*Journal of Prime Research in Mathematics Vol.* **7***(2011), 19-24*

# ON EXISTENCE OF CANONICAL NUMBER SYSTEM IN CERTAIN CLASSES OF PURE ALGEBRAIC NUMBER FIELDS

ABDUL HAMEED[1], TORU NAKAHARA[*)2], SYED MUHAMMAD HUSNINE[3], SHAHZAD AHMAD[**)4]

Abstract. Canonical Number System can be considered as natural generalization of radix representation of rational integers to algebraic integers. We determine the existence of Canonical Number System in two classes of pure algebraic number fields of degree $2^n$ and $n$.

*Key words*: CNS, Eisenstein polynomial, discriminant and index of an algebraic integer, field discriminant, monogeneity.
*AMS SUBJECT CLASSIFICATION 2010*: Primary 11R04, Secondary 11R16.

## 1. Introduction

**1.1. Introduction and Motivation.** To discover an algebraic number field whose ring of integers has a power basis is a classical problem in Algebraic Number Theory [4].

Let $L$ be an algebraic number field, $Z_L$ be the ring of integers in $L$ and $N$ be the norm function with respect to $L/\boldsymbol{Q}$. The pair $(\alpha, \mathbf{N}_0)$, where $\mathbf{N}_0 = \{0, 1, 2, \cdots, |N(\alpha)| - 1\}$ is called a canonical number system in $Z_L$ for an

*)* Partially supported by grant (♯20540019) from the Japan Society for the Promotion of Science.
**)* Supported by PhD scholar fund from the Ministry of Education and Research, the Islamic Republic of Pakistan, through PN II-Ideas, Grant No 26/28-09-2007, CNCSIS Code ID-593.
[1,3,4]National University of Computer & Emerging Sciences, Lahore Campus, Lahore, Pakistan. Email: abdul.hameed@lhr.nu.edu.pk, syed.husnine@nu.edu.pk, shahzad.ahmad@lhr.nu.edu.pk
[2]National University of Computer & Emerging Sciences, Peshawar Campus, Peshawar, Pakistan. Email: toru.nakahara@nu.edu.pk, nakahara@ms.saga-u.ac.jp.

algebraic integer $\alpha$ if each algebraic integer $\alpha$ in $L$ can be represented uniquely as

$$\alpha = a_0 + a_1\alpha + \cdots + a_l\alpha^l,\ \pm a_i \in \mathbf{N}_0, a_l \neq 0$$

According to B. Kovács [1], the existence of a power integral basis in an extension field is equivalent to the existence of a canonical number system (CNS) for its maximal order. B, Kovács also proved that up to parallel translations by rational integers or algebraic conjugates of a generating integer of CNS there exist only finite many CNSes in the ring of integers of an algebraic number field [1].

The increased difficulty of theoretical attacks on the problem, and accompanying complexity of computational work due to increase in the degree of field extension, has opened up research areas in the field. Recent calculations by Y. Bilu, I. Gaál and K. Győry claim that the totally real sextic field $F$ whose Galois closure coincides with the symmetric group $S_6$ generated by

$$f(x) = x^6 - 5x^5 + 2x^4 + 18x^3 - 11x^2 - 19x + 1$$

took 4.8 months of total CPU time to enumerate the power bases generators [13]. The group of mathematicians of the period noted that this work took more time than all the previous smaller degree fields combined. This just goes on to show that difficulties of the problem increase multiplicatively with increase in the degree of extension.

CNS can be viewed as a natural generalization of the expression of rational integers to algebraic integers[11]. Namely, the pair$(\alpha, \mathbf{N}_0)$ with $\mathbf{N}_0 = \{0, 1, 2, \cdots, |N(\alpha)| - 1\}$ of CNS ensures in $Z_L$ a $|N_L(\alpha)|$-mal representation as same phenomena as for $0 < a \in \boldsymbol{Z}$ the decimal representation

$$a = a_0 + a_1 10 + \cdots + a_l 10^l,\ a_i \in \mathbf{N}_0, a_l \neq 0,$$

with $\mathbf{N}_0 = \{0, 1, 2, \cdots, 9\}$.

There are connections of the theory of CNS to the theories of finite Automata and Fractal Tiling [5, 6, 8]. Recently S. Akiyama [7] put CNS into a more general framework theory opening links to other areas, e.g. to long-standing problem on Salem Numbers [3].

### 1.2. Notations, Terminologies and Known Results.

**1.2.1. Monogeneity.** Let $L = \boldsymbol{Q}(\theta)$ be an algebraic number field of degree $n$ over the field $\boldsymbol{Q}$ of rational numbers, where $\theta$ is a root of an irreducible polynomial $f(x)$ of degree $n$ over $\boldsymbol{Q}$. The ring of integers of $L$ is denoted by $Z_L$. The field $L$ is said to be monogenic if $Z_L$ is generated by a single element, that is, there exists $\eta$ in $Z_L$ such that $Z_L = \boldsymbol{Z}[\eta]$[cf. 4, 9]. The discriminant of algebraic number $\theta$ denoted by $D(\theta)$ is defined by

$$D(\theta) = \prod_{1 \leqq i < j \leqq n} (\theta_i - \theta_j)^2 \tag{1}$$
$$= \prod_{1 \leqq i \leqq n} f'(\theta_i)$$

where $f'(x)$ denotes the derivative $\frac{df(x)}{dx}$ and $\theta_i$ denote the conjugates of $\theta$ with respect to the field extension $L/\boldsymbol{Q}$ [9]

Let $L$ be an algebraic number field $\boldsymbol{Q}(\theta)$ of degree $n$, where $\theta = \sqrt[n]{m}$ and $m \neq 1$ is a square free integer, then

$$D(\theta) = (-1)^{\frac{n(n-1)}{2}} n^n (-m)^{(n-1)} = (-1)^{\frac{(n+2)(n-1)}{2}} n^n m^{(n-1)} \tag{2}$$

Discriminant of an algebraic number $\theta$ can also be calculated directly by using any excellent computer programme like PARI/GP, GAP, MAGMA, MAPLE and so on. Let $d_L$ denotes the field discriminant of $L/\boldsymbol{Q}$, then we have the relation

$$D(\theta) = Ind(\theta)^2 d_L, \tag{3}$$

where $Ind(\theta)$ denotes the module index $[Z_L : \boldsymbol{Z}[\theta]]$ of a submodule $\boldsymbol{Z}[\theta]$ of $Z_L$ for an integer $\theta$.

**Lemma 1.1**[12]. *Let $L$ be an algebraic number field $\boldsymbol{Q}(\theta)$ of degree $n$ for some algebraic number $\theta \in Z_L$. Then $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$ is an integral basis for $L$ if and only if $Ind(\theta) = 1$.*

**1.2.2 Canonical Number System.** Let $L$ be an algebraic number field and $N$ be the norm function with respect to $L/\boldsymbol{Q}$. The pair $(\alpha, \mathbf{N}_0)$, where $\mathbf{N}_0 = \{0, 1, 2, ..., \mid N(\alpha) \mid -1\}$ is called a canonical number system (CNS) in $Z_L$ for an algebraic integer $\alpha$ if each algebraic integer in $L$ can be represented uniquely as

$$a_0 + a_1\alpha + \cdots + a_l\alpha^l, a_i \in \mathbf{N}_0, a_l \neq 0.$$

The most important relation of CNS to monogeneity of an algebraic number field is due to B. Kovács who claims

**Theorem 1.2**[2]. *In the ring $Z_L$ of integers in a number field $L$ of degree $n \geqq 3$, there exists a CNS if and only if $L$ is monogenic, that is $Z_L = \mathbb{Z}[\theta]$ for some $\theta$ in $L$.*

**1.3. Strategy to determine the existence of CNS.** The general strategy to determine the existence of CNS in an algebraic number field $L$ is to find some $\eta$ in $Z_L$ such that $Ind(\eta) = 1$. This is satisfied by (3) when $D(\eta)$ is a square free rational integer. However, this is not the case for pure extension fields of degree $\geqq 3$ by (2). Sometimes L. Sticklberger's Theorem can be useful

in this regard, which claims that $D_L \equiv 0, 1 \pmod 4$. But, this still may not be very helpful in pure algebraic number fields of degree $\geqq 3$. Then the following result is useful in determining the existence of CNS.

**Lemma 1.3** [12]. *Let $\theta$ be an algebraic integer, and let $L = \boldsymbol{Q}(\theta)$ be the field generated by it. If the minimal polynomial of $\theta$ over $\boldsymbol{Q}$ is Eisensteinian with respect to the prime $p$, that is, it has the form $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where $a_0, \cdots, a_{n-1}$ are divisible by $p$ and $a_0$ is not divisible by $p^2$, then the $Ind(\theta)$ in $L$ is not divisible by $p$.*

The equality $D(\theta) = D(\theta + k)$ for $k \in \boldsymbol{Z}$, will also be used, which follows directly from (1.1).

## 2. Family of Infinitely Many Pure Extension Fields of Degree $2^n$.

**Theorem 2.1** *A canonical number system exists in pure algebraic number fields $L = \boldsymbol{Q}(\theta)$, where $\theta$ is a root of the polynomial $f(x) = x^{2^n} - m$, with a square free integer $m \neq \pm 1$ and $m \equiv 2, 3 \pmod 4$.*

*Proof.* For a square free integer $m \neq \pm 1$ , the polynomial $f(x) = x^{2^n} - m$ is $p$-Eisenstein for every prime $p$ dividing $m$. Thus $f(x)$ is irreducible over $\boldsymbol{Q}$. Therefore $L = Q(\theta)$ for $f(\theta) = 0$ is a pure algebraic number field of degree $2^n$.
From (1.2), by $D(\theta) = (-1)^{\frac{2^n(2^n-1)}{2}} N_L(2^n\theta^{2^n-1})$
$= (-1)^{(2^{n-1})(2^n-1)}(2^n)^{2^n} N_L(\theta^{2^n-1}) = (-1)^{(2^{n-1})(2^n-1)}(2^n)^{2^n}(-m)^{2^n-1}$
$= (-1)^{2^{n-1}}(2^n)^{2^n} m^{2^n-1}$.
Thus we have

$$D(\theta) = (-1)^{2^{n-1}}(2^n)^{2^n} m^{2^n-1}. \tag{4}$$

**Case-I**: Given $m \equiv 2 \pmod 4$ implies that $m = 2(2k+1),\ k \in \boldsymbol{Z}$, so that prime factorization of $m$ in $\boldsymbol{Z}$ is $m = 2p_1p_2\cdots p_l$ with $p_i$ odd primes for $1 \leqq i \leqq l$. Therefore

$$D(\theta) = \pm(2^n)^{2^n}(2p_1p_2\cdots p_l)^{2^n-1} = Ind(\theta)^2 d_L \tag{5}$$

By Lemma 1.3 $Ind(\theta)$ is not divisible by 2 as well as $p_i$ for $1 \leqq i \leqq l$. Thus we obtain $Ind(\theta) = 1$ and $D(\theta) = d_L$, and hence $Z_L = \boldsymbol{Z}[\theta]$, i.e $L$ is monogenic. Hence CNS exists in $L$ by Theorem 1.2.

**Case-II**: Given $m \equiv 3 \pmod 4$ implies that $m = 4k + 3,\ k \in \boldsymbol{Z}$.
The next parallel transformation for $f(x)$ gives

$$g(x) = f(x-1) = (x-1)^{2^n} - m = x^{2^n} + a_{2^n-1}x^{2^n-1} + \cdots + (1-m),$$

where each $a_i, 1 \leqq i \leqq 2^n - 1$ is divisible by 2 and by $1 - m = 1 - (4k + 3) = -4k - 2 = -2(2k + 1)$, $(1 - m)$ is exactly divisible by 2. Thus $g(x)$ is 2-Eisenstein. Then $g(x)$ is irreducible over $\boldsymbol{Q}$, and so is $f(x) = x^{2^n} - m$. Thus again as in Case-I, none of the prime factors of $D(\theta) = D(\theta-1)$ divides $Ind(\theta)$. Therefore $Ind(\theta) = 1$ and $D(\theta) = d_L$, and hence $Z_L = \boldsymbol{Z}[\theta]$ holds, i.e $L$ is monogenic. Hence CNS exists in $L$. □

**Example 2.2** *Monogeneity of pure quartic fields $L = Q(\theta), \theta = \sqrt[4]{m}$ with a square free integer $m \equiv 2, 3 \pmod 4$ is evident from the above theorem for $n = 2$. The same result can be verified from* [10].

**Example 2.3** *Canonical Number System exists in pure octic fields $L = \boldsymbol{Q}(\theta)$, $\theta = \sqrt[8]{m}$ with a square free integer $m \equiv 2, 3 \pmod 4$. This is an immediate consequence from the above theorem for $n = 3$.*

## 3. Family of Infinitely Many Pure Extension Fields of Degree $n$.

Here we call an irreducible polynomial $f(x)$ over the field $\boldsymbol{Q}$ a CNS polynomial, if a root of $f(x)$ gives a CNS.

**Theorem 3.1** *Let $L = \boldsymbol{Q}(\theta)$, where $\theta = \sqrt[n]{m}$, with a square free integer $m \neq \pm 1$. If all the prime factors of $n$ divide $m$ then $L$ is monogenic and the minimal polynomial of $\theta$ is a CNS polynomial.*

*Proof.* Let $f(x) = x^n - m$ be the minimal polynomial of $\theta$. As $m \neq \pm 1$ is a square free integer, $f(x)$ is irreducible over $\boldsymbol{Q}$. From the equation (2)

$$D(\theta) = (-1)^{\frac{(n+2)(n-1)}{2}} n^n m^{n-1}. \tag{6}$$

Let $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ and $m = q_1 q_2 \cdots q_l$ be the prime factorizations of $n$ and $m$ respectively. Since each prime divisor of $n$ divides $m$, for each $i \in \{1, 2, \cdots, k\}$ there exists $j \in \{1, 2, \cdots, l\}$ such that $p_i = q_j$. We re-index the $q_j$ if it is necessary,such that,

$$p_1 = q_1,\ p_2 = q_2, \cdots,\ p_k = q_k; \qquad n = {q_1}^{\alpha_1} {q_2}^{\alpha_2} \cdots {q_k}^{\alpha_k},$$

so that from the equation (6)

$$\begin{aligned} D(\theta) &= (-1)^{\frac{(n+2)(n-1)}{2}} ({q_1}^{\alpha_1} {q_2}^{\alpha_2} \cdots {q_k}^{\alpha_k})^n (q_1 q_2 \cdots q_l)^{n-1} \\ &= (-1)^{\frac{(n+2)(n-1)}{2}} {q_1}^{n\alpha_1 + n - 1} {q_2}^{n\alpha_2 + n - 1} \cdots {q_k}^{n\alpha_k + n - 1} q_{k+1}^{n-1} q_{k+2}^{n-1} \cdots q_l^{n-1} \\ &= Ind(\theta)^2 d_L. \end{aligned}$$

But $f(x) = x^n - m$ is $q_j$-Eisenstein for each $1 \leqq j \leqq l$. Therefore by Lemma

1.3, none of $q_j$ divides $Ind(\theta)(1 \leqq j \leqq l)$. Hence $Ind(\theta) = 1$ implies that $D(\theta) = d_L$. Therefore $L$ is monogenic and a CNS exists in $L$. □

**Example 3.2** *Consider* $f(x) = x^{12} - 6$. *The polynomial is* 2 *as well as* 3*-Eisenstein, hence is irreducible over* $\boldsymbol{Q}$ *and* $L = \boldsymbol{Q}(\theta)$, *with a root* $\theta$ *of* $f(x)$ *is an algebraic number field of degree* 12. $D(\theta) = -12^{12}6^{11} = -2^{35}3^{23} = (Ind(\theta))^2 d_L$. *But* $Ind(\theta)$ *is not divisible by* 2 *and* 3. *Therefore* $Ind(\theta) = 1$. *Hence* $f(x) = x^{12} - 6$ *is a CNS polynomial.*

## References


[1] B. Kovács, Canonical number systems in algebraic number fields, Acta Math, Acad. Sci. Hungar., **37** (1981), 405 - 407.

[2] B. Kovács and A. Pethő, Number systems in integral domains, especially in orders of algebraic number fields. Acta Sci. Math. (Szeged), **55** (1991), 287 - 299.

[3] H. Brunotte, A. Huszti and A. Pethő, Bases of Canonical Number System in quartic algebraic number fields, Journal de Théorie des Nombers de Bordeaux, Tome **18**, no-3 (2006), 537 - 557.

[4] I. Gaál Diophantine equations and power integral bases, Birkhauser (Berlin), (2002)

[5] J. M. Thuswaldner, Elementary properties of canonical number systems in quartic fields, in: Applications of Fibinacci Numbers, Vol. 7, G. E. Bergum et al. (eds.), Kluwer Academic Publishers, Dordrecht (1998), 405-414.

[6] K. Scheicher, Kanonische Ziffernsysteme und Automaten, Grazer Mart. Ber., **333**, (1997), 1 - 17.

[7] S. Akiyama, T. Borbely, H. Brunotte, A. Pethő and J. M. Thuswaldner, Generalized radix representations and dynamical systems, Acta Math. Hung. **108** (2005), 207 - 238.

[8] S. Akiyama and J. M. Thuswaldner, On the topological structure of fractal tilings generated by quadratic number systems. Comput. Math. Appl. **49** (2005), no. 9-10, 1439 - 1485

[9] Ş. Alaca and K. S. Williams, Introductory Algebraic Number Theory, *Introductory Algebraic Number Theory*, Cambridge Univ. Press, (2004)

[10] T. Funakura, On integral bases of pure quartic fields, Math. J. Okayama Univ., **26** (1984), 27-41.

[11] V. Grünwald, Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale), Giornale di matematiche di Battaglini, **23**(1885), 203 - 221.

[12] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag, Third edition, Berlin-Heidelberg-New York; PWM-Polish Scientific Publishers, Warszawa, 2007.

[13] Y. Bilu, I. Gaál and K. Győry, Index form equations in sextic fields: a hard computation. Acta Arithmetica **115**, (2004), no-1, 85 - 96.