INFORMATIQUE THÉORIQUE ET APPLICATIONS

NGUYEN HUONG LAM

On codes having no finite completion

Informatique théorique et applications, tome 30, n° 6 (1996), p. 483-493

<http://www.numdam.org/item?id=ITA_1996__30_6_483_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 30, n° 6, 1996, p. 483-493)

ON CODES HAVING NO FINITE COMPLETION (*)

by NGUYEN HUONG LAM ([1])

Communicated by J. BERSTEL

Abstract. – *For each natural number $n \geq 5$ and $n \neq 6$, we propose a class of finitely incompletable codes that contain a^n on a binary alphabet $\{a, b\}$. The construction is essentially based on unambiguous pairs unembeddable to a factorization of $\mathbf{Z}_n$.*

Résumé. – *On présente une technique pour construire une famille de codes finiment incompletables contenant le mot a^n pour tout $n \geq 5$ et $n \neq 6$ sur un alphabet $\{a, b\}$. Cette construction est basée sur la notion de paires nonambigües incompletables en une factorisation de $\mathbf{Z}_n$.*

1. INTRODUCTION

In this article, we deal with the notion of maximal code, which plays an important role in the theory of variable length codes. For background we refer to the book of Berstel and Perrin [1].

A typical result about codes is that every code is embedded into a maximal one *i.e.*, a code any proper superset of it is no longer a code. Proving existence of such a maximal code is a standard technique by application of Zorn's lemma. Similarly, the problem of embedding a code into a maximal one is raised for special families of codes, which often requires more elaborate constructions than a simple application of Zorn's lemma. We mention two major results. First, Ehrenfeucht and Rozenberg proved that each regular code is embedded into a maximal code which is also regular [5]. Second, for the family of regular codes with finite deciphering delay, V. Bruyère, Limin Wang and Liang Zhang have recently showed that every such code is included in a regular maximal code with the same delay [2].

For finite codes, the situation is different. In [10], Restivo proposed a class of finite codes not contained in any finite maximal code. As the

(*) Received April 1993; accepted October 1993.
([1]) Hanoi Institute of Mathematics, P.O. Box 631, Bo Ho, 10 000 Hanoi, Vietnam.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/96/06/$ 7.00/

smallest among them one can take the code $\{a^5, a^2 b, ba, b\}$ on a binary alphabet $\{a, b\}$. The very same example can be found in an earlier work of A1. A. Markov [9]. Further, some extensions and other constructions are presented in [4]. All of them are codes in $a^* \cup a^* b \cup ba^*$, containing $\{a^n, b\}$, but the constructions work only in case n is a prime larger than 3 or $n-1$ is a composite larger than 6. In this paper, based on simple multiplication properties of integers, we propose some constructions yielding finite codes with no finite completion covering all the existing classes in [9], [10], [4]. In fact, we prove that for any integer $n \geq 5$ and $n \neq 6$, there exists a code in $a^* \cup a^* b \cup ba^*$ containing $\{a^n, b\}$ having no finite completion. The cases of $n = 2, 3, 4, 6$ remain open. Codes of the form $a^* \cup a^* b \cup ba^*$ are closely connected with the notion of factorization of the group $\mathbf{Z}_n$ of residues modulo n, so we investigate a special class of factorizations of $\mathbf{Z}_n$ called elementary factorizations. Those factorizations are helpful in generating codes having no finite completion to our purpose.

2. NOTATIONS AND MAIN RESULTS

Let $A = \{a, b\}$ be a binary alphabet and A^* the set of words on A with the catenation as product. A subset C of A^* is a code if a word is expressed as a product of words from C, it is so uniquely *i.e.*, whenever

$$c_1 ... c_n = c'_1 ... c'_m$$

then $n = m$ and $c_1 = c'_1, ..., c_m = c'_m$. A code is said to be *maximal* if it is not a proper subset of any other code. An application of Zorn's lemma shows that every code is contained in a maximal one, called a *completion* of it. If a code has a finite completion, we say also it is *finitely completable*; otherwise, we say that it is *finitely incompletable.* For some background information and definitions we refer to [1].

Let denote $\mathbf{N}$ the set of nonnegative integers and for $n \geq 1$,

$$\mathbf{N}_n = \{i : 0 \leq i \leq n-1\},$$

$\mathbf{Z}_n$ the residue class group modulo n. We recall a notion from [11]. A pair (H, K) of subsets of $\mathbf{N}$ is called an *unambiguous pair* provided, whenever

$$h + k = h' + k'$$

for $h, h' \in H$ and $k, k' \in K$, then $h = h'$, $k = k'$. More specifically, we say that (H, K) is an *unambiguous pair for* a subset S if it is an unambiguous pair and $H + K = \{i + j : i \in H, j \in K\} \subseteq S$. Likewise, we introduce the following

DEFINITION 1: The pair (H, K) of subsets of $\mathbf{Z}_n$ is called an *unambiguous pair* of $\mathbf{Z}_n$ if for any $s \in S$ there exist at most one pair $(i, j) \in (H, K)$ such that $s = i + j$.

The classical notion of *factorization* of $\mathbf{Z}_n$ [6] is that of unambiguous pair such that $H + K = \mathbf{Z}_n$.

Since $\mathbf{N}_n$ is a complete residue system to the modulus n, we usually identify each element of $\mathbf{Z}_n$ by its representative in $\mathbf{N}_n$. By this convention, every unambiguous pair of $\mathbf{Z}_n$ is an unambiguous pair and, vice versa, every unambiguous pair for $\mathbf{N}_n$ can be viewed as that of $\mathbf{Z}_n$. In particular, an unambiguous pair (H, K) for $\mathbf{N}_n$ with $H + K = \mathbf{N}_n$ is obviously a factorization of $\mathbf{Z}_n$ and is called in [11] an *elementary factorization* of $\mathbf{Z}_n$.

From now on, for our purposes, the summands of unambiguous pairs of $\mathbf{Z}_n$ are supposed to contain 0, if we do not specify otherwise. We say that an unambiguous pair is *nontrivial* if each summand contains more than one element.

For any subset $C \subseteq A^*$, we define the pair of subsets of $\mathbf{N}$ [11]

$$L(C) = \{i : b^+ a^i \cap C \neq \emptyset\}, \qquad R(C) = \{j : a^j b^+ \cap C \neq \emptyset\}.$$

and for any pair of subsets (L, R) of $\mathbf{Z}_n$ let define the following language

$$C(L, R) = \{a^n, b\} \cup \{ba^i : i \in L\} \cup \{a^j b : j \in R\}.$$

The following assertion is straightforward [11].

PROPOSITION 1: *If $C \subseteq A^*$ is a code such that $\{a^n, b\} \subseteq C$, $n \geq 1$, then*

(i) *$(L(C), R(C))$ is an unambiguous pair of $\mathbf{Z}_n$;*

(ii) *for any unambiguous pair (L, R) of $\mathbf{Z}_n$, $C = C(L, R)$ is a code and $L(C) = L$, $R(C) = R$.*

The following statement is simple but important for our consideration [11].

PROPOSITION 2: *Let C be a code such that $\{a^n, b\} \subseteq C$ then C has a finite completion only if there exists a factorization (H, K) of $\mathbf{Z}_n$ such that $L(C) \subseteq H$ and $R(C) \subseteq K$.*

Proof: Suppose that C has a finite completion X. Clearly, $L(C) \subseteq L(X)$, $R(C) \subseteq R(X)$. To prove that $(L(X), R(X))$ is a factorization of $\mathbf{Z}_n$, by Proposition 1, it suffices to show that for any $s \in \mathbf{Z}_n$, there exists $(i, j) \in (L(X), R(X))$ such that $s \equiv i + j \bmod n$. Let d be any integer larger than the maximal length of the words of X and congruent to s

modulo n. Consider the word $w = b^d a^d b^d$. Since X is maximal, it is *complete* [1], hence there are $u, v \in A^*$, $x_1, ..., x_m \in X$ such that

$$ub^d a^d b^d v = x_1 \dots x_m \in X^*.$$

Let p be the largest and q the smallest integer such that

$$|ub^d| \leq |x_1 \dots x_p| \leq |vb^d a^d| \leq |x_1 \dots x_q|.$$

Since $d \geq |x_q|$ we have

$$x_p \in b^* a^i,\ x_{p+1} = \dots = x_{q-1} = a^n,\ x_q \in a^j b^*$$

and thus $s \equiv d \equiv i + j \bmod n$. By Proposition 1, $(L(X), R(X))$ is a factorization of $\mathbf{Z}_n$. The proof is complete.

Now we attend to the construction of finitely incompletable codes. The following observation is crucial: for any factorization (H, K) of $\mathbf{Z}_n$, $|H|\,|K| = n$, where $|H|$ denotes the cardinality of H. The argument in [4] and [10] requires the existence of a nontrivial factorization of $\mathbf{Z}_{n-1}$ that is possible only in case $n - 1$ is a composite number, in particular, that is the case when $n = p$ is a prime ≥ 5. However, we have the following proposition which will give rise to a construction yielding the desired code for all $n \geq 5$ and $n \neq 6$.

PROPOSITION 3: *Let n, d, t, j be integers such that d does not divide n and $n = td + j$ with $t \geq 2$, $0 < j \leq d - 1$. If (L, R) is an unambiguous pair of $\mathbf{Z}_n$ such that $|R| = t$ and either of the following conditions*

(i) *$t \nmid j$ and $|L| = d$,*

(ii) *$\{0, 1, ..., d - 1\} = L$ and $d \in R$*

holds then $C(L, R)$ has no finite completion.

Proof: Suppose on the contrary that $C(L, R)$ has a finite completion, therefore $L \subseteq H$, $R \subseteq K$ for some factorization (H, K) of $\mathbf{Z}_n$. For $|L| \geq d$, we have $|K| = |R|$, otherwise it follows

$$n = |K|\,|H| \geq (|R| + 1)\,|L| \geq (t + 1)\,d > dt + j = n$$

So in both cases (i) and (ii), $K = R$.

Let now (i) hold. Since $n = |H|\,|K| = (|H| - d)\,t + dt$, it follows $j = (|H| - d)\,t$ which contradicts the assumption $t \nmid j$. Therefore, $C(L, R)$ has no finite completion in this case.

Next, suppose that (ii) holds. Let $K = R = \{k_0, k_1, ..., k_{t-1}\}$, where $k_0 = x_0\,d + j_0, ..., k_{t-1} = x_{t-1}\,d + j_{t-1}$ with $0 \leq J_0, ..., j_{t-1} < d$ and

$x_0 \leq x_1 \leq \ldots \leq x_{t-1} \leq t$. Since $\{0, 1, \ldots, d-1\} = L$ and (L, R) is an unambiguous pair, we have

$$0 \leq x_0 < x_1 < \ldots < x_{t-1} \leq t.$$

If $x_{t-1} = t$, as $k_{t-1} < n$, then $j_{t-1} < j$, which implies

$$0 \equiv n = k_{t-1} + (j - j_{t-1}) \bmod n$$

that is impossible, since $0 \neq j - j_{t-1} \in L$ and $k_{t-1} \in R$. Consequently, we have

$$x_0 = 0, \qquad x_1 = 1, \ldots, x_{t-1} = t - 1.$$

As is supposed 0, $d \in R$, hence $j_0 = 0$, $j_1 = 0$. It can be seen also that

$$0 \leq j_2 \leq j_3 \leq \ldots \leq j_{t-1} \leq j.$$

In fact, for example, $j_3 < j_2$ implies

$$2\,d + j_2 + d - (j_2 - j_3) = 3\,d + j_3$$

with $0 < d - (j_2 - j_3) < d$ that contradicts the uniqueness of the presentation $L + R$. Further, if $j_0 = j_1 = \ldots = j_{t-1} = 0$, any element of $H - L$ must have the form $td + j'$, $j' < j$. Hence the congruence

$$td + j' + d \equiv d - j + j' \bmod n$$

with $0 < d - j + j' < d$ implies that (H, K) is not a factorization: a contradiction. Thus, otherwise, let s be the minimal number such that $j_s \neq 0$, hence $t - 1 \geq s \geq 2$. Consider the number sd. Clearly $sd \notin K$; sd cannot belong to H, since $sd + d = sd + j_s + (d - j_s)$ with $d - j_s \in L \subseteq H$ and $d \in K$. Consequently, $sd \equiv h + k$, $h \in H - \{0\}$, $k \in K - \{0\}$. We show that this possibility also leads to a contradiction. We have two cases

(1) $sd = h + k \Rightarrow k < sd \Rightarrow k = ld$ $(0 < l < s) \Rightarrow h = md$ $(m > 0)$. As $d \in K$, we have $m > 1$, which implies $l < s - 1$. But then

$$(s + 1)\,d = sd + j_s + (d - j_s) = md + (l + 1)\,d,$$

where $l + 1 < s \Rightarrow (l + 1)\,d \in K$ that violates the assumption.

(2) $sd + n = h + k$. Set $h = xd + j' \Rightarrow x \leq t$ (by convention $h < n$), $k = id + j_i \Rightarrow 0 < i \leq t - 1$. We have

$$(s + t)\,d + j = (x + i)\,d + (j' + j_i).$$

Since $j_i \leq j$, then $j = j' + j_i$, $x + i - t = s$. Hence $0 < i - s + 1 \leq i$ and $j' + j_{i-s+1} \leq j' + j_i = j$. But then

$$\begin{aligned} xd + j' + (i - s + 1)\, d + j_{i-s+1} &= n + d - j + j' + j_{i-s+1} \\ &\equiv d - j + j' + j_{i-s+1} \bmod n \end{aligned}$$

with $0 < d - j + j' + j_{i-s+1} \leq d$. This is a contradiction with the assumption (H, K) a factorization of $\mathbf{Z}_n$, since $xd + j' > 0$, $(i - s + 1)\, d + j_{i-s+1} > 0$. This concludes the proof.

It turns out that, for all $n \geq 5$, $n \neq 6$, we can find a pair (L, R) satisfying (i) or (ii) of Proposition 3:

If n is odd, we have $n = \dfrac{n-1}{2} . 2+1$, where $d = \dfrac{n-1}{2} > 1, t = 2, j = 1$ and $t \nmid j$ and any nontrivial unambiguous pair (L, R) with $|L| = d$ will do (for instance $L = \{0, ..., d-1\}$, $R = \{0, d\}$). If n is even, $n = \dfrac{n-2}{2} . 2+2$; $d = \dfrac{n-2}{2} \geq 3$ (as $n > 6$), $t = 2$, $j = 2$. We set $L = \{0, 1, ..., d - 1\}$, $R = \{0, d\}$ and see that (L, R), being a nontrivial factorization of $\mathbf{Z}_n$, satisfies (ii) of Proposition 3. Thus, we have proved

THEOREM 1: *For all $n \geq 5$, $n \neq 6$ there exists a code containing $\{a^n, b\}$ having no finite completion.*

Example 1: Let $n = 8$, we choose $d = 3$, $t = 2$, $j = 2$ and set $L = \{0, 1, 2\}$, $R = \{0, 3\}$; so $C(L, R) = \{a^8, ba, ba^2, a^3 b, b\}$ is finitely incompletable. For $n = 10$, beside $d = 4$, $t = 2$, $j = 2$, we can take also $d = 3$, $t = 3$, $j = 1$. As $t \nmid j$ for $L = \{0, 1, 2\}$, $R = \{0, 3, 7\}$, $C(L, R) = \{a^{10}, ba, ba^2, a^3 b, a^7 b, b\}$ is finitely incompletable.

For some values of n, the argument is simpler as direct consequences of Proposition 2. First, if $n = p$ is a prime number, there is no nontrivial factorization of $\mathbf{Z}_n$. So, we have [11].

COROLLARY 1: *Let p be a prime and (L, R) a nontrivial unambiguous pair of $\mathbf{Z}_p$, then $C(L, R)$ has no finite completion.*

Remark: In particular, when (L, R) is a nontrivial unambiguous pair for $\mathbf{N}_{p-1}$ $(p \geq 5)$, we obtain the class of codes of Restivo [10], [11].

Proof: If $C = C(L, R)$ has a finite completion then there is a factorization (H, K) of $\mathbf{Z}_p$ such that $L = L(C) \subseteq H$, $R = R(C) \subseteq K$, by Proposition 2. Then $|H| \geq |L(C)| \geq 2$, $|K| \geq |R(C)| \geq 2$ and $p = |\mathbf{Z}_p| = |H|\,|K|$, which is impossible as p is prime.

Example 2: For a prime $p > 3$ ($H = \{0, 1\}$, $K = \{0, 2\}$) is a nontrivial unambiguous pair of $\mathbf{Z}_p$. Then $C(H, K) = \{a^p, ba, a^2 b, b\}$ is a finitely incompletable code. If we take $H = \{0, p+1\}$, $K = \{0, p-2\}$, (H, K) is again a nontrivial unambiguous pair of $\mathbf{Z}_p$, thus $\{a^p, ba^{p+1}, a^{p-2} b, b\}$ has no finite completion.

Exploiting once again Proposition 2, we have the following assertion for odd composite numbers > 5.

COROLLARY 2: *Let $n > 5$ be an odd composite then there exists a code containing $\{a^n, b\}$ and having no finite completion.*

Proof: Let p be the least prime divisor of n, say, $n = ps$. As n is odd composite, p, s are odd and $n > s \geq p \geq 3$. Consider $L = \{0, 1\}$, $R = \{0, 2, ..., 2s\}$. Evidently, (L, R) is an unambiguous pair of $\mathbf{Z}_n$. If (L, R) could be completed to a factorization (H, K) of $\mathbf{Z}_n$, then $|H| \geq |L|$ and $|H|$ be a divisor of n, which imply $|H| \geq p$. Since $|K| \geq |R| = s + 1$, we get $n = |H|\,|K| \geq p(s+1) > ps = n$, which is a contradiction showing that $C(L, R)$ is finitely incompletable.

In the following proposition, we extend the construction of and [4].

PROPOSITION 4: *Let (L, R) be an unambiguous pair of $\mathbf{Z}_n$ such that $\min\{|L|, |R|\} > n - |L|\,|R| > 0$. Then the code $C(L, R)$ has no finite completion.*

Proof: Suppose on the contrary that $C(L, R)$ has a finite completion. By Proposition 2, $L \subseteq H$, $R \subseteq K$ for some factorization (H, K) of $\mathbf{Z}_n$. Since $|L|\,|R| < n$, either $|H| > |L|$ or $|K| > |R|$. Say, $|H| > |L|$, then

$$\begin{aligned} n &= |H|\,|K| \geq (|L| + 1)\,|K| \geq (|L| + 1)\,|R| \\ &= |L|\,|R| + |R| > |L|\,|R| + n - |L|\,|R| = n : \text{ a contraction.} \end{aligned}$$

Remark: For any nontrivial unambiguous pair (L, R) of $\mathbf{Z}_n$ with $|R|\,|L| = n - 1$, as (L, R) is an unambiguous pair for the set $S = \{i + j : i \in L, j \in R\} \equiv \{0, 1, ..., n-1\} \setminus t$ modulo n for some $t : 0 < t \leq n - 1$, we get the Corollary 2.3 of [4].

Example 3: (*a*) Let n be an odd integer ≥ 5, $n - 1$ is even and ≥ 4. It is easy to obtain a nontrivial unambiguous pair for $\mathbf{N}_{n-1}$, for instance, let $n - 1 = 2s$, $s \geq 2$, we set $H = \{0, 1\}$, $K = \{0, 2, ..., 2(s-1)\}$. Therefore, the code $C(H, K)$ has no finite completion. It is another proof of Corollary 2.

(*b*) For some even integers, the construction of Proposition 4 is straightforward. Let $n = 14$, the subsets $H = \{0, 1, 2\}$ and $K = \{0, 3, 6, 9\}$ constitute an unambiguous pair of $\mathbf{Z}_{14}$ with $|K| > |H| = 3 > 14 - 12 = 2$. Analogously proceeded for $n = 18$.

Note that when $n = 2$, 3, 4 or 6, the existing methods fail. For many other values of n, Proposition 4 cannot be applied readily as above, the smallest one is $n = 8$, then Theorem 1 comes in handy (Example 1).

3. FACTORIZATIONS OF $\mathbf{N}_n$

In the previous section, factorizations of $\mathbf{Z}_n$ play an important role in our consideration. It is of an interest to search for a method to generate them. Determining all factorizations of $\mathbf{Z}_n$ is very difficult and is still an open question (*see* [6] and [8] for further reference). In this part, as an appendix, we describe completely the structure of elementary factorizations of $\mathbf{Z}_n$. As a matter of fact, this is an established result (e.g. [3], [7]). Our approach is direct.

Let (H, K) be any elementary factorization of $\mathbf{Z}_n$. Obviously, $0 \in H$ and $0 \in K$. There exists uniquely a biggest integer $d = d(H, K)$ such that either $\{0, 1, ..., d-1\} \subseteq H$ or $\{0, 1, ..., d-1\} \subseteq K$. We always say by convention that $\{0, 1, ..., d-1\} \subseteq K$, hence $1, ..., d-1 \notin H$. Define

$$H \setminus d = \{i : id \in H\},\ K \setminus d = \{i : id \in K\}.$$

The theorem below gives a recursive method for constructing all elementary factorizations of $\mathbf{Z}_n$; (i) and (ii) were proved in [7], (iv) in [3].

THEOREM 2: *Let (H, K) be an elementary factorization of $\mathbf{Z}_n$, then*

(i) *H conttains only multiples of d.*

(ii) *For all $j \in \mathbf{N}$, either $\{jd, jd+1, ..., jd+d-1\} \subseteq K$ or $\{jd, jd+1, ..., jd+d-1\} \cap K = \emptyset$.*

(iii) *$d(H, K)$ is a divisor of n : $d(H, K) | n$,*

(iv) *$(H \setminus d, K \setminus d)$ constitutes a factorization of $\mathbf{Z}_n$, where $q = \dfrac{n}{d(H, K)}$.*

Proof: Actually, (i) and (ii) can be reformulated respectively as follows:

$$A(r) : \forall r \geq 0, \quad 0 \leq \forall s < d : rd + s \in H \Rightarrow s = 0;$$

and

$$B(r) : \forall r \geq 0, \quad 0 \leq \forall i, \quad j < d : rd + i \in K \Rightarrow rd + j \in K,$$

which we handle by induction on r. $A(0)$ and $B(0)$ hold trivially. Suppose now $A(r)$ $B(r)$ hold for all $r \leq l$ we prove them valid for $r = l + 1$.

If $(l+1)d + s \in H$ for some $0 < s < d$, then clearly $n > d$ and $d \in H$. As $s \in K$, we have $(l+1)d \notin H$. Further, the equality

$$(l+1)d + d = (l+1)d + s + (d - s)$$

with d, $(l+1)d+s \in H-\{0\}$ and $d-s \in K-\{0\}$ shows that $(l+1)d \notin K$. Thus, we have the representation

$$(l+1)d = h + k, \quad h > 0, \quad h \in H, \quad k > 0, \quad k \in K.$$

We write $h = rd + t$, $0 \leq t < d$, $r \geq 0$. Since $h < (l+1)d$, we have $r \leq l$ and by $A(r)$ $t = 0$, hence $k = r'd$. Since $k < (l+1)d$, $r' \leq l$, by $B(r')$ we get $r'd + s \in K$. But then the equality

$$(l+1)d + s = h + r'd + s$$

with h, $(l+1)d+s \in H-\{0\}$ and $r'd+s \in K-\{0\}$ yields a contradiction. Thus $s = 0$ and $A(l+1)$ holds.

Next, we prove $B(l+1)$. Suppose that $0 \leq i, j < d$ such that $(l+1)d + i \in K$, $(l+1)d + j \notin K$. Indeed $n > d$ and $d \in H$. In a similar manner as above, from

$$(l+1)d + i \in K$$

and

$$(l+1)d + j + (i - j) = (l+1)d + i$$

if $i > j$, or

$$(l+1)d + j + (d - (j - i)) = d + (l+1)d + i$$

if $j > i$, we conclude that

$$(l+1)d + j \notin H \cup K$$

and as a consequence

$$(l+1)d + j = h + k, \quad h \in H, \quad h > 0, \quad k \in K, \quad k > 0.$$

Consequently, $h = rd + s$, $k = r'd + t$ for

$$r \leq l+1, \quad 0 \leq s < d, \quad r' \leq l+1, \quad 0 \leq t < d.$$

As $h > 0$ then $r > 0$ thus $h \geq d$ and $r' \leq l$. By $B(r')$, $r' d + i \in K$ that leads to

$$(l+1)d + i = h + r' d + i$$

that is quite a contradiction. So $B(l+1)$ holds and (i) and (ii) are proved.

(iii) By (ii) d is a divisor of $d|K \setminus d| = |K|$ that divides $|H|\,|K| = n$. So $d|n$.

(iv) For every $0 \leq i < q = \dfrac{n}{d}$, id is represented uniquely in the form

$$id = rd + ld, \quad rd \in H, \quad ld \in K.$$

Hence i has a unique representation

$$i = r + l, \quad r \in H \setminus d, \quad l \in K \setminus d$$

that means $(H \setminus d,\ K \setminus d)$ is an elementary factorization of $\mathbf{Z}_q$. The proof is completed.

The theorem shows that each elementary factorization of (H, K) is uniquely determined by $d = d(H, K)$ and $(H \setminus d,\ K \setminus d)$. Given any proper divisor d of n and an elementary factorization (H, K) of $\mathbf{Z}_{\frac{n}{d}}$ with $1 \in K$, a simple direct verification shows that $(dK,\ dH + \{0, 1, \ldots, d-1\})$ is the unique elementary factorization of $\mathbf{Z}_n$ with

$(dK \setminus d,\ dH + \{0, 1, \ldots, d-1\} \setminus d) = (H, K)$

and

$$d(dK,\ dH + \{0, 1, \ldots, d-1\}) = d.$$

Thus, all elementary factorizations of $\mathbf{Z}_n$ can be recursively found.

Example 4: We determine all elementary factorizations of $\mathbf{Z}_8$. Clearly, $\mathbf{Z}_1$ possesses only one elementary factorization: $H_0 = \{0\}$, $K_0 = \{0\}$ and $\mathbf{N}_2$ possesses only one elementary factorization: $H_1 = \{0, 1\}$, $K_1 = \{0\}$; $\mathbf{Z}_4$ has two elementary factorizations: $H_2 = \{0, 1, 2, 3\}$, $K_2 = \{0\}$ and $H_3 = \{0, 1\}$, $K_3 = \{0, 2\}$. Therefore $\mathbf{Z}_8$ has the following elementary factorizations: $(H, K) = (\{0\}, \{1, 2, 3, 4, 5, 6, 7\}), (\{0, 4\}, \{0, 1, 2, 3\}), (\{0, 2, 4, 6\}, \{0, 1\}), (\{0, 2\}, \{0, 1, 4, 5\})$ with respectively $d = 8, 2, 2, 2$ and $(H \setminus d,\ K \setminus d) = (H_0, K_0), (H_1, K_1), (H_2, K_2), (H_3, K_3)$.

Note Added in the Final Version. For the case $n = 6$, the code $\{a^6, ba, a^2 ba, a^4 ba, a^3 b, b\}$ is finitely incompletable. Detailed argument will appear elsewhere.

ACKNOWLEDGEMENTS

I would like to thank the referee for his useful information and suggestions, and Do Long Van for critically reading the manuscript and helping improve the presentation.

REFERENCES

1. J. Berstel and D. Perrin, *Theory of Codes,* Academic Press, New York, 1985.
2. V. Bruyère, Limin Wang and Liang Zhang, On Completion of Codes with Finite Deciphering Delay, *European Journal of Combinatorics*, 1990, *16*, pp. 513-521.
3. C. De Felice, Construction of a Family of Finite Maximal Codes, *Theoretical Computer Science*, 1989, *63*, pp. 157-184.
4. C. De Felice and A. Restivo, Some Results on Finite Maximal Codes, *RAIRO Informatique théorique*, 1985, *19*, pp. 383-403.
5. A. Ehrenfeucht and G. Rozenberg, Each Regular Code Is Included in a Regular Maximal Code, *RAIRO Informatique théorique,* 1986, *16*, pp. 89-96.
6. L. Fuchs, *Abelian Groups,* Akadémiai kiadó, Budapest, 1958, Pergamon Press, Oxford-London-New York-Paris, 1960.
7. M. Krasner and B. Ranulac, Sur une propriété des polynômes de la division du cercle, *C.R. Acad. Sci. Paris*, 1937, *240*, pp. 297-299.
8. G. Lallement, *Semigroups and Combinatorial Applications*, John Wiley and Sons, New York, 1979, 1969.
9. Al A. Markov, An Example of Independent System of Words Which Cannot Be Included into a Finite Complete System, *Matematicheskie Zametki*, 1967, *1*, No. 1, pp. 87-90 (in Russian).
10. A. Restivo, On Codes Having No Finite Completions, *Discrete Mathematics*, 1977, *17*, pp. 309-316.
11. A. Restivo, S. Salemi and T. Sportelli, Completing Codes, *RAIRO Informatique théorique,* 1989, *23*, pp. 135-147.