Rep. Fac. Sci., Kagoshima Univ.,
No. 41, pp. 1–5 (2008)

A note on existences of norm- and trace- compatible sequences

Tsuyoshi Atsumi

(Received Octobor 14, 2008)

Abstract

An extension of a theorem [5] is given and by using this result we give more transparent proofs to existences of norm- and trace- compatible sequences.

Keywords: finite fields, normal basis, norm- compatible sequence, trace- compatible sequences, Euclidean domain.

1 Introduction and Summary

In this paper an extension of a theorem [5] is given and by using this result we give more transparent proofs to existences of norm- and trace- compatible sequences. Let R be a principal ideal domain and M denote a finite, cyclic module over R. We follow notations of [2]. For an element α of M. let $<\alpha>:=\{r\alpha \mid r \in R\}$ be the R-submodule of M generated by α. $Ann_R(\alpha) := \{r \in R \mid r\alpha = 0\}$ denotes the annihilator ideal of α. The generator $Ord_R(\alpha)$ of $Ann_R(\alpha)$ is called the R-order of α. $Ord_R(\alpha)$ is uniquely determined modulo the group of units in R. The generator of $Ann_R(M) = \{r \in R \mid r\alpha = 0 \; \forall \alpha \in M\}$ is denoted by $Ord_R(M)$.

Throughout this note we may assume that $R/(r)$ is finite for all $r \in R - \{0\}$. (Here (r) denotes the ideal generated by r). Let $\Phi_R(r)$ denote the number of generators of the module $R/(r)$. In order to prove main proposition we need the following two propositions which we take from the paper of [2].

Proposition 1. *(i) $\Phi_R(a) = 1$ if and only if a is a unit in R.*

(ii) Let $a,\ b \in R - \{0\}$ with $gcd(a, b) = 1$, then $\Phi_R(ab) = \Phi_R(a)Phi_R(b)$.

(iii) If $a = p^k$ where $k \geqslant 1$ and p is irreducible in R, the $\Phi_R(a) = |R/(p^k)| - |R/(p^{k-1})|$.

(iv) Let $\Pi_{i=1}^t p_i^{k_i}$ be the prime decomposition of $a \in R - \{0\}$, $(p_i, p_j) = 1$ for $i \neq j$ and $k_i \geqslant 1$ for all i. Then $\Phi_R(a) = \Pi_{i=1}^t(|R/({p_i}^{k_i})| - |R/({p_i}^{k_i-1})|)$.

Proposition 2. *Let $A := Ord_R(M)$, then*

(i) Every R-submodule N of M is cyclic and $Ord_R(N)$ is a divisor of A.

(ii) Modulo the group of units in R, for every divisor r of A there exists exactly one R-submodule U_r of M satisfying $Ord_R(U_r) = r$.

(iii) For every divisor r of A there are exactly $\Phi_R(r)$ elements of R-oder r in M. Moreover, one has

$$\sum_{r|A} \Phi_R(r) = |M| = |R/(A)|$$

where r runs over a complete system of pairwise non-associate divisors of A.

We also need the following which is the generalized Chinese remainder theorem.

Proposition 3. *Let R be a principal ideal domain and $m_1, \ldots, m_n$ elements of $R - \{0\}$. Then for every n-tuple $(a_1, \ldots, a_n) \in R^n$ such that $a_i \equiv a_j \pmod{gcd(m_i, m_j)}$ for all $i \neq j$ there exists an $x \in R$ such that $x \equiv a_i \pmod{m_i}$ for all $i = 1, \ldots, n$. Moreover, x is uniquely determined modulo $lcm(m_1, \ldots, m_n)$.*

Let R be a Euclidean domain and n an element in R. Then we have the following factorization of n

$$n = up_1^{e_1} \cdots p_k^{e_k}, \tag{1}$$

where u is a unit and $p_1, \cdots, p_k$ are primes and $e_1, \cdots, e_k$ are integers. We note that any divisor of n and $p_1^{\nu_1} \cdots p_k^{\nu_k}$ are associate, for some $0 \leqslant \nu_i \leqslant e_i,\ i = 1, \cdots, k$. Let $D^{(n)}$ be the set $\{p_1^{\nu_1} \cdots p_k^{\nu_k} \mid 0 \leqslant \nu_i \leqslant e_i,\ i = 1, \cdots, k\}$ and $D = \bigcup_{n \in R} D^{(n)}$.

We note that $D^{(n)}$ contains the element 1 and let i and j are elements in $D^{(n)}$ satisfying $i \mid j$, then $l = j/i \in D^{(n)}$.

2 Main proposition

From now on we may assume that R is a Euclidean domain so that $Ord_R(\alpha)$ is the unique element of D for every α in R-module M and also any two elements $a,\ b \in R$ have the unique greatest common divisor $gcd(a, b) \in D$.

Fix an element k in D. Let C_k be the cyclic R-module of $Ord_R(C_k) = k$, written additively. A proof of the following proposition can be found in [8].

Proposition 4. *Let $M =< \alpha >$ be a finite, cyclic module over R with R-order n. Let h be an element of R. Then*

$$Ord(h\alpha) = Ord(\alpha)/gcd(h, Ord(\alpha)).$$

Lemma 1. *Let j and k be elements in D satisfying $j \mid k$. Let the function $f : C_k \longrightarrow C_{k/j}$ be given by $f(x) = jx$. Then f is a surjective homomorphism.*

Definition 1. *Let R be a Euclidean domain and k an element in R. A system of compatible generators for C_k is a partial function*

$$\alpha : D^{(k)} \longrightarrow C_k,$$

defined on $def(\alpha) \subset D^{(k)}$, satisfying these properties:

1 The function is defined on 1, that is, $1 \in def(\alpha)$;

2 If $i \in def(\alpha)$, then $Ord_R(\alpha(i)) = i$; and

3 If $i \in def(\alpha)$ and $j \mid i$, then $j \in def(\alpha)$ and $(i/j)\alpha(i) = \alpha(j)$.

A system of compatible generators α' is an extension of α if $def(\alpha) \subset def(\alpha')$ and if $\alpha'(i) = \alpha(i)$ whenever $i \in def(\alpha)$. If $D^{(k)} = def(\alpha)$ then α is a complete system of compatible generators.

Proposition 5. *Assume that α is a system of compatible generators for C_k. Then there exists a complete system α' of compatible generators for C_k that extends α.*

Proof. Our proof of this proposition is similar to that in [5]. If $k \in def(\alpha)$, then the theorem immediately follows. Hence, we may assume that $k \notin def(\alpha)$. We first show how to extend $def(\alpha)$ by one element. That is, we show that there exists a system of compatible generators α' satisfying $\alpha'(i) = \alpha(i)$ whenever $i \in def(\alpha)$ and $|def(\alpha') - def(\alpha)| = 1$. Let $s = min\ T$ be the smallest integer in $T = \{d(a) | a \in D^{(k)} - def(\alpha)\}$, where d is a Euclidean function from R to the non-negative integers.

Let $s = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ be the unique prime factorization of s. For $1 \leqslant i \leqslant m$, define $q_i = s/p_i$. By the observation above, each $q_i \in def(\alpha)$. Also, each of the $\alpha(q_i)$ is in C_s, the unique cyclic submodule of C_k of R-order s.

First suppose that $m = 1$ and $e_1 = 1$. Define α' to be a system of compatible generators that extends by the element s, where $\alpha'(s)$ is chosen to be any one of the $\Phi_R(s)$ generators of C_s that exists by Proposition 1 (iii).

Now suppose that $m = 1$ and $e_1 > 1$. Since $C_s \supseteq C_{s/p_1} =< \alpha(p_1^{e_1 - 1}) >$, by Lemma 1 there exists an $x \in C_s$ such that $px = \alpha(p_1^{e_1 - 1})$. Then Proposition 4 tells us that $Ord_R(x) = p_1^{e_1}$. So x generates C_s.

Finally suppose that $m > 1$. Let $\gamma \in C_k$ of R-order s, that is, a generator of C_s. There exists r_i satisfying

$$r_i\gamma = \alpha(q_i)$$

Hence, $q_i(r_i\gamma) = 0$. This shows that $Ord_R(\gamma) \mid q_i r_i$. So if we set $s_i' = r_i/p_i$, then $s_i' \in R$. Applying Proposition 3, we obtain an element $x \in R$ satisfying the system of congruences

$$x \equiv r_i/p_i \pmod{q_i},$$

provided that

$$r_i/p_i \equiv r_j/p_j \pmod{gcd(q_i,\ q_j)}, \tag{2}$$

for every pair i, j, where $1 \leqslant i < j \leqslant m$.

To establish the congruences (2), fix i and j satisfying $1 \leqslant i < j \leqslant m$. Eliminating q_i and q_j from the congruences (2), we obtain

$$r_i/p_i \equiv r_j/p_j \pmod{s/(p_ip_j)},$$

Now the element $s/(p_ip_j) \in def(\alpha)$, by the definition of s. Furthermore,

$$\alpha(s/(p_ip_j)) = r_ip_j\gamma = r_jp_i\gamma$$

it follows that

$$r_ip_j \equiv r_jp_i \pmod{s}$$

and that

$$r_i/p_i \equiv r_j/p_j \pmod{s/(p_ip_j)},$$

as required. We obtain x satisfying the system of congruences (2). Equivalently, x satisfies this system of congruences:

$$xp_i \equiv r_i \pmod{s} \tag{3}$$

We now define α' to be a system of compatible generators that extends α by the one element s, where $\alpha'(s) = x\gamma$. Since x is unique modulo s, $x\gamma$ is uniquely defined. We must verify that α' is also a system of compatible generators.

First note that

$$\begin{aligned} s/q_i(\alpha'(s)) &= p_i(x\gamma) \\ &= (p_ix)\gamma \\ &= r_i\gamma \\ &= \alpha(q_i), \end{aligned}$$

by the system of congruences (3) and the fact that R-order of γ is s.

Second we must show that $Ord_R(\alpha'(s)) = s$. Observe that, for each i, $p_i\alpha'(s)$ generates the cyclic module of R-order q_i and $\alpha'(s) \in C_s$. So $Ord_R(\alpha'(s)) = (s/p_i)l_i$ for some $l_i \in R$ and $Ord_R(\alpha'(s)) \mid s$. Since $m > 1$ and the uniqueness of factorization of the element $Ord_R(\alpha'(s))$ in R, we see that $s \mid Ord_R(\alpha'(s))$. We conclude that $Ord_R(\alpha'(s)) = s$. □

3 Two cyclic module structures in finite fields

In order to prove Theorems 1 and 2 (see Theorems 1 and 2 in [9]) we need the following two elementary lemmas.

Lemma 2. *If $n,\ r,\ s$ are integers with $n \geqslant 2$, $r \geqslant 1$, $s \geqslant 1$, then*

$$n^s - 1 \mid n^r - 1 \quad \textit{if and only if} \quad s \mid r.$$

Lemma 3. *In any field*

$$x^s - 1 \mid x^r - 1 \quad \textit{if and only if} \quad s \mid r.$$

Let F_q and F_{q^m} be the finite fields of order q and q^m, respectively. For $n \in Z$ and $\alpha \in \bar{F_q}^*$ the mapping $(n, \alpha) \longmapsto \alpha^n$ makes the multiplicative group of $\bar{F_q}$ a module over Z, where $\bar{F_q}$ denotes an algebraic closure of F_q and $\bar{F_q}^* = \bar{F_q} - \{0\}$. It is well-known that $F^*_{q^m} = F_{q^m} - \{0\}$ is a cyclic group of order $q^m - 1$. So the multiplicative group $(F^*_{q^m}, \cdot)$ is a cyclic Z-module and its generators are the primitive roots of F_{q^m}. We have the following(see [9]).

Fact 1. *Let $\alpha \in \bar{F_q}^*$. Then α is primitive in F_{q^m} if and only if $ord(\alpha) = q^m - 1$, if and only if the Z-submodule of $\bar{F_q}^*$ generated by α equals $\bar{F_q}^*$*

Let $f := \sum_{i=0}^n f_i x^i$ be a polynomial of $F_q[x]$ and let $\alpha \in F_{q^m}$, then the scalar multiplication $\Diamond$: $F_q[x] \times F_{q^m} \longrightarrow F_{q^m}$

$$(f, \alpha) \longmapsto f \Diamond \alpha := \sum_{i=0}^{n} f_i \alpha^{q^i}$$

turns the additive group $(F_{q^m}, +)$ into a finite, cyclic module over $F_q[x]$, its generators are generators of normal bases.

The following holds(see [9]).

Fact 2. *Let $\alpha \in \bar{F_q}^*$. Then α is normal in F_{q^m} in over F_q, if and only if $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ constitutes a basis of F_{q^m} over F_q, if and only if $Ord(\alpha) = X^m - 1$, if and only if the $F_q[X]$-submodule of $\bar{F_q}$ generated by α equals F_{q^m}.*

Let $I \subset N$ denote a devisor-closed set and, for $m \in N$ divisible by d, let $N_{m:d}$ and $T_{m:d}$ denote the norm and the trace function from F_{q^m} onto F_{q^d} respectively.

Definition 2. *A sequence $(\alpha_n)_{n \in I}$ of elements $\alpha_n \in \bar{F_q}$ is called norm-compatible if for every $n \in I, \alpha_n$ is primitive in F_{q^n} and $N_{n:d}(\alpha_n) = \alpha_d$ for all divisors d of n.*

Definition 3. *A sequence $(\alpha_n)_{n \in I}$ of elements $\alpha_n \in \bar{F_q}$ is called trace-compatible if for every $n \in I, \alpha_n$ is normal in F_{q^n} and $T_{n:d}(\alpha_n) = \alpha_d$ for all divisors d of n.*

Note that$N_{m:d}(\alpha) = \alpha^{(q^m-1)/(q^d-1)}$ and that $T_{m:d}(\alpha) = (X^m - 1)/(X^d - 1) \Diamond \alpha$.

Theorem 1. *Norm compatible sequences $(\alpha_n)_{n \in N}$, $\alpha_n \in F_{q^n}$, do exist.*

Proof. We note that $F^*_{q^n} = F_{q^n} - \{0\}$ is a $Z-$module of order $q^n - 1$ and Z is a Euclidean domain with a Euclidean function $d(n) = |n|$. And in this case D is the set of positive integers in Z. So by Proposition 5 there exists a complete system of compatible generators α'. Then we let α be the restriction of α' to $\{q^d - 1 \mid d|n\}$. And we set $\beta(d) = \alpha(q^d - 1)$. By Lemma 2 and Fact 1 we see that$\{\beta(d)\}_d$ is a norm-compatible sequences. □

Theorem 2. *Trace compatible sequences $(\alpha_n)_{n \in N}$, $\alpha_n \in F_{q^n}$, do exist.*

Proof. (cf. the proof of Theorem 1 in [9].) From the above the additive group of F_{q^n} becomes a cyclic module over $F_q[X]$ of $Ord_R\ X^n - 1$ and $F_q[X]$ is an Euclidean domains with a Euclidean function $d(f) = deg\ f$, the degree of the polynomial f. And in this case D is the set of the monic polynomials in $F_q[X]$. So by Proposition 5 there exists a complete system of compatible generators α'. Then we let α be the restriction of α' to $\{X^d - 1 \mid d|n\}$. And we set $\beta(d) = \alpha(X^d - 1)$. By Lemma 3 and Fact 2 we see that$\{\beta(d)\}_d$ is a trace-compatible sequences. □

References

[1] Y. Chang, T. K. Truong, I. S. Reed, and G. L. Mullen, Normal bases over $GF(q)$, Jounal of Algebra 241, 89–101(2001)

[2] Dirk Hachenberger, On primitive and free roots in a finite field, Appl. Algebra Eng. Commun. Comput. 3, 139–150(1992)

[3] Dirk Hachenberger, Characterizing normal bases via the trace map, Communications in Algebra 32 , 269-277(2004).

[4] Dirk Hachenberger, Generators for primary closures of Galois fields, Finite Fields and their Applications 9, 122-128 (2003).

[5] Lenwood S. Heath & Nicholas A. Loehr, New algorithms for generating Conway polynomials over finite fields, Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (Baltimore, MD, 1999), 429–437, ACM, New York (1999)

[6] Dieter Jungnickel, Finite fields, Structure and Arithmetic, Bibliographisches Institut, Mannheim,(1993)

[7] H. W. Lenstra & R. J. Schoof, Primitive normal bases for finite fields, Mathematics of Computation 48, 217–231(1987)

[8] Rudolf Lidl & Harald Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Toronto, London, Amsterdam: Addison-Wesley, Reading, Mass.1983

[9] Alfred Scheerhorn, Trace- and norm-compatible extensions of finite fields, Appl. Algebra Eng. Commun. Comput. 3, 199–209(1992)