Cerfim (Research Center for Mathematics and Physics of Locarno, situated opposite the "Rivellino"[1]).

1. Introduction: a search for an hermitean operator associated with the Riemann Zeta Function

There is much interest in understanding the complexity related to the Riemann Hypothesis (RH) and concerned with the location and the structure of the nontrivial zeros of the Riemann Zeta function $\zeta(s)$, where $s = \rho + it$ is the complex variable.

Following a suggestion of Hilbert and Polya, in recent years many efforts have been devoted to a possible construction of an hermitean operator having as eigenvalues the imaginary parts t_n of the nth nontrivial zeros of ζ (ζ being meromorphic, the zeros are countable). These are given by the solutions of the equation $\zeta(\rho_n + it_n) = 0$, $n = 1, 2, \ldots$. If $\rho_n = \frac{1}{2}$ for all n, then all the zeros lie on the critical line (the RH is true); the program is then to find an hermitean "operator" T such that $T \cdot \varphi_n = t_n \cdot \varphi_n$ in some appropriate (Hibert) space (φ_n would be the nth eigenvector of T).

There are today many strategies in the direction of constructing such an operator and in the sequel we will shortly comment on some (among many others) very stimulating works on the subject.

1991 *Mathematics Subject Classification.* 11M26.

Key words and phrases. Riemann Zeta function, Lambert W-function, Riemann zeros, harmonic oscillator, Riemann Hypothesis.

[1]The Bastion "Il Rivellino", is 95% attribuable to Leonardo da Vinci (1507).

In [1], Pitkänen's heuristic work goes in the direction of constructing orthogonality relations between eigenfunctions of a non hermitean operator related to the superconformal symmetries; a different operator than the one just mentioned has also been proposed in [2] by Castro, Granik and Mahecha in terms of the Jacobi Theta series and an orthogonal relation among its eigenfunctions has also been found. In the rigorous work by Elizalde et al. [3] some problems with those approches have been pointed out.

In a work of some years ago Julia [4] proposed a fermionic version of the Zeta function which should be related to the partition function of a system of p-adic oscillators in thermal equilibrium.

In two others pioneering works of these years, Berry and Keating [5, 6] proposed an interesting heuristic operator to study the energy levels t_n (the imaginary parts of the nontrivial zeros of the Zeta function). The proposed Hamiltonian (in one dimension) has a very simple form given, on a dense domain, by: $H = p \cdot x + \frac{1}{2}$, where

$$p = \left(\frac{1}{i}\right) \frac{\partial}{\partial x}. \tag{1}$$

As explained by the authors, the difficulty is then to define appropriate spaces and boundary conditions to properly determine p and H as hermitean operators. In such an approach the heuristic appearance of "instantons" is also discussed.

In another important work Bump et al. [7] introduced a local RH and proved in particular that the Mellin transform of the Hermite polynomials (associated with the usual quantum mechanical harmonic oscillator) contains as a factor a polynomial $p_n(s)$, corresponding to the nth energy eigenstate of the oscillator, whose zeros are exactly located on the critical line $\sigma = \frac{1}{2}$. The relation of the polynomials $p_n(s)$ with some truncated approximation of the entire funcion $\xi(s)$ (the Xi-function), related to the Riemann Zeta function seems to be still lacking.

Other important mathematical results concerning the nontrivial Riemann zeros, have been obtained by many leading specialists (see among others the work by Connes [8], the work by Albeverio and Cebulla [9] and the recent work on the xp Hamiltonian by Sierra [10]).

Let us also mention that for the nontrivial zeros of the Zeta function an interesting equation has been proposed originally by Berry and Keating in [5]. In fact, remembering the definition of $\xi(s)$, given by:

$$\xi(s) := \frac{1}{2} s\,(s-1)\,\pi^{-\frac{s}{2}}\,\Gamma\left(\frac{s}{2}\right)\zeta\,(s) = \xi(1-s) \tag{2}$$

an equation possibly giving an approximation to the zeros of ξ is proposed in [5] and given by:

$$\frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)} + \frac{\pi^{\frac{1-s}{2}}}{\Gamma\left(\frac{1-s}{2}\right)} = 0. \tag{3}$$

As stated by the authors, (3) could be considered as a "quantization condition". Unfortunately, as mentioned in [5], (3) possesses complex zeros and so can not be used to provide an hermitean operator which would generate the nontrivial zeros of ζ.

The content of our note is concerned with the "mean staircase" of the Riemann zeros. We first construct sets of solutions of a parametric equation involving a linear combination of $\mathrm{Re}\,\zeta\,(s)$ and $\mathrm{Im}\,\zeta\,(s)$ and point out an explicit characterization of

them using the Lambert W-function. Then we introduce a specific argument (an $n \times n$ hermitean matrix H, describing a discrete harmonic oscillator with creation and annihilation "operators" a and a^* such that $[a, a^*] = -2$) into the Lambert W-function. So we obtain, for the above values, the same goal that the "Polya-Hilbert program" has for the nontrivial zeros of the Zeta function.

2. The mean staircaise of the Riemann zeros and the trivial critical values on the critical line associated with it

Let $\xi(s)$ be the Xi-function given by (2) and $s = \frac{1}{2} + it$ a complex variable on the critical line. If $N(t)$ denotes the number of zeros of ξ in the critical strip of height smaller or equal to t, and if $S(t) := \frac{1}{\pi} \arg\left(\zeta\left(\frac{1}{2} + it\right)\right)$, then from [11] we have:

$$N(t) = \langle N(t) \rangle + S\,(t) + O\left(\frac{1}{t}\right) \tag{4}$$

where

$$\langle N(t) \rangle = \frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) + \frac{7}{8}. \tag{5}$$

$\langle N(t) \rangle$, the "bulk contribution" to N, is called the "mean staircase of the zeros". The fluctuations of the number of zeros around the mean staircase, are given by the function $S(t)$. It is known [11] that $S(t) = O\,(\ln t)$ without assuming RH while, assuming RH is true, it is known that $S(t) = O\left(\frac{\ln t}{\ln(\ln t)}\right)$.

We introduce a model related to (4) by replacing (4) by (6), which corresponds to setting $S(t) + O\left(\frac{1}{t}\right) = \lambda$ for a fixed real parameter λ. So (4) becomes:

$$N(t) = \frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) + \frac{7}{8} + \lambda. \tag{6}$$

For each fixed λ and for each $n \in \mathbb{N}$, we can define a set of real values $t_n(\lambda)$ which are solutions of:

$$N(t) = \frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) + \frac{7}{8} + \lambda = n. \tag{7}$$

We call the $t_n(\lambda)$ "trivial values on the critical line" or shortly "trivial critical values". Trivial because they are fully given by (7) and critical because they lie on the critical line. On the other hand, we will indicate the imaginary part of the nth nontrivial zero of ζ simply by t_n and call it a true zero (of ζ).

Notice that since $\arg\left(\zeta\left(\frac{1}{2} + it\right)\right) = \arctan\left(\frac{\operatorname{Im}\zeta\left(\frac{1}{2}+it\right)}{\operatorname{Re}\zeta\left(\frac{1}{2}+it\right)}\right)$, we obtain

$$\frac{\operatorname{Im}\zeta\left(\frac{1}{2} + it\right)}{\operatorname{Re}\zeta\left(\frac{1}{2} + it\right)} = \tan\left(\lambda\pi\right). \tag{8}$$

So for every λ and for $\operatorname{Re}\zeta\left(\frac{1}{2} + it\right) \neq 0$ the sequences $\{\, t_n(\lambda) \,\}$ are defined by:

$$\{\, t_n(\lambda) \,\} = \left\{\, t \in \mathbb{R} \mid \operatorname{Im}\zeta\left(\frac{1}{2} + it\right) - \tan\left(\lambda\pi\right)\operatorname{Re}\zeta\left(\frac{1}{2} + it\right) = 0 \,\right\}. \tag{9}$$

Note that we may restrict the values of λ to the interval $\left]-\frac{1}{2}, \frac{1}{2}\right[$ and for $|\lambda| = \frac{1}{2}$ (8) is aquivalent to $\operatorname{Re}\zeta\left(\frac{1}{2} + it\right) = 0$ and $\operatorname{Im}\zeta\left(\frac{1}{2} + it\right) \neq 0$.

Two particular sets of interest are defined by the choices $\lambda = 0$ and $\lambda = \frac{1}{2}$. In the first case we have the set:

$$\{\, t_n^* \,\} := \{\, t_n(0) \,\} = \left\{ t \in \mathbb{R} \mid \operatorname{Re}\zeta\left(\frac{1}{2} + it\right) \neq 0 \wedge \operatorname{Im}\zeta\left(\frac{1}{2} + it\right) = 0 \right\} \tag{10}$$

or equivalently each t_n^* is the solution of

$$\frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) + \frac{7}{8} = n. \tag{11}$$

This set has been known for a long time and constitutes the "Gram points" [11].

The second set is given by the solutions t_n^{**} of

$$\frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) + \frac{7}{8} = n - \frac{1}{2}, \text{ or} \tag{12}$$

$$\{\, t_n^{**} \,\} := \{\, t_n(1/2) \,\} = \left\{ t \in \mathbb{R} \mid \operatorname{Re}\zeta\left(\frac{1}{2} + it\right) = 0 \wedge \operatorname{Im}\zeta\left(\frac{1}{2} + it\right) \neq 0 \right\} \tag{13}$$

We note that the values t_n^* and t_n^{**} are given by the abscissa of the intersection points between the staircase (5) and the two functions $\pi^{-1}\arg\left(\xi\left(\frac{1}{2} + it\right)\right)$ and $\pi^{-1}\arg\left(\xi\left(\frac{1}{2} + it\right)\right) - \frac{1}{2}$. The plot of Fig. 1 illustrates the situation for some low lying true zeros. The values for t_n^* lie mostly in between the exact value of the Riemann zeros t_{n-1} and t_n, but it is known that the "Gram law" [11] fails for the first time at $t = 282.4\ldots$ ("first instanton" according to [5]).

The solution of the above equations which give t_n^* and t_n^{**} using a very special function (the Lambert W-function, see [12]) is given below in Section 3.

3. An exact solution for the sequence t_n^*, t_n^{**} and $t_n(\lambda)$

The equation corresponding to (11), may be written in the form

$$\left(\frac{t}{2\pi\mathrm{e}}\right)^{\frac{t}{2\pi\mathrm{e}}} = \exp\left(\frac{n - \frac{7}{8}}{\mathrm{e}}\right) \tag{14}$$

and the equation corresponding to (12) in the form

$$\left(\frac{t}{2\pi\mathrm{e}}\right)^{\frac{t}{2\pi\mathrm{e}}} = \exp\left(\frac{n - \frac{1}{2} - \frac{7}{8}}{\mathrm{e}}\right) \tag{15}$$

so that introducing the new variables $x = \frac{n - \frac{7}{8}}{\mathrm{e}}$ respectively $x = \frac{n - \frac{1}{2} - \frac{7}{8}}{\mathrm{e}}$ we obtain the equation (from (14) and (15), $x > 0$)

$$W(x)\exp\left(W(x)\right) = x. \tag{16}$$

The function $W(x)$ defined by the functional equation (16) is called the Lambert W-function and has been studied extensively in these recent years. In fact such an equation appears in many fields of science. In particular the use of such a function has appeared in the study of the wave equation in the double-well Dirac delta function model or in the solution of a jet fuel problem. See [12] for an important work on the subject. Moreover the Lambert W-function appears also in combinatorics as the generating function of trees and as explained in [12] it has many applications, although its presence often goes unrecognized.

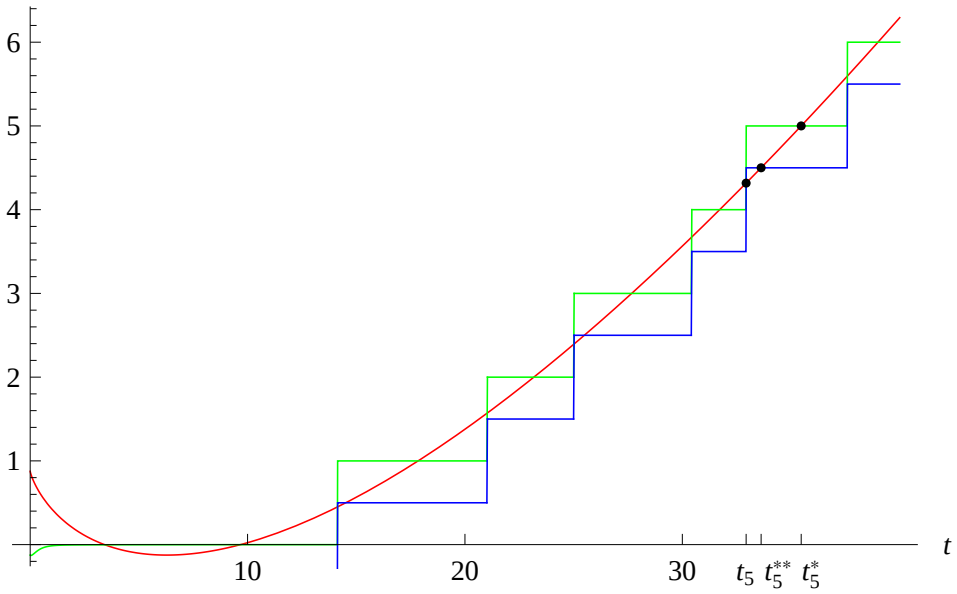


FIGURE 1. Plot of $\langle N(t)\rangle = \frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right)-1\right)+\frac{7}{8}$ (red curve), $\langle N(t)\rangle + S(t)$ (green stair) and $\langle N(t)\rangle + S(t) - \frac{1}{2}$ (blue stair), where $S(t) := \frac{1}{\pi}\arg\left(\zeta\left(\frac{1}{2}+it\right)\right)$

The Lambert W-function has many complex branches; of interest here is the principal branch of W which is analytic at $x = 0$. The solutions of (11) and (12) are given by:

$$t_n^* = 2\pi\mathrm{e}\cdot\exp\left(W\left(\frac{n-\frac{7}{8}}{\mathrm{e}}\right)\right) \tag{17}$$

$$t_n^{**} = 2\pi\mathrm{e}\cdot\exp\left(W\left(\frac{n-\frac{1}{2}-\frac{7}{8}}{\mathrm{e}}\right)\right) \tag{18}$$

with W here understood as the principal branch of the Lambert W-function. We have thus constructed, with the help of the Lambert W-function, the sequences $\{t_n^*\}$ and $\{t_n^{**}\}$. In the general case where $S(t) + O\left(\frac{1}{t}\right) = \lambda$, we obtain the general set of $t_n(\lambda)$ values given by:

$$t_n(\lambda) = 2\pi\mathrm{e}\cdot\exp\left(W\left(\frac{n-\frac{7}{8}-\lambda}{\mathrm{e}}\right)\right). \tag{19}$$

Getting back now to the case $\lambda = 0$, it should be noted that, having replaced in (4) $S(t) + O\left(\frac{1}{t}\right)$ by 0 we cannot expect in (11) n, which would correspond to the exact value t_n of a true zero, to be an integer. For the first few low lying true zeros t_n of ζ, it may be observed numerically that the corresponding values of the index n, let say n^*, are randomly distributed mostly between two consecutive integers, but their mean values are nearby the integers plus $\frac{1}{2}$. A calculation with some known true zeros of ζ gives a mean value of 0.49. So, in average it seems that the

behavior of the true zeros t_n "follows" more the pattern of the t_n^{**}. In a similar way the values of the first set, i.e. t_n^*, lie mostly in between two true zeros of ζ, but of course it is known that there are very complicated phenomena associated with the chaotic behavior of the non trivial zeros of the Riemann ζ function.

As an example, the first of the instantons [5] corresponding to $n = 127$, is located at the value of $t_{127} = 282.4651\ldots$. In Table 1 we give the values of t_n^* and of t_n (a true zero) around $t = 280$.

$$
\begin{aligned}
t_{126} &= 279.22925\\
t^*_{126} &= 280.80246\\
t^*_{127} &= 282.4547596\\
t_{127} &= 282.4651147\\
t_{128} &= 283.211185\\
t^*_{128} &= 284.1045158\\
t_{129} &= 284.8359639
\end{aligned}
$$

TABLE 1

From such numerical computations we see that two consecutive zeros of $\operatorname{Im}\zeta$ alone are followed by two consecutive true zeros, in particular t^*_{127} anticipates t_{127}. The difference between the two subsequent t values (i.e. $t_{127} - t^*_{127}$) is very small and given by $\Delta t = 0.0103$. The phase change is given by $i\pi$ as illustrated on the plot of $\operatorname{Im}\ln\left(\zeta\left(\frac{1}{2}+it\right)\right)$ (step curve) and that of $\operatorname{Im}\zeta\left(\frac{1}{2}+it\right)$.

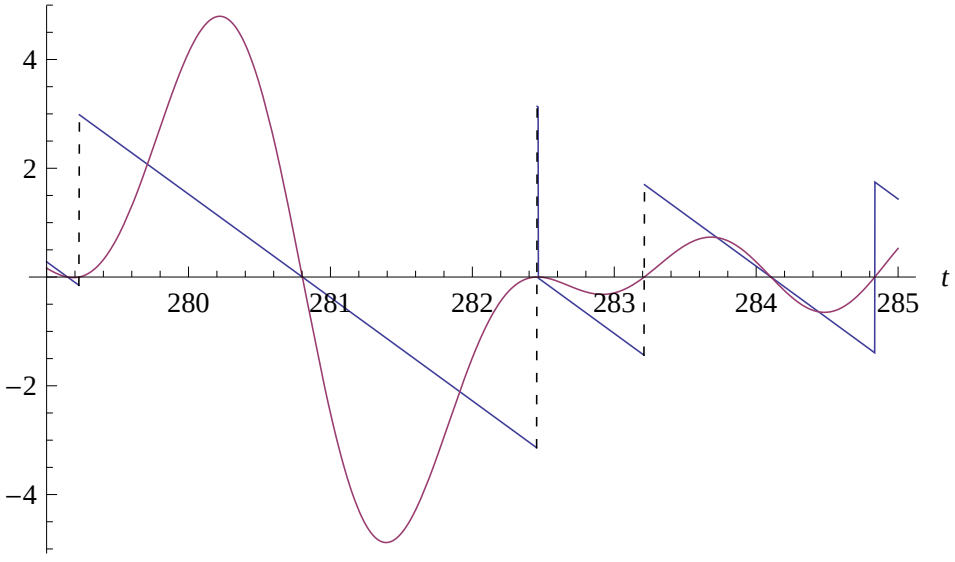


FIGURE 2. Plot of $\operatorname{Im}\zeta\left(\frac{1}{2}+it\right)$ (continuous curve) and $\operatorname{Im}\ln\left(\zeta\left(\frac{1}{2}+it\right)\right) = \pi S(t)$ (step curve).

For the first 500 energy levels, that is for values of t from 0 to $t = 811.184\ldots$ (level number $n = 500$), it may be seen that there are 13 instantons (in the language

of [5]), all with a Maslov phase change of $+i\pi$ or of $-i\pi$. The width Δt is usually small but it is larger for the instanton located at $t = 650.66$ (n corresponding to 379), where $\Delta t = 0.31\ldots$. Returning now to the two sets $\{\, t_n^* \,\}$ and $\{\, t_n^{**} \,\}$, we note the elementary relation which follows from (11) and (12) given by:

$$\frac{t_n^* + t_{n+1}^*}{2} = t_{n+1}^{**} \tag{20}$$

and

$$\frac{t_{n-1}^{**} + t_{n+1}^{**}}{2} = t_n^*. \tag{21}$$

(20) and (21) say that the zeros of the real part of $\zeta\left(\frac{1}{2} + it\right)$ alone are obtained by those of the imaginary part alone by simple average and viceversa. The two sequences are regularly spaced and the mean distance between two trivial critical values at the height t, as the mean staircase indicates (5), is given approximatively by:

$$\frac{t}{\langle N(t)\rangle} = \frac{2\pi}{\ln \frac{t}{2\pi}} = \frac{2\pi}{\ln n} \tag{22}$$

for t and n large.

Before proposing an hermitean operator for the sequences of the trivial critical values it is important to investigate a possible "quantization condition" for the nontrivial zeros. For this we start with the functional equation of the ζ function.

From the exact relation for the ξ-function given by:

$$\begin{aligned} \xi(s) &= \frac{1}{2}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)s(s-1) \\ &= \xi(1-s) = \frac{1}{2}\pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)(1-s)(1-s-1) \end{aligned} \tag{23}$$

$s \in \mathbb{C}$, we have that

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s). \tag{24}$$

In equation (24) we limit ourselves to consider the values $s = \frac{1}{2} + \varepsilon + it$, t, $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, and thus $1 - s = \frac{1}{2} - \varepsilon - it$; moreover we are interested in high values of t so that we may use Stirling's formula for the Gamma function given (in the sense of asymptotic equivalence) by:

$$\Gamma(x) \cong (2\pi)^{\frac{1}{2}}\, x^{x-\frac{1}{2}}\mathrm{e}^{-x} \tag{25}$$

as $x \to \infty$. From (24) and (25) we then obtain (asymptotically for $t \to \infty$)

$$\begin{aligned} &\exp\left(i\pi\left(\frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) - \frac{1}{8}\right) + i\arg\left(\zeta\left(\frac{1}{2+\varepsilon} + it\right)\right)\right) = \\ &\exp\left(-i\pi\left(\frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) - \frac{1}{8}\right) + i\arg\left(\zeta\left(\frac{1}{2-\varepsilon} - it\right)\right)\right). \end{aligned} \tag{26}$$

Since

$$\begin{aligned} \exp\left(i\arg\left(\zeta\left(\frac{1}{2} - \varepsilon - it\right)\right)\right) &= \exp\left(i\arg\left(\zeta\left(\frac{1}{2} + \varepsilon + it\right) + i\pi\right)\right) \\ &= -\exp\left(i\arg\left(\zeta\left(\frac{1}{2} + \varepsilon + it\right)\right)\right) \end{aligned}$$

we then have, taking the limit $\varepsilon \to 0$ i.e. at $\rho = \frac{1}{2}$, that:

$$\cos\Psi = 0 \text{ where } \Psi = \frac{t}{2}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) - \frac{\pi}{8} + \arg\left(\zeta\left(\frac{1}{2} + it\right)\right). \tag{27}$$

Thus $\Psi = \pi\left(n + \frac{1}{2}\right)$ with $n \in \mathbb{N}$. We then obtain:

$$\frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) - \frac{1}{8} + \frac{1}{\pi}\arg\left(\zeta\left(\frac{1}{2} + it\right)\right) = n - \frac{1}{2}$$

hence

$$\frac{t}{2\pi}\left(\ln\left(\frac{t}{2\pi}\right) - 1\right) + \frac{7}{8} + \frac{1}{\pi}\arg\left(\zeta\left(\frac{1}{2} + it\right)\right) = n + \frac{1}{2}. \tag{28}$$

(28) may be seen as a "quantum condition" for the nontrivial zeros of ζ and it is a consequence of the functional equation (24). In fact, if in (27) we neglect the last term $\arg(\zeta)$, then (27) has as a solution the second set of trivial critical values $\{t_n^{**}\}$. It is true, as remarked by Berry and Keating, that their equation stated above as (3) has complex zeros which are not the nontrivial zeros of ζ, but it should be remarked that if in (3) we set $\operatorname{Re} s = \frac{1}{2}$ then (3) reduces to (27) without the fluctuation term $\arg(\zeta)$; so the solution of (3) for $\operatorname{Re} s = \frac{1}{2}$ is the same as the second set of trivial critical values $\{t_n^{**}\}$.

Below the plots of $\cos\Psi$, with and without the term $\arg\left(\zeta\left(\frac{1}{2} + it\right)\right)$, are given. As an illustration, we may observe on that plot the first instanton discussed above and the second one located around $t = 295$. In fact the maximum of the function which gives t_n^* ((27) without the term $\arg(\zeta)$) is outside the plot of the step function given by (27). This is visible on the plot near $t = 282$ and near $t = 296$ (the second instanton). This concludes our remark on (3) and (27). In the next Section, we shall costruct an hermitean operator whose eigenvalues are the trivial critical values of the Zeta function defined above in (9).

Now in (19) a trivial critical value $t_n(\lambda)$ is given through its index n by means of the Lambert W-function so that such values are related in a non linear way to the integers n, i.e. in principle to the spectrum of an harmonic oscillator. So, for the trivial critical values, no boundary condition is needed here, since they are obtained by means of (19) in the large t limit. At this moment we are free to introduce an hermitean matrix which may generate the trivial critical values.

4. An Hermitean operator (matrix) associated with the mean staircase (trivial critical values) of the Riemann Zeta function

As remarked above, in (19) the only "quantal number" is the index n of the trivial critical values and the construction may be given using, for any n, an hermitean $n \times n$ matrix H related to the classical one dimensional many body system whose fluctuation spectrum around the equilibrium positions is that of the harmonic oscillator. In fact, the one dimensional Mehta-Dyson model of random matrices (which may be seen as a classical Coulomb system with n particles) has, at low temperature, an energy fluctuation spectrum given by the integers and it is possible to introduce correspondingly annihilation and creation operators, as studied in [13] (a short discussion is presented in the Appendix). The matrix elements of the associated hermitean matrix are then functions of the zeros of the Hermite polynomials; in this case we do not have a Hilbert space and no Schrödinger equation will be associated with the Lambert W-function.

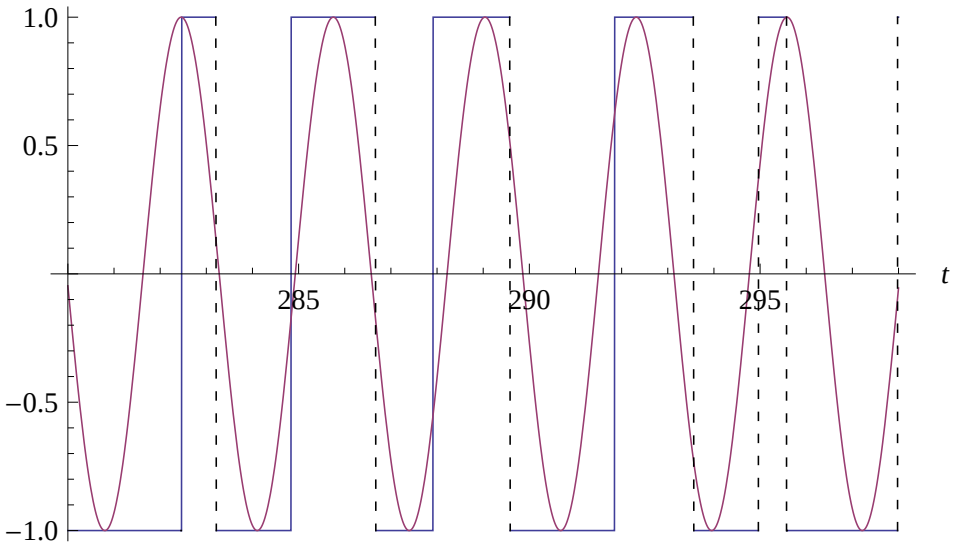


FIGURE 3. Plot of the function $\cos\Psi$ of (27) with the term $\arg\left(\zeta\left(\frac{1}{2}+it\right)\right)$ (step function) and without that term.

Another direction, i.e. that of introducing a Schrödinger equation to describe the trivial critical values may in principle be obtained as an application of the results given by Nash [14]; this is so because for large n, as it is known, (19) gives the behavior ([11], page 214) related to the asymptotic behavior of the Lambert W-function:

$$t_n(\lambda) = \frac{2\pi n}{\ln n}\left(1 - \frac{7/8+\lambda}{n}\right) \tag{29}$$

and thus the spectrum appears in fact as one for which the associated Schrödinger equation contains a Gaussian type of potential [14].

Here we will consider the matrix formulation: the point may seem to be somewhat artificial but the hermitean matrix we will use (specified in the Appendix) is related to the Mehta-Dyson model, the "starting point" of the random matrix theory and we are free to choose such a matrix (of course other choices are possible). To do this, we begin to write (19) in a slighly different form using the Stirling formula for the Gamma function of real argument given by (in the sense of the asymptotic equivalence):

$$\Gamma(x) \cong (2\pi)^{\frac{1}{2}}\, x^{x-\frac{1}{2}}\mathrm{e}^{-x} \ \text{ as } \ x \to \infty.$$

We then have that, as $t \to \infty$,

$$\begin{aligned} \ln\left(\Gamma\left(\frac{t}{2\pi}+\frac{1}{2}\right)\right) &\cong \frac{t}{2\pi}\ln\left(\frac{t}{2\pi}-1\right)+\frac{7}{8}+\frac{1}{2}\ln(2\pi)-\frac{7}{8}-\lambda \\ &= \langle N(t)\rangle + \frac{1}{2}\ln(2\pi) - \frac{7}{8} - \lambda = \langle N(t)\rangle + \theta(\lambda) \end{aligned} \tag{30}$$

where $\theta(\lambda) = \frac{1}{2}\ln(2\pi) - \frac{7}{8} - \lambda$.

Thus introducing the operator $T = T(H)$ whose eigenvalues should be the trivial critical values (as defined in the general case by (19)) as well as H, the hermitean matrix given in the Appendix and related to the Mehta-Dyson model, we may write following (30) the heuristic matrix equation:

$$\Gamma\left(\frac{T}{2\pi} + \frac{I}{2}\right) = \mathrm{e}^{H+\theta(\lambda)} \tag{31}$$

where I is the unit matrix. (31) is the equation for T, giving the trivial critical values. The inversion of this formula (if it is possible to take it) yields heuristically:

$$T(\lambda) = T(H) = 2\pi\left(\Gamma^{-1}\left(\mathrm{e}^{H+\theta}\right) - \frac{I}{2}\right). \tag{32}$$

To conclude, if $H\varphi_n = \left(n + \frac{1}{2}\right)\varphi_n$, where φ_n is the nth eigenfunction of H, then

$$T\varphi_n = 2\pi\left(\Gamma^{-1}\left(\mathrm{e}^{H+\theta(\lambda)}\right) - \frac{I}{2}\right)\varphi_n = 2\pi\left(\Gamma^{-1}\left(\mathrm{e}^{n+\theta(\lambda)}\right) - \frac{1}{2}\right)\varphi_n = t_n(\lambda)\varphi_n. \tag{33}$$

Of course (31) for the operator T is more appealing than (19) (where n is replaced by H and $t_n(\lambda)$ is replaced by matrix T) due to the combinatorial nature of the Gamma function, but the eigenvalues of the operators T are the same in the "termodynamic limit", $\dim H = n \to \infty$.

This completes the second part of our note i.e. the algebraic aspect in the construction of the trivial critical values using the two creation and annihilation operators a, a^* with $[a, a^*] = aa^* - a^*a = -2I$ connected with the Mehta-Dyson model.

Remark: If one considers the map $s = \sigma + it \to 1 - \frac{1}{s} = z$ then the critical line $s = \frac{1}{2} + it$ ($t \in \mathbb{R}$) is mapped onto the unit circumference $|z| = 1$; the set $\{\, \frac{1}{2} + it_n(\lambda)\,\}$ has as accumulation point $z = 1$ (as $n \to \infty$), which is the same accumulation point for the trivial zeros of the ζ function given by $z_n = 1 - \frac{1}{-2n} = 1 + \frac{1}{2n}$, as $n \to \infty$ (see Fig. 4). Neglecting the trivial zeros $\{z_n\}$, Fig. 4 illustrate by means of the set of trivial critical values $\{t_n(\lambda)\}$ an analogon of the Lee-Yang Theorem [15] for the zeros of the partition function for some general spin lattice system studied in statistical mechanics. If RH is true, then all nontrivial zeros of $\zeta(z)$ shall be located at the same circumference $|z| = 1$, with $z = 1$ as accumulation point.

Remark: Of course, (19) in matrix form or equivalently (31) or (32) give also the true zeros t_n, if λ is the corresponding value of the true zero. In fact a true zero (for example the first one given by $t_1 = 14.13472514\ldots$ where $\lambda_1 = -0.449\ldots$, i.e. where $\tan(\pi\lambda_1) = -6.28\ldots$) may be seen as the groundstate of the sequence of trivial critical values given by the Lambert W-function with $\lambda = \lambda_1$. The same for all the other true zeros. Thus as λ is varying in $\left]-\frac{1}{2}, \frac{1}{2}\right[$ we obtain a continuous spectrum including the imaginary part of the nontrivial zeros which are on the critical line. If λ is such that $\mathrm{Re}\,\zeta$ and $\mathrm{Im}\,\zeta$ are not both zero, then we obtain a continuous spectrum where the true zeros are missing. It is also interesting to analyse the two sequences $t_n(\lambda_1)$ and $t_n(-\lambda_1)$ and keeping those values of the two sequences which are closer to a true zero as given on Table 2 for n up to 19. From this Table we may compute the mean value of the absolute percentual error and we find the value 0.7%. Notice that such a value is smaller than the one computed with the sequence where $\lambda = \frac{1}{2}$ (i.e. with the t_n^{**}).

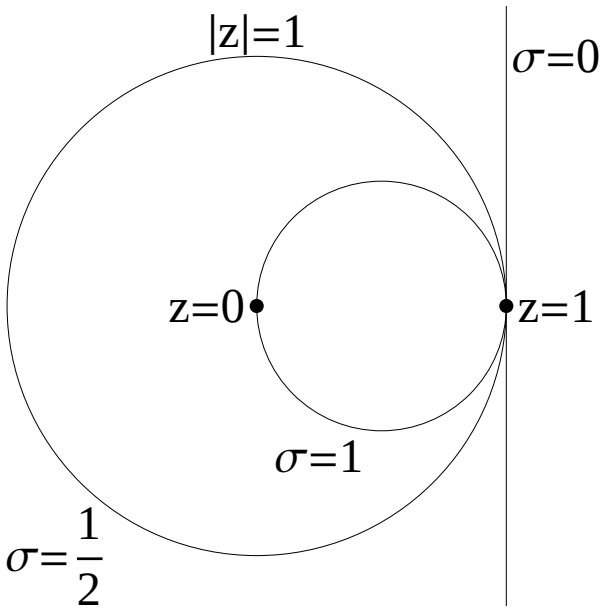


FIGURE 4. z-plane

t_n	$t_n(\lambda_1)$ or $t_n(-\lambda_1)$	t_n	$t_n(\lambda_1)$ or $t_n(-\lambda_1)$
14.134	14.138	52.970	53.066
21.022	20.919	56.446	56.263
25.010	25.266	59.347	59.097
30.424	29.942	60.831	61.595
32.424	33.435	65.112	64.593
37.586	37.434	67.079	66.999
40.918	40.869	69.546	69.632
43.327	43.831	72.067	72.225
48.005	47.321	75.704	75.043
49.773	50.081		

TABLE 2

5. Conclusion

In this note we have first obtained $t_n(\lambda)$, the explicit solution of (9) for the case where $S(t)+O(t) = \lambda$ i.e. the zeros of the function $\operatorname{Im}\zeta\left(\frac{1}{2}+it\right)-\tan(\pi\lambda)\operatorname{Re}\zeta\left(\frac{1}{2}+it\right)$ by means of the Lambert W-function.

The particular case $\lambda = 0$ gives the well known sequence of Gram points and for each value of λ, all the sequences of such trivial critical values are regularly spaced contrary to that of the nontrivial zeros which have so far been found numerically to lie on the critical line.

In the second part of our work concerning the algebraic aspect of $t_n(\lambda)$ we have formally given the construction of an operator equation for the operator $T(\lambda)$, related to an Hamiltonian H emerging from the one dimensional Mehta-Dyson model of N point charges. $T(\lambda)$ appears to be related to H in a strong nonlinear way, formally given by (19) or equivalently by (31), in operator form and has as eigenvalues the sets of trivial critical values given by (9). So in the construction, the sets of trivial critical values are related to the eigenvalues $n = 1, ..., N$ of a discrete harmonic oscillator furnished by the matrices a, a^*, i.e. the two discrete annihilation and creation operators of H (the only quantal number we have used is the index n of the corresponding trivial critical value given by (9)).

To the best of our knowledge, we do not know of any explicit existing treatment along these lines for the sets of the trivial critical values given by (9).

In a subsequent note we intend to treat (at least numerically) another sequence of values possibly "'more related"' to the nontrivial zeros of the Zeta function but not obtainable by a Lambert W-function or a Gamma function.

Updates

(1) Sierra and Townsend [16] introduced and studied an interesting physical model (a charged particle in the plane in the presence of an electrical and a magnetic potential). In particular, the lowest Landau level is connected with the smoothed counting function that gives the average number of zeros, i.e. the staircase which here we have studied, by means of a classical one-dimensional model of N interacting charged particles.

(2) Very recently Schumayer et al. [17] constructed (in particular) a quantum mechanical potential for the zeros of $\zeta(s)$, using the first 10^5 energy eigenvalues (nontrivial zeros). It is expected that the same form of a quantum mechanical potential would appear using only the values $t_n(\lambda)$ we have found in this note. For the construction of an Hamiltonian whose spectrum coincides with the primes, see also the interesting work of Sekatskii [18].

6. Appendix

We shall discuss the hermitean matrix H associated with the Mehta-Dyson model and the discrete annihilation and creation operators associated with H whose spectrum is given by the set of integers (1, 2, ..., N), for any finite N.

In [13, 19] the one dimentional Mehta-Dyson model defined by the potential energy $E = \sum_{i=0}^{N} \left(\frac{1}{2} y_i^2 - \sum_{i<j\leqslant N} \log\left(|y_i - y_j|\right) \right)$ was studied, where y_i is the position of the ith particle on the line. The fluctuation around the equilibrium positions (these are given by the zeros of the Hermite polynomials of degree N, where N is the number of particles on the line, for every finite N), i.e. the harmonic fluctuation spectrum, is given by the eigenvalues of the hermitean $N \times N$ real matrix whose elements are given by:

$$\begin{cases} H_{\mathrm{ij}} = \frac{-1}{|x_i - x_j|^2} & i \neq j \\ H_{\mathrm{ij}} = 1 + \sum_{k \neq i} \frac{1}{|x_i - x_k|^2} & i = j \end{cases}$$

$i, j = 1, \ldots, N$, where the x_i are the "equilibrium positions" i.e. the zeros of the Hermite polynomials of degree N.

The spectrum of H is given exactly by the integers (1, 2, ..., N) for every finite N and the eigenfunctions are given in terms of the Mehta-Dyson polynomials of order 1 up to N. The Hamiltonian describing the harmonic fluctuations takes then the form [13]:

$$H = N \cdot I - \frac{1}{2} a a^*$$

where I is the unit matrix of order N and a, resp a^*, are the discrete annihilation and creation operators (matrices of order $N \times N$) of H, which satisfy the commutation relation $[a, a^*] = -2I$. Moreover $[H, a^*] = a^*$ and $[H, a] = -a$.

If X_k is the kth eigenvector of H with eigenvalue the integer k, one has:

$$a^* X_{k+1} = X_{k+2}$$

and

$$a X_{k+1} = 2\,(N - k)\, X_k.$$

Explicitly, if $X_k = (\varphi_{1k}\,(x_1), \ldots, \varphi_{\mathrm{Nk}}\,(x_N))$ is the kth eigenvector, where $\varphi_k(x)$ is the kth Mehta-Dyson polynomial of argument x, then

$$a\varphi_{k+1}\,(x_1) = \frac{d}{dx_1}\,(\varphi_{k+1}\,(x_1)) = \sum_{i \neq 1}^{N} \frac{\varphi_{k+1}\,(x_1) - \varphi_{k+1}\,(x_i)}{(x_1 - x_i)}$$

and

$$a^* \varphi_{k+1}\,(x_1) = \left(2x_1 - \frac{d}{dx_1}\right) \varphi_{k+1}\,(x_1)\,.$$

H as above, with $N = n$ may be used to give the first n trivial critical values of the first set in (17) i.e. $t_1^*, \ldots, t_n^*$ while $H + \frac{1}{2}$ may be used for obtaining the first n trivial critical values of the second set in (18) i.e. $t_1^{**}, \ldots, t_n^{**}$ in the discussion on the mean staircases given in Section 2. The same holds true for the general case λ different from 0 and $\pm\frac{1}{2}$.

References

[1] Pitkänen M. A strategy for proving Riemann Hypothesis. *Acta Math. Univ. Comenianae*, 72(1):1–13, 2003.

[2] Castro C., Granik A., and Mahecha J. On susy-qm, fractal strings and steps towards a proof of the Riemann Hypothesis, arXiv:hep-th/0107266v3, September 2001.

[3] Elizalde E., Moretti V., and Zerbini S. On recent strategies proposed for proving the Riemann hypothesis. *Int. J. Mod. Phys*, A18:2189–2196, 2003.

[4] Julia B. On the statistics of primes. *Journal de physique*, 50(12):1371–1375, 1989.

[5] Berry M.V. and Keating J.P. H = xp and the Riemann zeros. In *Supersymmetry and Trace Formulae: Chaos and Disorder*, edited by Lerner et al., page 355–367, New York, Kluwer Academic Publishers, 1999.

[6] Berry M.V. and Keating J.P. The Riemann zeros and eigenvalue asymptotics. *SIAM Review*, 41(2):236–266, 1999.

[7] Bump D., Choi Kwok-Kwong, Kurlberg P., and Vaaler J. A local Riemann hypothesis, I. *Mathematische Zeitschrift*, 233(1):1–18, 2000.

[8] Connes A. Trace formula in noncommutative geometry and the zeros of the Riemann zeta function. *Selecta Mathematica, New Series*, 5(1), May 1999.

[9] Albeverio S. and Cebulla C. Müntz formula and zero free regions for the Riemann zeta function. *Bulletin des Sciences Mathématiques*, 131(1):12–38, 2007.

[10] Sierra G. A quantum mechanical model of the Riemann zeros. *New Journal of Physics*, 10, 033016, 2008.

[11] Titchmarsh E.C. The Theory of the Riemann Zeta-Function. *Oxford University Press*, 2 edition, 1986.
[12] Corless R.M., Gonnet G.H., Hare D.E.G., Jeffrey D.J., and Knuth D.E. On the Lambert W-function. *Advances in Computational Mathematics*, 5:329–359, 1996.
[13] Merlini D., Rusconi L., and Sala N. I numeri naturali come autovalori di un modello di oscillatori classici a bassa temperatura. *Bollettino della Società ticinese di Scienze naturali*, 87:29–32, 1999.
[14] Nash C. The spectrum of the Schrödinger operator and the distribution of primes. *Advances in Applied Mathematics*, 6(4):436–446, December 1985.
[15] Yang C.N., Lee T.D. Statistical Theory of Equations of State and Phase Transitions. I. Theory of Condensation, *Physical Review Letters*, 87:404–409, 1952.
[16] Sierra G. and Townsend P.K. Landau levels and Riemann zeros. *Physical Review Letters*, 101, 110201, 2008.
[17] Schumayer D., van Zyl B., and Hutchinson D. Quantum mechanical potentials related to the prime numbers and Riemann zeros. *Physical Review E*, 78, 056215, 2008.
[18] Sekatskii S.K. On the hamiltonian whose spectrum coincides with the set of primes. arXiv:0709.0364v1 [math-ph], 2007.
[19] Bernasconi A., Merlini D., and Rusconi L. Complex aspects of the Riemann Hypothesis: a computational approach. In Losa G. et al., editors, *Fractals in Biology and Medicine*, volume 3, page 333. Birkhäuser, 2002.

D. a Marca, CERFIM, Research Center for Mathematics and Physics, PO Box 1132, 6600 Locarno, Switzerland
E-mail address: davide.amarca@ti.ch

S. Beltraminelli, CERFIM, Research Center for Mathematics and Physics, PO Box 1132, 6600 Locarno, Switzerland
E-mail address: stefano.beltraminelli@ti.ch

D. Merlini, CERFIM, Research Center for Mathematics and Physics, PO Box 1132, 6600 Locarno, Switzerland
E-mail address: merlini@cerfim.ch

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 4, Pages 175–188
ISSN 1930-1235: (2009)

SOME CLASSES OF GENERAL NONCONVEX VARIATIONAL INEQUALITIES

MUHAMMAD ASLAM NOOR

Abstract. In this paper, we introduce and consider a new class of variational inequalities, which is called the general nonconvex variational inequality. We establish the equivalence between the general nonconvex variational inequalities and the fixed point problems as well as the Wiener-Hopf equations using the projection method. This alternative equivalent formulation is used to study the existence of a solution of the general convex variational inequalities. We also use this equivalence formulation to suggest some iterative methods. Convergence criteria of these new iterative is also discussed under suitable conditions. Our method of proofs is very simple as compared with other techniques.

1. Introduction

Variational inequalities theory, which was introduced by Stampacchia [39], can be viewed as a natural generalization and extension of the variational principles, the origin of can be traced back to Fermat, Newton, Leibniz, Bernoulli, Euler and Lagrange. It is tool of great power that can be applied to a wide variety of problems, which arise in almost all branches of pure, applied, physical, regional and engineering sciences. During this period, variational inequalities have played an important, fundamental and significant part as a unifying influence and as a guide in the mathematical interpretation of many physical phenomena. In fact, it has been shown that the variational inequalities provide the most natural, direct, simple and efficient framework for the general treatment of wide range of problems.Variational inequalities have been extended and generalized in several directions for studying a wide class of equilibrium problems arising in financial, economics, transportation, elasticity, optimization, pure and applied sciences, see [1-40] and the references therein. An important and useful generalization of variational inequalities is called the *general variational inequality* introduced by Noor [12] in 1988, which enables us to study the odd-order and nonsymmetric problems in a unified framework. See, for example 2.1 and example 2.2 for some applications of the general variational inequalities in differential equations and nonlinear optimization.

Received by the editors October 26, 2009 .
2000 *Mathematics Subject Classification.* Primary 49J40; Secondary 90C33.
Key words and phrases. Variational inequalities; nonconvex functions; fixed-point problem, Wiener-Hopf equations, convergence.

It is worth mentioning that almost all the results regarding the existence and iterative schemes for variational inequalities, which have been investigated and considered in the classical convexity. This is because all the techniques are based on the properties of the projection operator over convex sets, which may not hold in general for nonconvex sets. Motivated and inspired by the ongoing research in this area, we introduce and consider a new class of variational inequalities, which is called the general nonconvex variational inequality in conjunction with the uniformly prox-regular sets. It is well-known that the prox-regular are nonconvex sets and include the convex sets as a special case, see [7,37]. Using the idea and technique of Noor [26-30], we show that the projection technique can be extended for the general nonconvex variational inequalities. We establish the equivalence between the general nonconvex variational inequalities and fixed point problems using essentially the projection technique. This equivalent alternative formulation is used to discuss the existence of a solution of the nonconvex variational inequalities, which is Theorem 3.1. Theorem 3.1 extends the previous results for the general nonconvex variational inequalities. We use this alternative equivalent formulation to suggest and analyze an implicit type iterative methods for solving the nonconvex variational inequalities. In order to implement this new implicit method, we use the predictor-corrector technique to suggest a two-step method for solving the nonconvex variational inequalities, which is Algorithm 3.4. We also consider the convergence (Theorem 3.2) of the new iterative method under some suitable conditions. Some special cases are also discussed.

Related to the general nonconvex variational inequalities, we consider the problem of solving the nonconvex Wiener-Hopf equations. Using essentially the projection technique and Lemma 3.1, we show that the general nonconvex variational inequalities are equivalent to the Wiener-Hopf equations, which is Lemma 4.1. This alternative equivalent formulation is more general and flexible than the projection operator technique. This alternative equivalent formulation is used to suggest and analyze a number of iterative methods for solving the nonconvex variational inequalities. These iterative methods is the subject of Section 4. We also consider the convergence criteria of the proposed iterative methods under some suitable conditions. Several special cases are also discussed. Results obtained in this paper can be viewed as refinement and improvement of the previously known results for the variational inequalities and related optimization problems. We would like to point out that our methods of proof are very simple as compared with other techniques. It is an open problem to implement these methods numerically. The comparison of these new methods with other similar methods for solving nonconvex variational inequalities is also open problem and needs further research.

2. Preliminaries

Let H be a real Hilbert space whose inner product and norm are denoted by $\langle \cdot, \cdot \rangle$ and $\|.\|$ respectively. Let K be a nonempty and convex set in H.

We, first of all, recall the following well-known concepts from nonlinear convex analysis and nonsmooth analysis [7,37].

Definition 2.1. The proximal normal cone of K at $u \in H$ is given by

$$N_K^P(u) := \{\xi \in H : u \in P_K[u + \alpha\xi]\},$$

where $\alpha > 0$ is a constant and

$$P_K[u] = \{u^* \in K : d_K(u) = \|u - u^*\|\}.$$

Here $d_K(.)$ is the usual distance function to the subset K, that is

$$d_K(u) = \inf_{v \in K} \|v - u\|.$$

The proximal normal cone $N_K^P(u)$ has the following characterization.

Lemma 2.1. Let K be a nonempty, closed and convex subset in H. Then $\zeta \in N_K^P(u)$,
if and only if, there exists a constant $\alpha > 0$ such that

$$\langle \zeta, v - u \rangle \leq \alpha \|v - u\|^2, \quad \forall v \in K.$$

Poliquin et al. [37] and Clarke et al [7] have introduced and studied a new class of nonconvex sets, which are called uniformly prox-regular sets. This class of uniformly prox-regular sets has played an important part in many nonconvex applications such as optimization, dynamic systems and differential inclusions.

Definition 2.2. For a given $r \in (0, \infty]$, a subset K_r is said to be normalized uniformly r-prox-regular if and only if every nonzero proximal normal to K_r can be realized by an r-ball, that is, $\forall u \in K_r$ and $0 \neq \xi \in N_{K_r}^P(u)$, one has

$$\langle (\xi)/\|\xi\|, v - u \rangle \leq (1/2r)\|v - u\|^2, \quad \forall v \in K.$$

It is clear that the class of normalized uniformly prox-regular sets is sufficiently large to include the class of convex sets, p-convex sets, $C^{1,1}$submanifolds (possibly with boundary) of H, the images under a $C^{1,1}$ diffeomorphism of convex sets and many other nonconvex sets; see [7,37]. It is clear that if $r = \infty$, then uniformly prox-regularity of K_r is equivalent to the convexity of K. It is known that if K_r is a uniformly prox-regular set, then the proximal normal cone $N_{K_r}^P(u)$ is closed as a set-valued mapping.

For a given nonlinear operator T, g, we consider the problem of finding $u \in H$: $g(u) \in K_r$ such that

$$\langle Tu, g(v) - g(u) \rangle \geq 0, \quad \forall v \in H : g(v) \in K_r, \tag{1}$$

which is called the *general nonconvex variational inequality.*

If $g \equiv I$, the identity operator, then problem (1) is equivalent to finding $u \in K_r$ such that

$$\langle Tu, v - u \rangle \geq 0, \quad \forall v \in K_r, \tag{2}$$

which is known as the nonconvex variational inequality, studied and introduced by Noor [26].

If $K_r \equiv K$, the convex set in H, then problem (1) is equivalent to finding $u \in H : g(u) \in K$ such that

$$\langle Tu, g(v) - g(u) \rangle \geq 0, \forall v \in H : g(v) \in K, \tag{3}$$

which was introduced and studied by Noor [12] in 1988. To convey an idea of the applications of the general variational inequalities (3) in the differential equations, we have the following.

Example 2.1. For simplicity, we consider the third-order obstacle boundary value problem of finding u such that

$$\begin{cases} -u''' \geq f(x) & \text{on } \Omega = [0,1] \\ u \geq \psi(x) & \text{on } \Omega = [0,1] \\ [-u''' - f(x)][u - \psi(x)] = 0 & \text{on } \Omega = [0,1] \\ u(0) = 0, \quad u'(0) = 0, \quad u'(1) = 0. \end{cases} \tag{4}$$

where $f(x)$ is a continuous function and $\psi(x)$ is the obstacle function. We study the problem (4) in the framework of variational inequality approach. To do so, we first define the set K as

$$K = \{v : v \in H_0^2(\Omega) : v \geq \psi \quad \text{on } \Omega\},$$

which is a closed convex set in $H_0^2(\Omega)$, where $H_0^2(\Omega)$ is a Sobolev (Hilbert) space, see [9]. One can easily show that the energy functional associated with the problem (4) is

$$\begin{aligned} I[v] &= -\int_0^1 \left(\frac{d^3v}{dx^3}\right)\left(\frac{dv}{dx}\right)dx - 2\int_0^1 f(x)\left(\frac{dv}{dx}\right)dx, \quad \text{for all } \tfrac{dv}{dx} \in K \\ &= \int_0^1 \left(\frac{d^2v}{dx^2}\right)^2 dx - 2\int_0^1 f(x)\left(\frac{dv}{dx}\right)dx \\ &= \langle Tv, g(v)\rangle - 2\langle f, g(v)\rangle \end{aligned} \tag{5}$$

where

$$\begin{aligned} \langle Tu, g(v)\rangle &= \int_0^1 \left(\frac{d^2u}{dx^2}\right)\left(\frac{d^2v}{dx^2}\right)dx \\ \langle f, g(v)\rangle &= \int_0^1 f(x)\frac{dv}{dx}dx \end{aligned} \tag{6}$$

and $g = \dfrac{d}{dx}$ is the linear operator.

It is clear that the operator T defined by (6) is linear, g-symmetric, that is, $\langle Tu, g(v)\rangle = \langle Tv, g(u),\rangle \quad \forall u, v \in H$ and g-positive, that is, $\langle Tu, g(u) \geq 0, \quad \forall u \in H$. Using the technique of Noor [20], one can easily show that the minimum $u \in H$ of the functional $I[v]$ defined by (5) associated with the problem (4) on the closed convex set K can be characterized by the inequality of type

$$\langle Tu, g(v) - g(u)\rangle \geq \langle f, g(v) - g(u)\rangle, \quad \forall g(v) \in K,$$

which is exactly the general variational inequality (3). It is worth mentioning that a wide class of unrelated odd-order and nonsymmetric obstacle, unilateral, contact, free, moving, and equilibrium problems arising in regional, physical, mathematical, engineering and applied sciences can be studied in the unified and general framework of the general variational inequalities (1), see [2-5, 14-24,32-34] and the references therein.

Example 2.2. We now show that the minimum of a class of differentiable nonconvex functions on g-convex set K in H can be characterized by general variational inequality (3). For the sake of completeness and to convey an idea of the applications, we give all the details.

For this purpose, we recall the following well known concepts, see [8].

Definition 2.3. Let K be any set in H. The set K is said to be g-convex, if there exist a function $g : H \longrightarrow H$ such that

$$g(u) + t(g(v) - g(u)) \in K, \quad \forall u, v \in H : g(u), g(v) \in K, \quad t \in [0, 1].$$

Note that every convex set is g-convex, but the converse is not true, see [8]. We would like to mention that the g-convex set K was introduced by Noor [12] in 1998 implicitly. See also Youness [40] for other properties of the g-convex set.

Definition 2.4. The function $F : K \longrightarrow H$ is said to be g-convex, if there exists a function g such that

$$\begin{aligned} F(g(u) + t(g(v) - g(u))) \quad &\leq \quad (1-t)F(g(u)) + tF(g(v)), \\ &\forall u, v \in H : g(u), g(v) \in K, \quad t \in [0, 1]. \end{aligned}$$

Clearly every convex function is g-convex, but the converse is not true, see [8,40].

We now show that the minimum of a differentiable g-convex function on the g-convex set K in H can be characterized by the general variational inequality (1) and this is the main motivation of our next result, which is due to Noor [16].

Lemma 2.2[16]. Let $F : K \longrightarrow H$ be a differentiable g-convex function. Then $u \in H : g(u) \in K$ is the minimum of g-convex function F on K, if and only if, $u \in H : g(u) \in K$ satisfies the inequality

$$\langle F'(g(u)), g(v) - g(u) \rangle \geq 0, \quad \forall v \in H : g(v) \in K, \tag{7}$$

where $F'(u)$ is the differential of F at $g(u) \in K$.

Proof. Let $u \in H : g(u) \in K$ be a minimum of g-convex function F on K. Then

$$F(g(u)) \leq F(g(v)), \quad \forall v \in H : g(v) \in K. \tag{8}$$

Since K is a g-convex set, so, for all $u, v \in H : g(u), g(v) \in K, t \in [0, 1], g(v_t) = g(u) + t(g(v) - g(u)) \in K$. Setting $g(v) = g(v_t)$ in (8), we have

$$F(g(u)) \leq F(g(u) + t(g(v) - g(u))).$$

Dividing the above inequality by t and taking $t \longrightarrow 0$, we have

$$\langle F'(g(u)), g(v) - g(u) \rangle \geq 0, \quad \forall v \in H : g(v) \in K, \langle F'(g(u)), g(v) - g(u) \rangle \geq 0, \quad \forall v \in H : g(v) \in K,$$

which is the required result(7).

Conversely, let $u \in H : g(u) \in K$ satisfy the inequality (7). Since F is a g-convex function, $\forall u, v \in H : g(u), g(v) \in K, \quad t \in [0, 1], \quad g(u) + t(g(v) - g(u)) \in K$ and

$$F(g(u) + t(g(v) - g(u))) \leq (1-t)F(g(u)) + tF(g(v)),$$

which implies that

$$F(g(v)) - F(g(u)) \geq \frac{F(g(u) + t(g(v) - g(u))) - F(g(u))}{t}.$$

Letting $t \longrightarrow 0$, and using (7), we have

$$F(g(v)) - F(g(u)) \geq \langle F'(h(u)), g(v) - g(u) \rangle \geq 0,$$

which implies that

$$F(g(u)) \leq F(g(v)), \quad \forall v \in H : g(v) \in K$$

showing that $u \in H : g(u) \in K$ is the minimum of F on K in H. □

Lemma 2.2 implies that g-convex programming problem can be studied via the general variational inequality (1) with $Tu = F'(g(u))$. In a similar way, one can

show that the general variational inequality (1) is the Fritz-John condition of the inequality constrained optimization problem.

If $g \equiv I$, the identity operator, then problem (3) is equivalent to finding $u \in K$ such that

$$\langle Tu, v-u\rangle \geq 0, \quad v \in K, \tag{9}$$

which is known as the classical variational inequality, introduced and studied by Stampacchia [39] in 1964. It turned out that a number of unrelated obstacle, free, moving, unilateral and equilibrium problems arising in various branches of pure and applied sciences can be studied via variational inequalities, see [1-39] and the references therein.

It is well-known that problem (9) is equivalent to finding $u \in K$ such that

$$0 \in Tu + N_K(u), \tag{10}$$

where $N_K(u)$ denotes the normal cone of K at u in the sense of convex analysis. Problem (10) is called the variational inclusion associated with variational inequality (9).

Similarly, if K_r is a nonconvex (uniformly prox-regular) set, then problem (1) is equivalent to finding $u \in K_r$ such that

$$0 \in \rho Tu + g(u) - g(u) + \rho N_{K_r}^P(g(u)), \tag{11}$$

where $N_{K_r}^P(g(u))$ denotes the normal cone of K_r at $g(u)$ in the sense of nonconvex analysis. Problem (11) is called the nonconvex variational inclusion problem associated with nonconvex variational inequality (1). This implies that the variational inequality (1) is equivalent to finding a zero of the sum of two monotone operators (11). This equivalent formulation plays a crucial and basic part in this paper. We would like to point out this equivalent formulation allows us to use the projection operator technique for solving the general nonconvex variational inequality (1).

We now recall the well known proposition which summarizes some important properties of the uniform prox-regular sets.

Lemma 2.3. Let K be a nonempty closed subset of H, $\quad r \in (0, \infty]$ and set $K_r = \{u \in H : d(u, K) < r\}$. If K_r is uniformly prox-regular, then

i. $\forall u \in K_r, P_{K_r}(u) \neq \emptyset$.

ii. $\forall r^{'} \in (0, r)$, P_{K_r} is Lipschitz continuous with constant $\frac{r}{r-r'}$ on $K_{r'}$.

We now consider the problem of solving the nonlinear Wiener-Hopf equations. To be more precise, let $Q_{K_r} = I - P_{K_r}$, where P_{K_r} is the projection operator, and I is the identity operator. For given nonlinear operators T, g, consider the problem of finding $z \in H$ such that

$$Tg^{-1}P_{K_r}z + \rho^{-1}Q_{K_r}z = 0, \tag{12}$$

where g^{-1} is the inverse of the operator g. Equations of the type (12) are called the general nonconvex Wiener-Hopf equations. Note that, if $r = \infty$, Then the nonlinear Wiener-Hopf equations are exactly the same Wiener-Hopf equations associated with the general variational inequalities (3), which were introduced and studied by Noor [14]. For $g \equiv I$, the identity operator and $r = \infty$, one can obtain the original Wiener-Hopf equations which were introduced and studied by Shi [38] in conjunction with the variational inequalities. This shows that the original Wiener-Hopf equations are the special case of the general nonconvex Wiener-Hopf

equations (12). The Wiener-Hopf equations technique has been used to study and develop several iterative methods for solving variational inequalities and related optimization problems, see [14-33].

Definition 2.6. An operator $T : H \to H$ is said to be:

(i) *strongly monotone*, if and only if, there exists a constant $\alpha > 0$ such that

$$\langle Tu - Tv, u - v\rangle \geq \alpha||u - v||^2, \quad \forall u, v \in H.$$

(ii) *Lipschitz continuous*, if and only if, there exists a constant $\beta > 0$ such that

$$||Tu - Tv|| \leq \beta||u - v||, \quad \forall u, v \in H.$$

3. Projection Iterative Algorithms

In this section, we establish the equivalence between the general nonconvex variational inequality (1) and the fixed point problem using the projection operator technique. This alternative formulation is used to discuss the existence of a solution of the problem (1) and to suggest some new iterative methods for solving the general nonconvex variational inequality (1).

Lemma 3.1. $u \in H : g(u) \in K_r$ is a solution of the general nonconvex variational inequality (1) if and only if $u \in H : g(u) \in K_r$ satisfies the relation

$$g(u) = P_{K_r}[g(u) - \rho Tu], \tag{13}$$

where P_{K_r} is the projection of H onto the uniformly prox-regular set K_r.

Proof. Let $u \in H : g(u) \in K_r$ be a solution of (1). Then, for a constant $\rho > 0$,

$$\begin{aligned} 0 &\in g(u) + \rho N^P_{K_r}(g(u)) - (g(u) - \rho Tu) = (I + \rho N^P_{K_r})(g(u)) - (g(u) - \rho Tu) \\ &\iff \\ g(u) &= (I + \rho N^P_{K_r})^{-1}[g(u) - \rho Tu] = P_{K_r}[g(u) - \rho Tu], \end{aligned}$$

where we have used the well-known fact that $P_{K_r} \equiv (I + N^P_{K_r})^{-1}$. □

Lemma 3.1 implies that the general nonconvex variational inequality (1) is equivalent to the fixed point problem (13). This alternative equivalent formulation is very useful from the numerical and theoretical point of views.

We rewrite the the relation (13) in the following form

$$F(u) = u - g(u) + P_{K_r}[g(u) - \rho Tu], \tag{14}$$

which is used to study the existence of a solution of the general nonconvex variational inequality (1).

We now study those conditions under which the general nonconvex variational inequality (1) has a solution and this is the main motivation of our next result.

Theorem 3.1. Let P_{K_r} be the Lipschitz continuous operator with constant $\delta = \frac{r}{r-r'}$. Let T, g be strongly monotone with constants $\alpha > 0, \sigma > 0$ and Lipschitz continuous with constants $\beta > 0, \delta > 0$, respectively. If there exists a constant $\rho > 0$ such that

$$|\rho - \frac{\alpha}{\beta^2}| < \frac{\sqrt{\delta^2\alpha^2 - \beta^2(1 - (1+\delta)k))^2)}}{\delta\beta^2}, \tag{15}$$

$$\delta\alpha > \beta\sqrt{k(1+\delta)(2 - k(1+\delta))}, \quad k < \frac{2}{1+\delta}, \tag{16}$$

where

$$k = \sqrt{1 - 2\sigma + \delta^2}, \tag{17}$$

then there exists a solution of the general nonconvex variational inequality (1).

Proof. From Lemma 3.1, it follows that problems (13) and (1) are equivalent. Thus it is enough to show that the map $F(u)$, defined by (14), has a fixed point. For all $u \neq v \in K_r$, we have

$$\begin{aligned} \|F(u) - F(v)\| &= \|u - v - (g(u) - g(v))\| + \|P_{K_r}[g(u) - \rho Tu] - P_{K_r}[v - \rho Tv]\| \\ &\leq \|u - v - (g(u) - g(v))\| + \delta\|g(u) - g(v) - \rho(Tu - Tv)\|, \\ &\leq \|u - v - (g(u) - g(v))\| + \delta\|u - v - \rho(Tu - Tv)\| \\ &\quad +\delta\|u - v - (g(u) - g(v))\|, \end{aligned} \tag{18}$$

where we have used the fact that the operator P_{K_r} is a Lipschitz continuous operator with constant δ.

Since the operator T is strongly monotone with constant $\alpha > 0$ and Lipschitz continuous with constant $\beta > 0$, it follows that

$$\begin{aligned} \|u - v - \rho(Tu - Tv)\|^2 &\leq \|u - v\|^2 - 2\rho\langle Tu - Tv, u - v\rangle + \rho^2\|Tu - Tv\|^2 \\ &\leq (1 - 2\rho\alpha + \rho^2\beta^2)\|u - v\|^2. \end{aligned} \tag{19}$$

In a similar way, we have

$$\|u - v - (g(u) - g(v))\| \leq \sqrt{1 - 2\sigma + \delta^2}\|u - v| = k\|u - v\|, \tag{20}$$

where $\sigma > 0$ is the strongly monotonicity constant and $\delta > 0$ is the Lipschitz continuity constant of the operator g respectively.

From (18), (19) and (20), we have

$$\begin{aligned} \|F(u) - F(v)\| &\leq \left\{k + \delta\left\{k + \sqrt{1 - 2\alpha\rho + \beta^2\rho^2)}\right\}\|u - v\|\right\| \\ &= \theta\|u - v\|, \end{aligned}$$

where

$$\theta = k + \delta\left\{\sqrt{1 - 2\alpha\rho + \beta^2\rho^2}\right\}. \tag{21}$$

From (15) and (16), it follows that $\theta < 1$, which implies that the map $F(u)$ defined by (14), has a fixed point, which is a unique solution of (1). □

This fixed point formulation (13) is used to suggest the following iterative method for solving the nonconvex variational inequality (1).

Algorithm 3.1. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative scheme

$$\begin{aligned} u_{n+1} &= (1 - \alpha_n)u_n - \alpha_n\{u_n - g(u_n) \\ &\quad +P_{K_r}[g(u_n) - \rho Tu_n]\}, \quad n = 0, 1, 2, \ldots, \end{aligned} \tag{22}$$

where $\alpha_n \in [0, 1], \forall n \geq 0$ is a constant. Algorithm 3.1 is also called the Mann iteration process.

For $\alpha_n = 1$, Algorithm 3.1 collapse to:

Algorithm 3.2. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative scheme

$$g(u_{n+1}) = P_{K_r}[g(u_n) - \rho Tu_n], \quad n = 0, 1, 2, \ldots$$

We again use the fixed formulation to suggest and analyze an iterative method for solving the nonconvex variational inequalities (1) as:

Algorithm 3.3. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative scheme

$$g(u_{n+1}) = P_{K_r}[g(u_{n+1}) - \rho T u_{n+1}], \quad n = 0, 1, 2, \ldots$$

Algorithm 3.3 is an implicit type iterative method, which is difficult to implement. To implement Algorithm 3.3, we use the predictor-corrector technique. Here we use the Algorithm 3.1 as a predictor and Algorithm 3.3 as a corrector. Consequently, we have the following iterative method

Algorithm 3.4. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative schemes

$$\begin{aligned} g(y_n) &= P_{K_r}[g(u_n) - \rho T u_n] \\ g(u_{n+1}) &= P_{K_r}[g(y_n) - \rho T y_n], \quad n = 0, 1, 2, \ldots \end{aligned}$$

which is called the two-step or splitting type iterative method for solving the general nonconvex variational inequalities (1). It is worth mentioning that Algorithm 3.4 can be suggested by using the updating the technique of the solution.

In this paper, we suggest and analyze the following two-step iterative method for solving the general nonconvex variational inequalities (1).

Algorithm 3.5. For a given $u_0 \in K_r$, find the approximate solution u_{n+1} by the iterative schemes

$$\begin{aligned} y_n &= (1-\beta_n)u_n + \beta_n\{y_n - g(y_n) + P_{K_r}[g(u_n) - \rho T u_n]\} \\ u_{n+1} &= (1-\alpha_n)u_n + \alpha_n\{u_n - g(u_n) + P_{K_r}[g(y_n) - \rho T y_n]\}, \quad n = 0, 1, 2, \ldots, \end{aligned}$$

where $\alpha_n, \beta_n \in [0, 1], \quad \forall n \geq 0$.

Clearly for $\alpha_n = \beta_n = 1$, Algorithm 3.5 reduces to Algorithm 3.4. It is worth mentioning that, if $r = \infty$, then the nonconvex set K_r reduces to a convex set K. Consequently Algorithms 3.1- 3.5 collapse to the following algorithms for solving the general variational inequalities (6). We would like to point that Algorithm 3.4 appears to be a new one for solving the variational inequalities (2)

We now consider the convergence analysis of Algorithm 3.1 and this is the main motivation of our next result. In a similar way, one can consider the convergence criteria of other Algorithms.

Theorem 3.2. Let P_{K_r} be the Lipschitz continuous operator with constant $\delta = \frac{r}{r-r'}$. Let the operators $T, g : H \longrightarrow H$ be strongly monotone with constants $\alpha > 0, \sigma > 0$ and Lipschitz continuous with constants with $\beta > 0, \delta > 0$, respectively. If (15), (16) hold and $\alpha_n, \in [0, 1], \quad \forall n \geq 0$ and $\sum_{n=0}^{\infty} \alpha_n = \infty$, then the approximate solution u_n obtained from Algorithm 3.1 converges to a solution $u \in K_r$ satisfying the nonconvex variational inequality (1).

Proof. Let $u \in H : g(u) \in K_r$ be a solution of the general nonconvex variational inequality (2.1). Then, using Lemma 3.1, we have

$$u = (1-\alpha_n)u + \alpha_n\{u - g(u) + P_{K_r}[g(u) - \rho T u]\}, \tag{23}$$

where $0 \leq \alpha_n \leq 1$ is a constant.

From (19), (20), (17), (22), (23) and using the Lipschitz continuity of the projection P_{K_r} with constant δ, we have

$$\begin{aligned}
\|u_{n+1}-u\| &= \|(1-\alpha_n)(u_n-u)+\alpha_n\{P_{K_r}[g(u_n)-\rho Tu_n]-P_{K_r}[g(u)-\rho Tu]\}\| \\
&\quad +\alpha_n\|u_n-u-(g(u_n)-g(u)\| \\
&\leq (1-\alpha_n)\|u_n-u\|+\alpha_n\|P_{K_r}[g(u_n)-\rho Tu_n]-P_{K_r}[g(u)-\rho Tu]\|+\alpha_n k\|u_n-u\| \\
&\leq (1-\alpha_n)\|u_n-u\|+\alpha_n\delta\|g(u_n)-g(u)+\rho(Tu_n-Tu)\|+\alpha_n k\|u_n-u\| \\
&\leq (1-\alpha_n)\|u_n-u\|+\alpha_n k\|u_n-u\| \\
&\quad \delta\|u_n-u-(g(u_n)-g(u))\|+\delta\|u_n-u-\rho(Tu_n-Tu)\| \\
&\leq (1-\alpha_n)\|u_n-u\|+\alpha_n\left\{k+\delta\left[k+\sqrt{1-2\alpha\rho+\beta^2\rho^2}\right]\right\}\|u_n-u\| \\
&= [1-\alpha_n(1-\theta)]\,\|u_n-u\| \\
&\leq \prod_{i=0}^{n}[1-\alpha_i(1-\theta)]\,\|u_0-u\|,
\end{aligned}$$

where, using (15), we have

$$\theta = k+\delta\sqrt{1-2\rho\alpha+\beta^2\rho^2}<1.$$

Since $\sum_{n=0}^{\infty}\alpha_n$ diverges and $1-\theta>0$, we have $\lim_{n\to\infty}\{\prod_{i=0}^{n}[1-(1-\theta)\alpha_i]\}=0$. Consequently the sequence $\{u_n\}$ convergences strongly to u. This completes the proof. □

4. Wiener-Hopf Equations Technique

In this section, we first establish the equivalence between the general nonconvex variational inequality (1) and the Wiener-Hopf equations (12) using essentially the projection method. This equivalence is used to suggest and analyze some iterative methods for solving the general nonconvex variational inequality (1).

Using Lemma 3.1, we show that the general nonconvex variational inequality (1) is equivalent to the Wiener-Hopf equations (12).

Lemma 4.1. The general nonconvex variational inequality (1) has a solution $u\in H: g(u)\in K_r$ if and only if the Wiener-Hopf equations (12) have a solution $z\in H$, provided

$$g(u) = P_{K_r}z \tag{24}$$

$$z = g(u)-\rho Tu, \tag{25}$$

where $\rho>0$ is a constant.

Proof. Let $u\in H: g(u)\in K_r$ be a solution of (1). Then, from Lemma 3.1, we have

$$g(u) = P_{K_r}[g(u)-\rho Tu]. \tag{26}$$

Taking $z=g(u)-\rho Tu$ in (26), we have

$$g(u) = P_{K_r}z. \tag{27}$$

From (26) and (27), we have

$$z = g(u)-\rho Tu = P_{K_r}z-\rho Tg^{-1}P_{K_r}z,$$

which shows that $z \in H$ is a solution of the Wiener-Hopf equations (12). This completes the proof. □

From Lemma 4.1, we conclude that the general nonconvex variational inequality (1) and the Wiener-Hopf equations (12) are equivalent. This alternative formulation plays an important and crucial part in suggesting and analyzing various iterative methods for solving variational inequalities and related optimization problems. In this paper, by suitable and appropriate rearrangement, we suggest a number of new iterative methods for solving the general nonconvex variational inequality (1).

I. The Wiener-Hopf equations (12) can be written as

$$P_{K_r}z = -\rho T g^{-1} P_{K_r}z,$$

which implies that, using(4.2)

$$z = P_{K_r}z - \rho T g^{-1} P_{K_r}z = g(u) - \rho T u.$$

This fixed point formulation enables us to suggest the following iterative method for solving the general nonconvex variational inequality (1).

Algorithm 4.1. For a given $z_0 \in H$, compute z_{n+1} by the iterative schemes

$$g(u_n) = P_{K_r}z_n \tag{28}$$

$$z_{n+1} = (1-\alpha_n)z_n + \alpha_n\{g(u_n) - \rho T u_n,\} \quad n = 0, 1, 2, \ldots, \tag{29}$$

where $0 \leq \alpha_n \leq 1$, for all $n \geq 0$ and $\sum_{n=0}^{\infty} \alpha_n = \infty$.

II. The Wiener-Hopf equations (12) may be written as

$$\begin{aligned} z &= P_{K_r}z - \rho T g^{-1} P_{K_r}z + (1-\rho^{-1})Q_{K_r}z \\ &= g(u) - \rho T u + (1-\rho^{-1})Q_{K_r}z. \end{aligned}$$

Using this fixed point formulation, we suggest the following iterative method.

Algorithm 4.2. For a given $z_0 \in H$, compute z_{n+1} by the iterative schemes

$$\begin{aligned} g(u_n) &= P_{K_r}z_n \\ z_{n+1} &= (1-\alpha_n)z_n + \alpha_n\{g(u_n) - \rho T u_n + (1-\rho^{-1})Q_{K_r}z_n,\} \quad n = 0, 1, 2, \ldots, \end{aligned}$$

where $0 \leq \alpha_n \leq 1$, for all $n \geq 0$ and $\sum_{n=0}^{\infty} \alpha_n = \infty$.

III. If the operator T is linear and T^{-1} exists, then the Wiener-Hopf equation (12) can be written as

$$z = (I - \rho^{-1}T^{-1})Q_{K_r}z,$$

which allows us to suggest the iterative method.

Algorithm 4.3. For a given $z_0 \in H$, compute z_{n+1} by the iterative scheme

$$z_{n+1} = (1-\alpha_n)z_n + \alpha_n\{(I - \rho^{-1}T^{-1})Q_{K_r}z_n,\} \quad n = 0, 1, 2 \ldots,$$

where $0 \leq \alpha_n \leq 1$, for all $n \geq 0$ and $\sum_{n=0}^{\infty} \alpha_n = \infty$.

We would like to point out that one can obtain a number of iterative methods for solving the general nonconvex variational inequality (1) for suitable and appropriate choices of the operators T, h and the space H. This shows that iterative methods suggested in this paper are more general and unifying ones.

We now study the convergence analysis of Algorithm 4.1. In a similar way, one can analyze the convergence analysis of other iterative methods.

Theorem 4.1. Let the operators T, A satisfy all the assumptions of Theorem 3.1. If the condition (15) holds and $\alpha_n \in [0, 1], \quad \forall n \geq 0$, and $\sum_{n=0}^{\infty} \alpha_n = \infty$, then

the approximate solution $\{z_n\}$ obtained from Algorithm 4.1 converges to a solution $z \in H$ satisfying the Wiener-Hopf equation (12) strongly.

Proof. Let $u \in H$ be a solution of (1). Then, using Lemma 4.1, we have

$$z = (1-\alpha_n)z + \alpha_n\{g(u) - \rho Tu\}, \tag{30}$$

where $0 \leq \alpha_n \leq 1$, and $\sum_{n=0}^{\infty} a_n = \infty$.

From(29), (30), (19) and (20), we have

$$\begin{aligned} \|z_{n+1} - z\| &\leq (1-\alpha_n)\|z_n - z\| + \alpha_n\|g(u_n) - g(u) - \rho(Tu_n - Tu)\| \\ &\leq (1-\alpha_n)\|z_n - z\| + \alpha_n\{\|u_n - u - (g(u_n) - g(u))\| + \|u_n - u - \rho(Tu_n - Tu)\|\} \\ &\leq (1-\alpha_n)\|z_n - z\| + \alpha_n\left\{k + \sqrt{1 - 2\rho\alpha + \beta^2\rho^2}\right\}\|u_n - u\|. \end{aligned} \tag{31}$$

Also from (28), (24) and the Lipschitz continuity of the projection operator P_{K_r} with constant δ, we have

$$\begin{aligned} \|u_n - u\| &= \|u_n - u - (g(u_n) - g(u))\| + \|P_{K_r}z_n - P_{K_r}z\| \\ &= k\|u_n - u\| + \delta\|z_n - z\| \end{aligned}$$

from which, we have

$$\|u_n - u\| \leq \frac{\delta}{1-k}\|z_n - z\|. \tag{32}$$

Combining (31), and (32), we have

$$\begin{aligned} \|z_{n+1} - z\| &\leq (1-\alpha_n)\|z_n - z\| + \alpha_n\delta\frac{k + \sqrt{1 - 2\rho\alpha + \beta^2\rho^2}}{1-k}\|z_n - z\| \\ &= (1-\alpha_n)\|z_n - z\| + \alpha_n\theta_1\|z_n - z\|, \end{aligned} \tag{33}$$

where

$$\theta_1 = \delta\frac{k + \sqrt{1 - 2\rho\alpha + \rho^2\beta^2}}{1-k}$$

From (15) and (16), we see that $\theta_1 < 1$ and consequently

$$\begin{aligned} ||z_{n+1} - z|| &\leq (1-\alpha_n)||z_n - z|| + \alpha_n\theta_1||z_n - z|| \\ &= [1 - (1-\theta_1)\alpha_n]||z_n - z|| \\ &\leq \prod_{i=0}^{n}[1 - (1-\theta_1)\alpha_i]||z_0 - z||. \end{aligned}$$

Since $\sum_{n=0}^{\infty}\alpha_n$ diverges and $1 - \theta_1 > 0$, we have $\lim_{n\to\infty}\prod_{i=0}^{n}[1 - (1-\theta_1)\alpha_i] = 0$. Consequently the sequence $\{z_n\}$ convergences strongly to z in H, the required result. □

Acknowledgement. The author would like to express his gratitude to Dr. M. Junaid Zaidi, Rector, CIIT, for providing excellent research facilities. The authhor would like to thank Prof. Dr. Enkelejd Hashorva for the kind invitation.

References

[1] H. Brezis, Operateurs maximaux monotone, Mathematical Studies, No. 5, North-Holland, 1973.

[2] A. Bnouhachem and M. Aslam Noor, Numerical methods for general mixed variational inequalities, Appl. Math. Comput. **204**(2008), 27-36.

[3] A. Bnouhachem, M. Aslam Noor and M. Khalfaoui, Modified descent-projection method for solving variational inequalities, Appl. Math. Comput. **190**(2008), 1691-1700.

[4] A. Bnouhachem and M. Aslam Noor, Numerical comparison between prediction-correction methods for general variational inequalities, Appl. Math. Comput. **186**(2007), 496-505.

[5] A. Bnouhachem and M. Aslam Noor, Inexact proximal point method for general variational inequalities, J. Math. Anal. Appl. **324**(2006), 1195-1212.

[6] M. Bounkhel, L. Tadj and A. Hamdi, Iterative schemes to solve nonconvex variational problems, J. Inequal. Pure Appl. Math.,**4**(2003), 1-14.

[7] F. H. Clarke, Y. S. Ledyaev and P. R. Wolenski, Nonsmooth Analysis and Control Theory, Springer-Verlag, Berlin, 1998.

[8] G. Cristescu and L. Lupsa, Non-connected Convexities and Applications, Kluwer Academic Publishers, Dordrecht, Holland, 2002.

[9] D. Kinderlehrer and G. Stampacchia, An Introduction to Variational Inequalities and Their Applications, SIAM, Philadelphia, 2000.

[10] J. L. Lions and G. Stampacchia, Variational inequalities, Comm. Pure Appl. Math. **20**(1967), 493-512.

[11] P. L. Lions and B. Mercier, Splitting algorithms for the sum of two nonlinear operators, SIAM J. Numer. Anal. **16**(1979), 964-979.

[12] M. Aslam Noor, General variational inequalities, Appl. Math. Letters, **1**(1988), 119-121.

[13] M. Aslam Noor, Quasi variational inequalities, Appl. Math. Letters, **1**(1988), 367-370.

[14] M. Aslam Noor, Wiener-Hopf equations and variational inequalities, J. Optim. Theory Appl. **79**(1993), 197-206.

[15] M. Aslam Noor, Some recent advances in variational inequalities, Part II, other concepts, New Zealand J. Math. **26**(1997), 229-255.

[16] M. Aslam Noor, New approximation schemes for general variational inequalities, J. Math. Anal. Appl. , **251**(2000), 217-229.

[17] M. Aslam Noor, A Wiener-Hopf dynamical system for variational inequalities, New Zealand J. Math. **31**(2002), 173-182.

[18] M. Aslam Noor, New extragradient-type methods for general variational inequalities. J. Math. Anal. Appl. **277**(2003), 379-395.

[19] M. Aslam Noor, Mixed quasi variational inequalities, Appl. Math. Computation, **146**(2003), 553-578.

[20] M. Aslam Noor, Some developments in general variational inequalities, Appl. Math. Computation, **152**(2004), 199-277.

[21] M. Aslam Noor, Iterative schemes for nonconvex variational inequalities, J. Optim. Theory Appl. **121**(2004), 385-395.

[22] M. Aslam Noor, Fundamentals of mixed quasi variational inequalities, Inter. J. Pure Appl. Math. **15**(2004), 137-258.

[23] M. Aslam Noor, Fundamentals of equilibrium problems, Math. Inequal. Appl. **9**(2006), 529-566.

[24] M. Aslam Noor, Merit functions for general variational inequalities, J. Math. Anal. Appl. **316**(2006), 736-752.

[25] M. Aslam Noor, Differentiable nonconvex functions and general variational inequalities, Appl. Math. Computation, **199** (2008), 623-630

[26] M. Aslam Noor, Some iterative methods for general nonconvex variational inequalities, Comput. Math. Modeling, **21**(2010).

[27] M. Aslam Noor, Projection methods for nonconvex variational inequalities, Optim. Letters(2009), DOI: 10.1007/s11590-009-0121.1.

[28] M. Aslam Noor, Implicit iterative methods for nonconvex variational inequalities, J. Optim. Theory Appl. **143**(2009).

[29] M. Aslam Noor, Iterative methods for general nonconvex variational inequalities, Albanian J. math. **3**(2009).
[30] M. Aslam Noor, Variational Inequalities and Applications, Lecture Notes, Mathematics Department, COMSATS Institute of Information Technology, Islamabad, Pakistan, 2007-2009.
[31] M. Aslam Noor and K. Inayat Noor, Projection algorithms for solving system of general variational inequalities, Nonl. Anal. **70**(2009), 2700-2706.
[32] M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Some aspects of variational inequalities, J. Comput. Appl. Math. **47**(1993), 285-312.
[33] M. Aslam Noor, K. Inayat Noor and H. Yaqoob, On general mixed variational inequalities, Acta Appl. Math. (2008), DOI 10.1007/s10440-008-9402.4
[34] M. Aslam Noor and Th. M. Rassias, On nonconvex equilibrium problems, J. Math. Anal. Appl. **312**(2005), 289-299.
[35] L. P. Pang, J. Shen and H. S. Song, A modified predictor-corrector algorithm for solving nonconvex generalized variational inequalities, Computers Math. Appl. **54**(2007), 319-325.
[36] M. Patriksson, Nonlinear Programming and Variational Inequality Problems: A Unified Approach, Kluwer Academic Publishers, Dordrecht, 1998.
[37] R. A. Poliquin, R. T. Rockafellar and L. Thibault, Local differentiability of distance functions, Trans. Amer. Math. Soc., **352**(2000), 5231-5249.
[38] P. Shi, Equivalence of variational inequalities with Wiener-Hopf equations, Proc. Amer. Math. Soc., **111**(1991), 339-346.
[39] G. Stampacchia, Formes bilineaires coercitives sur les ensembles convexes, C. R. Acad. Sci, Paris, **258**(1964), 4413-4416
[40] E. A. Youness, E-convex sets, E-convex functions and E-convex programming, J. Optim. Theory Appl. **102**(1999),439-450.

COMSATS Institute of Information Technology, Mathematics Department, Islamabad, Pakistan
E-mail address: noormaslam@gmail.com and noormaslam@hotmail.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 4, Pages 189–197
ISSN 1930-1235: (2009)

ON INTEGERS WITH TWO PRIME FACTORS

BENJAMIN JUSTUS

Abstract. Integers with two prime factors occur in the RSA cryptosystem. In this paper, we provide density estimates for such integers occuring in the RSA cryptosystem satisfying various conditions. Cryptographic applications are given as a consequence of the estimates obtained.

1. Introduction

The implementation of the RSA cryptosystem requires the selection of an integer n of the form $n = p \cdot q$ where the distinct prime factors p, q satisfy certain conditions. Such an integer in the literature is often referred as a RSA integer. We follow this convention in the paper. For certain cryptographic applications, it is important to know

- What is the probability that a randomly selected integer is a RSA integer?

In order to answer the question above adequately, one has to know a priori the specific conditions that are imposed on the prime factors p, q of n. A survey of literature shows that no precise and consistent definitions exist. The specific requirements for the the prime factors p, q of n differ among authors. The inventors of the RSA cryptosystem [1, 2] wrote that the primes factors p, q need to be large and be randomly selected. In [9], it is required to select p, q of approximately equal magnitude. In more applied works [3, 10], the authors require p, q to be of equal bit-length.

If one assumes the fact that a randomly selected integer in the interval $[1, x]$ has the probability $\log^{-1} x$ (a consequence of the prime number theorem) of being a prime and furthermore that the events of selecting prime numbers are independent, then one may guess that the answer to the above question is of the order $\log^{-2} x$. This intuition turns out to be true (see Theorem 2.1 and Theorem 3.1) only if one is willing to impose conditions on the prime factors p, q of n. The specific conditions imposed have to do with how close the prime factors p, q are with respect to each other and the tightness of the interval in which p, q are bounded.

Indeed, our original intention of writing the paper is to investigate the question how the density of RSA integers is related the conditions that are imposed upon the prime factors p, q of n. It turns out that in order to obtain the density estimate in the order of $\log^{-2} x$, it is necessary to impose those conditions on the prime factors p, q as described in section 2 and section 3. An early theorem of Landau [6] shows that, the number of integers $n \leq x$ of the form $n = p \cdot q$ with distinct p and q satisfies as x goes to infinity

Received by the editors September 1, 2009.
Key words and phrases. RSA cryptosystem, RSA integer, density estimate.

$$\pi_2(x) \sim \frac{x \log\log x}{\log x}.$$

In particular this result implies that the probability of a randomly selected integer n in the interval $[1, x]$ being of the form $n = p \cdot q$ (no conditions imposed on p, q) is of the order $\frac{\log\log x}{\log x}$.

The organization of the paper is as follows. In section 2 and section 3, we formulate two analytic notions of RSA integers which allow us to quantify: how close the prime factors of a RSA integer are with respect to each other and what we mean by selecting p, q of the same bit-length. We then count respectively the RSA integers satisfying each of the notions. In section 4, we give applications and thereby answer the question that is set out in the introduction.

For the benefit of the readers, we have included appendices at the end of the paper. The appendices contain some well known results from analytic number theory which are used in the paper.

2. First Notion

The first notion reflects the idea that a RSA integer $n = p \cdot q$ should have its prime factors p, q close to each other. Thus we say,

Definition 1. A RSA integer $n = p \cdot q$ in the interval $[1, x]$ is called θ-spaced if it satisfies the property: if $p < q$, then $p < q \leq x^\theta p$.

In order to provide the density estimate, we need to count θ-spaced RSA integers. Let us consider the following set

$$\mathcal{S}(x; \theta, c) := \{n = p \cdot q \leq x : \quad p < q \leq x^\theta p,\, p \leq x^c\}.$$

Note: since p is the smaller of the two prime factor we can always take $c \leq \frac{1}{2}$. The main result of the section is

Theorem 2.1. *Let $0 < \theta < 1$ and $0 < c \leq \frac{1}{2}$ be fixed. Then the following estimates for the cardinality of $\mathcal{S}(x; \theta, c)$ hold:*

$$|\mathcal{S}(x; \theta, c)| = \begin{cases} \frac{1}{2c(\theta+c)} \frac{x^{2c+\theta}}{\log^2 x} + \mathrm{O}\left(\frac{x^{2c+\theta}}{\log^3 x}\right), & c \leq \frac{1-\theta}{2}; \\ B \frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x}\right), & \frac{1-\theta}{2} < c \leq \frac{1}{2}. \end{cases}$$

where $B = B(\theta, c)$ is an explicitly computable nonzero constant that depends only on θ and c.

The above theorem shows that how the density of RSA integers changes according to the set parameters θ, c. It should be noticed, in particular, in order to achieve the density in the order of $\log^{-2} x$, the prime factors p, q need to be close (small θ) to each other.

Proof. We deal with the case $c \leq \frac{1-\theta}{2}$ first. Notice $x^\theta p \leq \frac{x}{p}$ if and only if $p \leq x^{\frac{1-\theta}{2}}$. We have

$$|\mathcal{S}(x; \theta, c)| = \sum_{\substack{p \\ p \leq x^c}} \sum_{\substack{q \\ p < q \leq x^\theta p}} 1.$$

The inner sum is treated by the prime number theorem (see Appendix A). Thus

$$|\mathcal{S}(x;\theta,c)| = x^\theta \sum_{\substack{p\\ p\le x^c}} \frac{p}{\log x^\theta p} + \mathrm{O}\left(x^\theta \sum_{\substack{p\\ p\le x^c}} \frac{p}{\log^2 x^\theta p}\right)$$

Partial summation gives (see Appendix B):

$$\begin{aligned} &= \frac{1}{2c(\theta+c)}\frac{x^{2c+\theta}}{\log^2 x} + \mathrm{O}\left(\frac{x^{2c+\theta}}{\log^3 x}\right) + \mathrm{O}\left(\frac{x^\theta}{\log^2 x}\sum_{\substack{p\\ p\le x^c}} p\right)\\ &= \frac{1}{2c(\theta+c)}\frac{x^{2c+\theta}}{\log^2 x} + \mathrm{O}\left(\frac{x^{2c+\theta}}{\log^3 x}\right). \end{aligned}$$

This settles the first case. In the second case $\frac{1-\theta}{2} < c \le \frac{1}{2}$, we have

$$|\mathcal{S}(x;\theta,c)| = \sum_{\substack{p\\ p\le x^{\frac{1-\theta}{2}}}} \sum_{\substack{q\\ p<q\le x^\theta p}} + \sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} \sum_{\substack{q\\ p<q\le \frac{x}{p}}} 1. \tag{2.1}$$

We can bound the first double sum as follows

$$\sum_{\substack{p\\ p\le x^{\frac{1-\theta}{2}}}} \sum_{\substack{q\\ p<q\le x^\theta p}} 1 \ll \sum_{\substack{p\\ p\le x^{\frac{1-\theta}{2}}}} \pi(x^\theta p) \ll x^\theta \sum_{\substack{p\\ p\le x^{\frac{1-\theta}{2}}}} \frac{p}{\log x^\theta p} \ll \frac{x}{\log^2 x}.$$

The second double sum in (2.1) is the main term. We have

$$\begin{aligned} &\sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} \sum_{\substack{q\\ p<q\le \frac{x}{p}}} 1\\ =&\sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} (\pi(x/p)-\pi(p))\\ =&x\sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} \frac{1}{p\log x/p} - \sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} \frac{p}{\log p} + \mathrm{O}\left(x\sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} \frac{1}{p\log^2 x/p}\right). \end{aligned}$$

We have $\sum \frac{p}{\log p} = \mathrm{O}(x\log^{-2} x)$ (Example 2, Appendix B) and the term

$$x\sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} \frac{1}{p\log^2 x/p} \ll \frac{x}{\log^2 x}\sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} \frac{1}{p} \ll \frac{x}{\log^2 x}.$$

Thus, (2.1) becomes

$$|\mathcal{S}(x;\theta,c)| = x\sum_{\substack{p\\ x^{\frac{1-\theta}{2}}<p\le x^c}} \frac{1}{p\log x/p} + \mathrm{O}\left(\frac{x}{\log^2 x}\right). \tag{2.2}$$

We are done for the proof except for the evaluation of the sum $\sum \frac{1}{p \log x/p}$. The evaluation of the sum is technical in nature and the proof of which is given at the end this section. Let us for the moment assume the result: for any $0 < \theta < 1$,

$$\sum_{p \leq x^\theta} \frac{1}{p \log x/p} = \frac{\log \log x}{\log x} + \frac{f(\theta)}{\log x} + \mathrm{O}\left(\frac{1}{\log^2 x}\right)$$

where $f(\theta)$ is a strictly increasing function in θ. Using this result, (2.2) becomes

$$|\mathcal{S}(x; \theta, c)| = B(\theta, c)\frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x}\right).$$

The constant $B(\theta, c)$ is positive and nonzero. The theorem is proved. □

Proposition 2.1. *Let $0 < \theta < 1$. Then the following estimate holds:*

$$\sum_{p \leq x^\theta} \frac{1}{p \log x/p} = \frac{\log \log x}{\log x} + \left(\log \frac{\theta}{1-\theta} + c_1\right)\frac{1}{\log x} + \mathrm{O}\left(\frac{1}{\log^2 x}\right)$$

where c_1 is an absolute constant.

Proof. We have

$$\begin{aligned}
&\sum_{p \leq x^\theta} \frac{1}{p \log x/p} = \sum_{p \leq x^\theta} \frac{1}{p \log x(1 - \frac{\log p}{\log x})} \\
=&\frac{1}{\log x} \sum_{p \leq x^\theta} \frac{1}{p} + \sum_{m \geq 1} \frac{1}{\log^{m+1} x} \sum_{p \leq x^\theta} \frac{\log^m p}{p} \\
=&\sum_{m \geq 1} \frac{1}{\log^{m+1} x} \sum_{p \leq x^\theta} \frac{\log^m p}{p} + \frac{\log \log x + c_1 + \log \theta}{\log x} + \mathrm{O}\left(\frac{1}{\log^2 x}\right). \qquad (2.3)
\end{aligned}$$

The inner sum over p can be dealt with using the following lemma:

Lemma 2.1. *For a positive integer $m \geq 1$,*

$$\sum_{p \leq z} \frac{\log^m p}{p} = \frac{\log^m z}{m} + \mathrm{O}(\log^{m-1} z).$$

Proof. The case $m = 1$ is a standard result. For example, the reader may see [7] for a proof. When $m \geq 2$, one has by partial summation

$$\begin{aligned}
&\sum_{p \leq z} \frac{\log^m p}{p} \\
=&\left(\sum_{p \leq z} \frac{1}{p}\right) \log^m z - \int_2^z \left(\sum_{p \leq z} \frac{1}{p}\right) d \log^m t \\
=&(\log \log z + c_1) \log^m z - \int_2^z \log \log t (d \log^m t) - c_1 \int_2^z d \log^m t + \mathrm{O}(\log^{m-1} z) \\
=&(\log \log z) \log^m z - \int_2^z \log \log t (d \log^m t) + \mathrm{O}(\log^{m-1} z)
\end{aligned}$$

Performing intergeration by parts to the integeral gives

$$=\frac{\log^m z}{m}+\mathrm{O}(\log^{m-1} z).$$

This proves the lemma. □

Thus in view of the lemma, (2.3) becomes

$$\begin{aligned}
&\sum_{p\le x^\theta}\frac{1}{p\log x/p}\\
=&\frac{1}{\log x}\sum_{m\ge1}\frac{\theta^m}{m}+\frac{\log\log x+c_1+\log\theta}{\log x}+\mathrm{O}\left(\frac{1}{\log^2 x}\sum_{m\ge1}\theta^{m-1}\right)+\mathrm{O}\left(\frac{1}{\log^2 x}\right)\\
=&-\frac{\log(1-\theta)}{\log x}+\frac{\log\log x+c_1+\log\theta}{\log x}+\mathrm{O}\left(\frac{1}{\log^2 x}\right)\\
=&\frac{\log\log x}{\log x}+\left(\log\frac{\theta}{1-\theta}+c_1\right)\frac{1}{\log x}+\mathrm{O}\left(\frac{1}{\log^2 x}\right).
\end{aligned}$$

This proves the proposition. □

The techniques used in the proof can be adapted to more general settings. We briefly mention that in the case $\theta=0$, there is a result of Decker and Moree [4] in the same spirit.

Corollary 2.1 (Decker, Moree)**.** *Let $C_r(x)$ denote the number of RSA integers $n=p\cdot q$ such that $p<q<rp$, where $r>1$ is a fixed real number. Then as x tends to infinity, we have*

$$C_r(x)=2\log r\frac{x}{\log^2 x}+\mathrm{O}\left(\frac{x}{\log^3 x}\right).$$

3. Second Notion

The second notion reflects the idea that the prime factors of a RSA integer should roughly have the same length. Thus, one is lead to consider the following set

$$\mathcal{B}(x;a,b):=\{n=p\cdot q\le x:\quad x^a<p<q\le x^b\}.$$

The set parameters a,b describe how small or large the prime factors p,q of a RSA integer are. The main result here is

Theorem 3.1. *Let a,b be two fixed real numbers such that $a<\frac{1}{2}$ and $a<b\le1$. Then the following estimates hold:*

$$|\mathcal{B}(x;a,b)|=\begin{cases}\frac{1}{2b^2}\frac{x^{2b}}{\log^2 x}+\mathrm{O}\left(\frac{x^{2b}}{\log^3 x}\right), & b\le\frac{1}{2};\\ B\frac{x}{\log x}+\mathrm{O}\left(\frac{x}{\log^2 x}\right), & b>\frac{1}{2}.\end{cases}$$

where $B=B(b)$ is an explicitly computable nonzero constant depending only on b.

The theorem basically says that, for a fixed a, the density of RSA integers under the current notion really hinges upon what the value b is. In order to achieve the density in the order of $\log^{-2} x$, b must be less than $\frac{1}{2}$.

Proof. We first consider the case $b \leq \frac{1}{2}$. We have

$$\begin{aligned}|\mathcal{B}(x;a,b)| &= \sum_{\substack{p \\ x^a < p \leq x^b}} \sum_{\substack{q \\ p < q \leq x^b}} 1 \\ &= \pi(x^b) \sum_{\substack{p \\ x^a < p \leq x^b}} 1 - \sum_{\substack{p \\ x^a < p \leq x^b}} \pi(p) \\ &= \pi(x^b)^2 - \sum_{\substack{p \\ x^a < p \leq x^b}} \frac{p}{\log p} + \mathrm{O}\left(\frac{x^{2b}}{\log^3 x}\right)\end{aligned}$$

now by the prime number theorem and partial summuation, this is equal to

$$= \frac{1}{2b^2}\frac{x^{2b}}{\log^2 x} + \mathrm{O}\left(\frac{x^{2b}}{\log^3 x}\right).$$

This settles the first case. In the second case $b > \frac{1}{2}$. If $a + b < 1$, then

$$|\mathcal{B}(x;a,b)| = \sum_{\substack{p \\ x^a < p \leq x^{1-b}}} \sum_{\substack{q \\ p < q \leq x^b}} 1 + \sum_{\substack{p \\ x^{1-b} < p \leq x^{1/2}}} \sum_{\substack{q \\ p < q \leq x/p}} 1 = I + II. \tag{3.1}$$

The term I is at most

$$I \ll \pi(x^{1-b})\pi(x^b) \ll \frac{x}{\log^2 x}. \tag{3.2}$$

And the second term II

$$\begin{aligned}II &= \sum_{\substack{p \\ x^{1-b} < p \leq x^{1/2}}} (\pi(x/p) - \pi(p)) \\ &= x \sum_{\substack{p \\ x^{1-b} < p \leq x^{1/2}}} \left(\frac{1}{p \log x/p} - \frac{p}{\log p}\right) + \mathrm{O}\left(x \sum_{\substack{p \\ x^{1-b} < p \leq x^{1/2}}} \frac{1}{p \log^2 x/p}\right) \\ &= B\frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x}\right).\end{aligned} \tag{3.3}$$

The estimate in the last line comes from Proposition 2.1. Therefore the assertion is true in view of (3.2), (3.3) and (3.1).

In the remaining case $a + b \geq 1$,

$$\begin{aligned}|\mathcal{B}(x;a,b)| &= \sum_{\substack{p \\ x^{1-b} < p \leq x^{1/2}}} \sum_{\substack{q \\ p < q \leq x/p}} 1 \\ &= \sum_{\substack{p \\ x^{1-b} < p \leq x^{1/2}}} (\pi(x/p) - \pi(p)) \\ &= B\frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x}\right).\end{aligned}$$

□

4. Generating RSA integers

In this section, we will answer the question that is set out in the introduction. Suppose first, we are generating RSA integers by picking the prime factors p, q inside a bounded interval. We then have

Theorem 4.1. *Let positive integers m, n and l be fixed such that $m - 1 < l \leq \frac{n}{2}$. Randomly generate a positive integer N with at most n bits. Then the probability of N being a RSA integer whose prime factors have at least m bits and at most l bits is asymptotic to (as $n \to \infty$)*

$$P(N) = \frac{1}{(l \log 2)^2 2^{n-2l+1}}.$$

Proof. The set of RSA integers whose prime factors have at least m bits and at most l bits is the set

$$\mathcal{B}\left(2^n; \frac{m-1}{n}, \frac{l}{n}\right) := \{N = p \cdot q < 2^n : \quad 2^{m-1} < p < q < 2^l\}.$$

$|\mathcal{B}\left(2^n; \frac{m-1}{n}, \frac{l}{n}\right)|$ can be estimated using Theorem 3.1. This gives

$$\left|\mathcal{B}\left(2^n; \frac{m-1}{n}, \frac{l}{n}\right)\right| = \frac{2^{2l}}{2(l \log 2)^2} + \mathrm{O}\left(\frac{2^{2l}}{n^3}\right).$$

The theorem readily follows. □

Definition 2. Let s and t be positive integers. We say that s and t are l bits apart if

$$1 < \frac{s}{t} \,(\text{or } \frac{t}{s}) \leq 2^l.$$

We may alternatively generate RSA integers by picking one prime first then selecting the other prime near the first prime. We then have the following result.

Theorem 4.2. *Let positive integers m, n and l be fixed such that $2m + l \leq n$. Randomly generate a positive integer N with at most n bits. Then the probability of N being a RSA integer whose prime factors have at most $m + l$ bits and are at most l bits aprart is asymptotic to (as $n \to \infty$)*

$$P(N) = \frac{1}{(\log 2)^2 (ml + m^2) 2^{n-2m-l}}.$$

Proof. The set of RSA integers less than 2^n and whose prime factors have at most m bits and are at most l bits apart has the cardinality twice the size of the following set:

$$\mathcal{S}\left(2^n; \frac{l}{n}, \frac{m}{n}\right) := \{N = p \cdot q < 2^n : \quad p < q < 2^l p,\, p < 2^m\}.$$

We invoke Theorem 2.1 for the estimate of $|\mathcal{S}\left(2^n; \frac{l}{n}, \frac{m}{n}\right)|$. Indeed

$$\left|\mathcal{S}\left(2^n; \frac{l}{n}, \frac{m}{n}\right)\right| = \frac{2^{2m+l}}{2(ml + m^2)(\log 2)^2} + \mathrm{O}\left(\frac{2^{2m+l}}{n^3}\right).$$

The theorem readily follows. □

5. Acknowledgements

The author wishes to thank referees' careful reading of the manuscript. Particular thanks go to Pieter Moree for showing the author how to reduce the error term in the main theorem to $\log^{-2} x$ from $\log\log x \log^{-1} x$ which is what author had originally.

Appendix A. The Prime Number Theorem

One usually denotes by $\pi(x)$ the number of primes not exceeding x. We have the following estimate for $\pi(x)$

Theorem A.1. *As x goes to infinity, we have*

$$\pi(x) = \frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x}\right).$$

We mention that better error terms exist (see [8]) though the error bound $\frac{x}{\log^2 x}$ is good enough for our applications. In particular, the prime number theorem implies

Corollary A.1. *The number of primes in any interval $(x^a, x^b]$ with $a < b$ is*

$$\sum_{x^a < p \leq x^b} 1 = \frac{x^b}{b \log x} + \mathrm{O}\left(\frac{x^b}{\log^2 x}\right).$$

The following estimate is needed in the paper. (See [5] for a proof)

Theorem A.2. *There exists a positive constant c such that for $x \geq 2$, one has*

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + c + \mathrm{O}\left(\frac{1}{\log x}\right).$$

Appendix B. The method of Partial Summation

The method of partial summation is a simple but effective tool for handling arithmetic sums.

Theorem B.1. *Let $\langle a_n \rangle$ be a sequence of complex numbers. Set*

$$A(t) = \sum_{n \leq t} a_n \quad (t > 0).$$

Let $b(t)$ be continuously differentiable function on the interval $[1, x]$. The we have

$$\sum_{1 \leq n \leq x} a_n b(n) = A(x)b(x) - \int_1^x A(t)b'(t)dt. \tag{B.1}$$

The readers can consult [5] for a proof. We illustrate the method by some examples.

Example 1. As z goes to infinity,

$$\sum_{p \leq z} p = \frac{z^2}{2 \log z} + \mathrm{O}\left(\frac{z^2}{\log^2 z}\right).$$

Indeed in the setting of Theorem B.1, define $\langle a_n \rangle$ by $a_n = 1, n = p$ and $a_n = 0$ otherwise; $b(t) = t$. In view of the prime number theorem, B.1 gives

$$\sum_{p \le z} p = z\pi(z) - \int_2^z \frac{t}{\log t} dt = \frac{z^2}{\log z} - \int_2^z \frac{t}{\log t} dt + \mathrm{O}\left(\frac{z^2}{\log^2 z}\right).$$

Performing integration by parts on the integral, the estimate follows.

Example 2. Let $\theta \ge 0$ and $c > 0$ be fixed. Then x goes to infinity

$$\sum_{p \le x^c} \frac{p}{\log x^\theta p} = \frac{x^{2c}}{2c(\theta + c)\log^2 x} + \mathrm{O}\left(\frac{x^{2c}}{\log^3 x}\right).$$

Define $\langle a_n \rangle$ by $a_n = n$ when $n = p$ and 0 otherwise; $b(t) = \frac{1}{\log x^\theta t}$.

References

[1] Ronald L. Rivest, Adi Shamir, Leonard Adleman. *A method for obtaining digital signatures and public-key cryptosystems.* Technical Report MIT/LCS/TM-82, MIT, Laboratory for Computer Science, Cambridge, Massachusetts,1977.

[2] Ronald L. Rivest, Adi Shamir, Leonard Adleman. *A method for obtaining digital signature and public-key cryptosystem.* Communications of the ACM 21(2), 120-126, 1978.

[3] A. Menezes, P. Van Oorschot, S. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Boca Raton FL. 1997.

[4] Andreas Decker, Pieter Moree. *Counting RSA-integers.* Results in mathematics, Volume 52, Number 1-2, 2008.

[5] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory.* Cambridge studies in advanced mathematics 46, 1995.

[6] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen.* Chelsea Publishing Co., New York, 1953.

[7] G.H. Hardy, E.M. Wright. *An introduction to the theory of numbers*, fourth Edition. The Clarendon Press, Oxford, 1968.

[8] A. Ivić. *The Riemann zeta-function.* Johh Wiley, New York, 1985.

[9] R. Crandall, C. Pomerance. *Prime numbers a computational perspective.* Springer-Verlag, 2001.

[10] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C.* John Wiley & Sons, New York, 2nd Edition, 1996.

University of Vlora, Department of Computer Science and Electrical Engineering, Vlora, Albania

E-mail address: bjustus@univlora.edu.al

Albanian Journal of Mathematics (ISSN: 1930-1235) was founded by T. Shaska in 2007 with the idea to support Albanian mathematicians in Albania and abroad.

The journal is not associated with any government institutions in Albania or any public or private universities in Albania or abroad. The journal does not charge any fees to the authors and has always been an open access journal. The journal supports itself with private donations and voluntary work from its staff. Its main office is in Vlora, Albania.