Science Bulletin of NCTU, Vol. V, No. 2

A STUDY ON PERIODIC SEQUENCES

C. C. HSIEH

(Received 12 September in revised form 6 November 1971)

Abstract—*This paper contains two parts. In one part, the minimum length required to identifying two periodic sequences will be formulated. In the other, two methods for decomposing a periodic sequence into two or more periodic sequences which have periods shorter than that of the original sequence will be presented. The theorems and methods derived in this paper may be applied to many fields, such as coding and decoding implementations, data processing, numerical analysis, data compression, etc.*

I. INTRODUCTION

In this paper, two problems associated with periodic sequences will be studied. The first one is to find the minimum number of consecutive digits which is required to identify two periodic sequences. This problem is solved in Section 2 of this paper. The second problem is: for a given periodic sequence, how to decompose it into two or more periodic sequences which have periods shorter than that of the former sequence such that the sum or the logic AND of the later sequences will generate the former one. This problem is treated in Section 3.

The periodic sequences studied in this paper are assumed to have elements over finite field GF(2). Extensions of the theorems presented in this paper to other number systems are possible. Some possible extensions and applications will be summarized in the concluding remarks.

II. IDENTIFICATION OF TWO PERIODIC SEQUENCES

A periodic sequence of finite period n can be expressed as

$$\ldots, a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_0, a_1, \ldots$$

In this paper, we will use

$$S(a)=a_0, a_1, \ldots, a_{n-1}$$

to denote such a periodic sequence, and use p_a to denote the period of $S(a)$. In the above case $p_a=n$. The period of a periodic sequence does not imply it is the minimum "true period" of the sequence. We will use the phrase "true period" to denote the minimum period of a sequence. The subscripts of elements of a periodic sequence are understood to be modular of its period.

[Defination] $S(1)\triangleq$a periodic sequence of all 1's, and $p_1=1$.

$S(0)\triangleq$a periodic sequence of all 0's, and $p_0=1$.

[Defination] $D^rS(a) \triangleq$ a sequence obtained by shifting $S(a)$ r places to its right.

Now let us do some mathematical derivation first.

[Defination] A chain graph is defined as a graph consisting of p nodes and $p-1$ links constructed to form a chain as shown in Figure 1, where the $a_0, a_1, \ldots, a_{p-1}$ are p nodes of the chain graph.

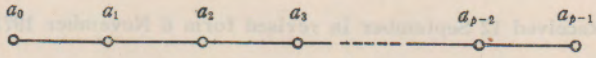

Fig. 1. The general form of a chain graph

The links of a chain define a relation R. Thus, we can write $a_i R a_j$ or $a_i \sim a_j$ if and only if there is a link from a_i to a_j. Let σ be a permutation function on the set $\{a_0, a_1, \ldots, a_{p-1}\}$. Let $\sigma\{a_0, a_1, \ldots, a_{p-1}\} \triangleq \{\sigma(a_0), \sigma(a_1), \ldots, \sigma(a_{p-1})\}$. If the following relations

$$\left.\begin{aligned} &\sigma(a_0) \sim \sigma(a_1) \\ &\sigma(a_1) \sim \sigma(a_2) \\ &\quad\vdots \\ &\sigma(a_{p-3}) \sim \sigma(a_{p-2}) \\ &\sigma(a_{p-2}) \sim \sigma(a_{p-1}) \end{aligned}\right\} \quad (1)$$

are satisfied, then the set $\{a_0, a_1, \ldots, a_{p-1}\}$ and equation (1) will still represent a chain graph.

Now, let a transformation function δ be a mapping from the set $\{a_0, a_1, \ldots, a_{p-1}\}$ into itself by the rule:

$$\left.\begin{aligned} &\delta(a_0) = a_{r-1} \\ &\delta(a_1) = a_{2r-1} \\ &\quad\vdots \\ &\delta(a_{p-1}) = a_{pr-1} \end{aligned}\right\} \quad (2)$$

where r is a positive number and g. c. d. $(p, r) = 1$. Then δ is a permutation function. This will be proved as follows. If for some $i \neq j$ and i, j belong to $\{1, 2, 3, \ldots, p\}$, the equation:

$$a_{ir-1} = a_{jr-1}$$

will imply

$$ir - 1 \equiv jr - 1 \quad \text{where "}\equiv\text{" denotes the congruence relation of modular } p,$$

then we have:

$$(i-j)r = kp \quad \text{for} \quad k = 0, 1, 2, 3, \ldots.$$

Since $(i-j) < p$, and g. c. d. $(p, r) = 1$, the above equation can not be held. Thus. $a_{ir-1} \neq a_{jr-1}$ for any $i \neq j$. Therefore the δ function in equation (2) must satisfy the relations in equation (1). The function δ is a 1—1 and onto mapping, and hence a permutation function.

This can be shown by tracing from $\delta(a_0) \sim \delta(a_1) \sim \delta(a_2) \ldots \sim \delta(a_{p-1})$ by noticing that every node will appear just once, therefore it is a connected graph of p nodes and $p-1$ links, no branch points, and hence a chain graph.

Now by substituting (2) into (1), we have the following equations:

$$\left.\begin{aligned} &a_{r-1}\sim a_{2r-1}\\ &a_{2r-1}\sim a_{3r-1}\\ &\quad\vdots\\ &a_{(p-1)r-1}\sim a_{pr-1}\end{aligned}\right\} \quad (3)$$

Since δ is a permutation function, and note that a_{pr-1} or a_{p-1} does not present at the left side of equation (1), the relation $x_{p-1}\sim x_{r-1}$ will not appear in equation (3). Equation (3) is rearranged as follows:

$$\left.\begin{aligned} &a_0\sim a_r\\ &a_1\sim a_{r+1}\\ &a_2\sim a_{r+2}\\ &\quad\vdots\\ &a_{p-2}\sim a_{p+r-2}\end{aligned}\right\} \quad (4)$$

So far, we have proved the following theorem:

[Theorem 1] The set $\{a_0, a_1, \ldots, a_{p-1}\}$ and equation (4) together will represent a chain graph if g.c.d. $(p, r)=r$ for some positive integer r.

Now, let us go back to periodic sequences.

[Theorem 2] Let $S(a)$ and $S(b)$ be two periodic sequences, and g.c.d. $(p_a, p_b)=1$. Then $S(a)=S(b)$ if $a_i=b_i$ for $i=0,1,2,\ldots,(p_a+p_b-2)$.

[Proof] If $p_a=p_b$, the theorem is trivial. Therefore we assume $p_a>p_b$ and $p_a=kp_b+r$ for $k=1,2,\ldots$; and $r<p_b$.

Step 1:

Construct a graph with $a_0, a_1, \ldots, a_{p_a-1}$, $b_0, b_1, \ldots, b_{p_b-1}$ as nodes and $a_i=b_i$ for $i=1,2,3,\ldots,(p_a-1)$ as links. Note that the relation defined by links is the equality relation. This graph is shown in Figure 2. In Figure 2, we see that there

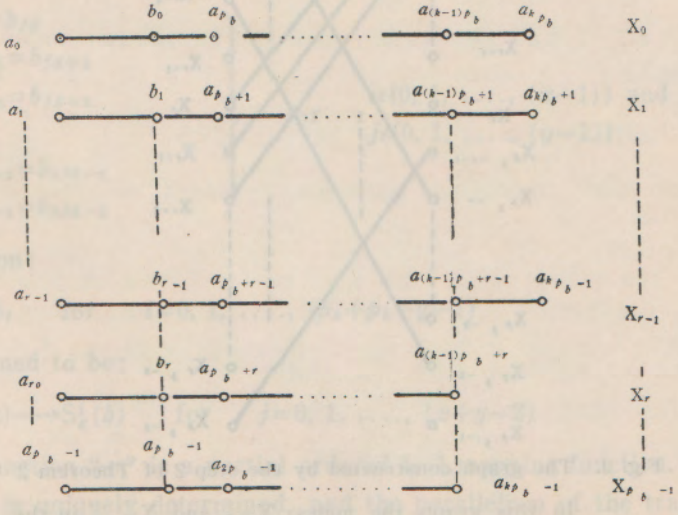

Fig. 2. The graph constructed by the step 1 of Theorem 2

are p_b separated components. For convenience let's denote those p_b components as $X_0, X_1, \ldots, X_{p_b-1}$ with respect to the nodes $b_0, b_1, \ldots, b_{p_b-1}$ respectively.

Step 2:

Now, let us construct another graph by using $X_0, X_1, \ldots, X_{p_b-1}$ as nodes and the relations

$$a_i = b_i \quad \text{for} \quad i = p_b, \ldots, (p_a + p_b - 2)$$

as links. This graph is shown in Figure 3. Since

$$\begin{cases} a_{p_a} = a_0, & a_{p_a+1} = a_1, \quad \ldots, \quad a_{p_a+p_b-2} = a_{p_b-2} \\ b_{p_a} = b_r, & b_{p_a+1} = b_{r+1}, \quad \ldots, \quad b_{p_a+p_b-2} = b_{r-2} \end{cases}$$

the link set can be written as:

$$\begin{aligned} &X_0 = X_r \\ &X_1 = X_{r+1} \\ &\vdots \\ &X_{p_b-2} = X_{r-2} \end{aligned}$$

Since $p_a = k p_b + r$, g. c. d. $(p_b, r) = 1$, so g. c. d. $(p_b, r) = 1$, by applying Theorem 1, the graph in Figure 3 is a connected chain graph.

Now, substituting the components $X_0, \ldots, X_{p_b-1}$ shown in Figure 2 into the graph in Figure 3, we have a connected graph with $p_a + p_b$ nodes and $p_a + p_b - 1$ links. Since the link of the resulting graph represents the equality relation, we have $a_i = b_j = a_j = a_i$ for any i & j, hence $S(a) = S(b)$.

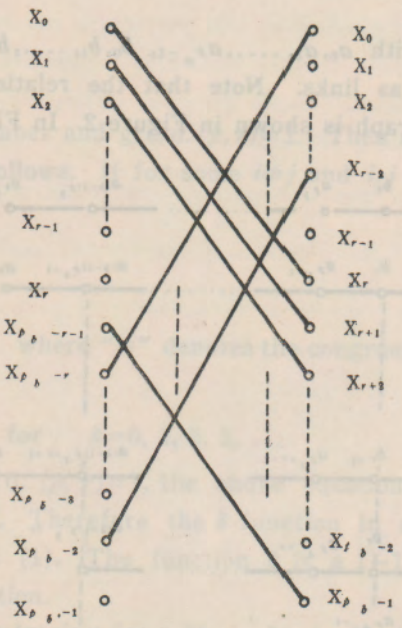

Fig. 3. The graph constructed by the step 2 of Theorem 2
In this graph the nodes, X_{r-1} and X_{p_b-1}, in the right and left column respectively, are not used.

By examining the numbers of nodes and links, we know that p_a+p_b+1 is the necessary number of links for a connected graph of p_a+p_b nodes. Therefore the constraint $a_i=b_i$ for $i=0,1,2,\ldots,(p_a+p_b-2)$ is the necessary condition for $S(a)=S(b)$. An example is given below to illustrate this point.

[Example 1] Let $S(a)=101$, and $S(b)=10110$. Thus, $p_a=3$, $p_b=5$. For the first $p_a+p_b-2=3+5-2=6$ digits, the two sequences are the same:

$$\begin{array}{ll} S(a)=101101 & 1 \\ S(b)=101101 & 0 \\ i=012345 & 6 \end{array}$$

The seventh digital, $i=6$, will show the difference of these two sequences.

[Theorem 3] Let $S(a)$ and $S(b)$ be two periodic sequences and g. c. d. $(p_a,p_b)=g$. Then,

$$S(a)=S(b) \quad \text{if} \quad a_i=b_i \quad \text{for} \quad i=0,\ 1,\ 2,\ \ldots,\ (p_a+p_a-g-1)$$

[Proof] Let $p_a=x\cdot g$, $P_b=y\cdot g$. By grouping g successive terms together, $S(a)$ can be written as follows:

$$\begin{aligned} S(a) &= a_0,\ a_1,\ a_2,\ \ldots,\ a_{p_a-1} \\ &= (a_0, a_1, \ldots, a_{g-1}),\ (a_g, a_{g+1}, \ldots, a_{2g-1}),\ \ldots,\ (a_{(x-1)g}, \ldots, a_{xg-1}) \\ &= S_g^0(a),\ S_g^1(a),\ S_g^2(a),\ \ldots,\ S_g^{x-1}(a) \end{aligned}$$

where $S_g^k(a)=(a_{kg}, a_{kg+1}, \ldots, a_{2kg-1})$ for $k=0,\ 1,\ 2,\ \ldots,\ (x-1)$.

Following the same notation, $S(b)$ can be written as:

$$S(b)=S_g^0(b),\ S_g^1(b),\ S_g^2(b),\ \ldots,\ S_g^{y-1}(b)$$

Now, define a function "$\rightarrow$" operating on $S_g^i(a)$ and $S_g^j(b)$ as follows:

$$S_g^i(a) \longrightarrow S_g^j(b)$$

iff

$$\left.\begin{array}{l} a_{ig}=b_{jg} \\ a_{ig+1}=b_{jg+1} \\ a_{ig+2}=b_{jg+2} \\ \quad\vdots \\ a_{2ig-2}=b_{2jg-2} \\ a_{2ig-1}=b_{2jg-1} \end{array}\right\} \quad \text{for} \quad \begin{array}{l} i\in\{0,\ 1,\ \ldots,\ (x-1)\} \text{ and} \\ j\in\{0,\ 1,\ \ldots,\ (y-1)\} \end{array} \qquad (5)$$

Then, the relation:

$$a_i=b_i \quad \text{for} \quad i=0,\ 1,\ \ldots,\ (p_a+p_b-g-1)$$

can be transformed to be:

$$S_g^j(a) \longrightarrow S_g^j(b) \quad \text{for} \quad j=0,\ 1,\ \ldots,\ (x+y-2) \qquad (6)$$

Note that the function "$\rightarrow$" is a partial ordered 1—1 mapping function. The inverse of this function is uniquely determined, and the parallelism of the transfer will be preserved.

Now let us construct a graph with the set

$$S_g^0(a),\ S_g^1(a),\ \ldots,\ S_g^{x-1}(a) \quad \text{and} \quad S_g^0(b),\ S_g^1(b),\ \ldots,\ S_g^{y-1}(b)$$

to be the nodes and the relation defined in equation (6) to be the links. Since g. c. d. $(x, y)=1$, by Theorem 2, this graph is a chain graph and we have

$$S_g^0 \longrightarrow S_g^1(a) \longrightarrow \ldots \longrightarrow S_g^{x-1}(a) \longrightarrow S_g^0(b) \longrightarrow \ldots \longrightarrow S_g^{y-1}(b) \qquad (7)$$

By inverse transformation of the function "$\rightarrow$", we have the following equations equivalent to equation (7).

$$\left.\begin{aligned} &a_0=a_g=a_{2g}=\ldots=a_{(x-1)g}=b_0=b_g=b_{2g}=\ldots=b_{(y-1)g}\\ &a_1=a_{g+1}=a_{2g+1}=\ldots=a_{(x-1)g+1}=b_1=b_{g+1}=\ldots=b_{(y-1)g+1}\\ &\vdots\\ &a_{g-1}=a_{2g-1}=\ldots=a_{x-1}=b_{g-1}=b_{2g-1}=\ldots=b_{y-1} \end{aligned}\right\} \qquad (8)$$

By inspecting equation (8), $S(a)$ and $S(b)$ both can be expressed as an identical sub-periodic-sequence of period g, namely:

$$(a_{kg},\ a_{kg+1},\ \ldots,\ a_{2kg-1})=(b_{kg},\ b_{kg-1},\ \ldots,\ b_{2kg-1})$$

for $k=0, 1, 2, \ldots$.

Therefore $S(a)=S(b)$. Q. E. D.

In Theorem 3, the condition

$$a_i=b_i \quad \text{for} \quad i=0, 1, \ldots, (p_a+p_b-g-1)$$

is necessary to guarantee that $S(a)=S(b)$. This can be illustrated by the following example.

[Example 2] Let $S(a)=0001$, $p_a=4$ and $S(b)=000100$, $p_b=6$. Thus $g=2$, and $p_a+p_b-g-1=7$. The first p_a+p_b-g digits are:

$$S(a)=0001000\,\vdots\,1\ldots.$$
$$S(b)=0001000\,\vdots\,0\ldots.$$

Therefore, the eighth digit, the (p_a+p_b-g)th digit, will tell the difference between those two sequences.

III. DECOMPOSITION OF PERIODIC SEQUENCES

Firstly, we shall summarize some properties of periodic sequences in the following.

[Defination] The modular sum, logic AND sum and logic OR sum of two sequences are difined as follows

$$S(a)=S(b)\oplus S(c) \quad \text{iff} \quad a_i=b_i\oplus c_i$$
$$S(a)=S(b)\wedge S(c) \quad \text{iff} \quad a_i=b_i\wedge C_i$$
$$S(a)=S(b)\vee S(c) \quad \text{iff} \quad a_i=b_i\vee C_i$$

for $i=0,1,2,\ldots$. where $\oplus$ denotes the modular two sum, $\vee$ denotes the logic OR sum and $\wedge$ denotes the logic AND sum of two elements.

[Theorem 4] Let $S(x)=S(a)\oplus S(b)$. Then $p_a=p_b=m$ implies $p_x\leqq m$ and p_x divides m.

[Definition] The sequence $S(a)$ is complementary symmetric iff $S(a)$ can be expressed as:

$$S(a)=a_0,\ a_1,\ \ldots,\ a_{m-1},\ \bar{a}_0,\ \bar{a}_1,\ \ldots,\ \bar{a}_{m-1}$$

[Theorem 5] Let $S(x)=S(a)\oplus D^rS(a)$ and $p_a=2m$, if $S(a)$ is complementary symmetric then $p_x\leqq m$, for any positive integer r.

[Theorem 6] Let $S(x)=D^0S(a)\oplus D^1S(a)\oplus\ldots\oplus D^{(k-1)}S(a)$, If $p_a=k\cdot r$, then $p_x\leqq k$. The proofs of the above theorems are obvious and thus omitted here.

[Theorem 7] Let $S(x)=S(a)\oplus D^rS(a)$. Let p_a and p_x be the true periods of $S(a)$ and $S(x)$, respectively.

IF g. c. d. $(p_a, r)=1$,

then 1) $p_x=p_a$, whenever $S(a)$ is not complementary symmetric.

2) $p_x=\dfrac{p_a}{2}$, whenever $S(a)$ is complementary symmetric.

[Proof] By applying Theorem 4, it is easly seen that $p_x\leqq p_a$ and p_x divides p_a. Now, for g. c. d. $(p_a, r)=1$, assume $p_x=k$, $p_a=km$ and $m\geqq 1$. Then

$$\left.\begin{aligned} &x_0=x_k\\ &x_1=x_{k+1}\\ &\vdots\\ &x_{mk-1}=x_{(m+1)k-1}\end{aligned}\right\}\quad(9)$$

Since k divides p_a, equation (9) can be grouped into m groups as shown in equation (10).

$$\left.\begin{aligned} &x_0=x_k=x_{2k}=\ldots\ldots\ldots=x_{(m-1)k}\\ &x_1=x_{k+1}=x_{2k+1}=\ldots\ldots=x_{(m-1)k+1}\\ &\vdots\\ &x_{k-1}=x_{2k-1}=\ldots\ldots\ldots=x_{mk-1}\end{aligned}\right\}\quad(10)$$

Substituting $x_i=a_i\oplus a_{i+r}$, for $i=0,1,\ldots,mk-1$, into equation (10) we obtain equation (11).

$$\left.\begin{aligned} &x_0=a_0\oplus a_r=a_k\oplus a_{k+r}=\ldots\ldots\ldots=a_{(m-1)k}\oplus a_{(m-1)k+r}\\ &x_1=a_1\oplus a_{r+1}=a_{k+1}\oplus a_{k+r+1}=\ldots\ldots=a_{(m-1)k+1}\oplus a_{(m-1)k+r-1}\\ &\vdots\\ &x_{k-1}=a_{k-1}\oplus a_{k+r-1}=\ldots\ldots\ldots=a_{mk-1}\oplus a_{mk+r-1}\end{aligned}\right\}\quad(11)$$

Since g. c. d. $(p_a, r)=1$ implies g. c. d. $(k, r)=1$ and g. c. d. $(m, r)=1$, therefore by applying Theorem 1, equation (11) can be rearranged in the form of equation (12).

$$\left.\begin{aligned} &a_0,\ a_r,\ a_{2r},\ \ldots\ldots\ldots\ldots,\ a_{(k-1)r},\ a_{kr}\\ &a_{kr},\ a_{(k+1)r},\ \ldots\ldots\ldots\ldots,\ a_{(2k-1)r},\ a_{2kr}\\ &\vdots\\ &a_{(m-1)kr},\ a_{((m-1)k+1)r},\ \ldots,\ a_{(mk-1)r},\ a_{mkr}\end{aligned}\right\}\quad(12)$$

m rows; k columns

In equation (12), the $(k+1)$th column is equal to the first column, and the elements $a_{(j+i)r}$ and $a_{(j+i+1)r}$ in the $(i+1)$th and $(i+2)$th columns respectively will have a relation $a_{(j+i)r} \oplus a_{(j+i+1)r} = x_i$, for $i=0,1,\ldots,k$ and $j=0,1,\ldots,(m-1)$. Note further that the set $\{a_0, a_r, a_{2r}, \ldots, a_{(mk-1)r}\}$ will be identical to the set $\{a_0, a_1, a_2, \ldots, a_{mkr-1}\}$, and each column is equation (12) is corresponding to a residue class of m.

Now, if the weight of $\{x_0, \ldots, x_{k-1}\}$ is even, all the elements in any one column of equation (12) are equal. This means that the true period of $S(a)$ is k, and $m=1$. If the weight of $\{x_0, x_1, \ldots, x_{k-1}\}$ is odd, the elements in each column of equation (12) is alternating with a period of 2, ie 0101.... or 1010.... therefore $S(a)$ will have a true period equals to $2k$ and $S(a)$ is complementary symmetric. And note in this case, m must be even to ensure $a_{mkr}=a_0$. Therefore p_a must be even and r must be odd. Q. E. D.

[Theorem 8] Let $S(a)=S(a)\oplus D^r S(a)$. Let p_a and p_x be the true periods of $S(a)$ and $S(x)$ respectively. If g. c. d. $(p_a, r)=1$ and g. c. d. $(h, g)=1$ where $h=\frac{p_a}{g}$, then $\frac{p_a}{2g} \leqq p_x \leqq p_a$ and p_x divides p_a.

[Proof] For g. c. d. $(p_a, r)=g$ and g. c. d. $(h, g)=1$, let us suppose $S(a)=S(b)\oplus S(c)$ where $p_b=h$ and $p_c=g$. Then, we can write

$$S(x)=S(a)\oplus D^r S(a)=S(b)\oplus S(c)\oplus D^r(S(b)\oplus S(c)$$
$$=[S(b)\oplus D^r S(b)]\oplus[S(c)\oplus D^r S(c)]$$

Since g divides r, $S(c)\oplus D^r S(c)=S(0)$. Therefore, we have

$$S(x)=S(b)\oplus D^r S(b)$$

By applying the previously derived result, $S(b)+D^r S(b)$ may have a true period $\geqq h/2$. In case of $p_x=h/2$, $S(b)$ must be complementary symmetric.

If $S(a)\neq S(b)\oplus S(c)$ for any $S(b)$ and $S(c)$, p_x will be p_a or $p_a/2$. In case of $p_x=p_a/2$, $S(a)$ must be complementary symmetric. If $p_x<p_a/2$, these always exists a certain $S(c)$ and $S(b)$ such that $S(a)=S(b)\oplus S(c)$. This contradiction conclude our proof of this theorem. Q. E. D.

The proofs of Theorem 7 and Theorem 8 are constructive. They can be used to decompose a periodic sequence. Let $S(a)$ be given and we want to find $S(b)$ and $S(c)$ such that $S(a)=S(b)\oplus S(c)$. If p_b is known, we can compute $S(a)\oplus D^{p_b} S(a)=S(x)$ and use Theorem 7 and Theorem 8 to check p_x. If $p_x=p_a$, the decomposition is impossible because $p_c \geqq p_x$. If we find p_x satisfactory, we can solve

$$S(c)\oplus D^{p_b} S(c)=S(x)$$

for $S(c)$ and then, substract $S(c)$ from $S(a)$, $S(b)$ can be found. This method is illustracted in the following example.

[Example 4] Given $S(a)=00111101001001011110$ and $p_a=20$. We want to find $S(b)$ and $S(c)$ satisfying

$$S(a)=S(b)\oplus S(c).$$

Since $20=5\times4$, let us first compute

$$S(x)=S(a)+D^4S(a)=\underbrace{11011}\,\underbrace{11011}\,\underbrace{11011}\,\underbrace{11011}$$

$\because\ p_x=5$,

we can solve the following equations for $S(c)$.

$$\begin{aligned}
&b_a+b_1=1\\
&b_1+b_2=1\\
&b_2+b_3=0\\
&b_3+b_4=1\\
&b_4+b_0=1
\end{aligned}$$

and we obtain $S(c)=\begin{cases}10110\\01001\end{cases}$, or by computing $S(b)=S(a)+S(b)$ we find two sets of solutions $\begin{cases}S(b)=1000\\S(c)=10110\end{cases}$ and $\begin{cases}S(b)=0111\\S(c)=01001\end{cases}$.

[Theorem 9] Let $S(a)$ be a periodic sequence. Assume $p_a=xy$ and g.c.d. $(x,y)=1$. Let $S(a)$ be arranged as follows:

$$\left.\begin{array}{lllll}
 & X^0 & X^1 & \cdots. & X^{x-1}\\
S_x^0(a)= & (a_0, & a_1, & \cdots., & a_{x-1})\\
S_x^1(a)= & (a_x, & a_{x+1}, & \cdots., & a_{2x-1})\\
\vdots & & & & \\
S_x^{y-1}(0)= & (a_{(y-1)x}, & a_{(y-1)x+1}, & \cdots., & a_{xy-1})
\end{array}\right\}\quad(13)$$

$$\left.\begin{array}{lllll}
 & Y^0 & Y^1 & \cdots. & Y^{y-1}\\
S_y^0(a)= & (a_0, & a_1, & \cdots., & a_{y-1})\\
S_y^1(a)= & (a_y, & a_{y+1}, & \cdots., & a_{2y-1})\\
\vdots & & & & \\
S_y^{x-1}(a)= & (a_{(x-1)y+1}, & a_{(x-1)y+1}, & \cdots., & a_{xy-1})
\end{array}\right\}\quad(14)$$

where X's and Y's denote the columns of each array. Then we can always find two unique periodic sequences $S(b)$ and $S(c)$ such that

$$S(a)=S(b)\wedge S(c)\quad\text{and}\quad P_b=x,\ p_c=y$$

where $S(b)=S_x^0(a)\vee S_x^1(a)\vee\cdots.S_x^{y-1}(a)$.
$S(c)=S_y^0(a)\vee S_y^1(a)\vee\cdots.S_y^{x-1}(a)$,

Iff the following conditions are satisfied:

1) All the non-zero columns of X's have the same weight which is equal to the weight of $S(c)$.
2) All the non-zero columns of Y's have the same weight which is equal to the weight of $S(b)$.

[Proof] Following pre-defined notation, let

$$\left.\begin{aligned}
&S(a)=a_0,\ a_1,\ \cdots.,\ a_{p_a-1}\\
&S(b)=b_0,\ b_1,\ \cdots.,\ b_{x-1}\\
&S(c)=c_0,\ c_1,\ \cdots.,\ c_{y-1}
\end{aligned}\right\}\quad(15)$$

If $S(a)=S(b)\wedge S(c)$, we have

$$a_k=b_k\wedge c_k \quad \text{for} \quad k=0, 1, 2, \ldots, (p_a-1) \tag{16}$$

Since the subscripts of b's are modular x and those of c's are modular y, equation (14) may be written as

$$a_k=b_i\wedge c_j$$

where $k=\alpha x+i=\beta y+j$ for $0\leqq i\leqq(x-1)$, $0\leqq j\leqq(y-1)$,

and α, β are non-negative integers.

By appling Theorem 1, since g. c. d. $(x, y)=1$, the pairs $(b_k, c_k)\neq(b_l, c_l)$ for $k\neq l$ within the range $0\leqq k\leqq(p_a-1)$, $0\leqq l\leqq(p_a-1)$. Therefore, a_k is uniquely determined by $b_i\cdot c_j$. Thus we can write

$$a_k\triangleq a_{(i,j)}$$

and $a_k=1$ iff $b_i\wedge c_j=1$,

$$a_k=0 \quad \text{iff} \quad b_i\wedge c_j=0 \quad \text{for} \quad k=0, 1, \ldots, (p_a-1) \tag{17}$$

Now, let us construct a table us shown in Figure 4.

	b_0	b_1	.....	b_{x-1}
c_0	$a_{(0,0)}$	$a_{(1,0)}$	.....	$a_{(x-1,0)}$
c_1	$a_{(0,1)}$			
	⋮	⋮		
c_{y-1}	$a_{(0,y-1)}$	$a_{(1,y-1)}$	.....	$a_{(x-1,y-1)}$

Fig. 4

In this table, the set of entries $\{a_{(00)}, \ldots, a_{(x-1,y-1)}\}=\{a_0, a_1, \ldots, a_{p_a-1}\}$. For a given sequence $S(a)$ and x, y, that table can always be constructed.

Now, since any entry $a_{(i,j)}=1$ implies $b_i=c_j=1$, we may find a set of values for $(b_0, b_1, \ldots, b_{x-1})$ by Oring up all the rows in the table, and a set of values for $(c_0, c_1, \ldots, c_{y-1})$ by Oring up all the columns.

Note that the 1st and 2nd subscripts of entries in the above table are arranged according to the residue classes of x and y respectively. This means the a's in the $(i+1)$th column will have subscripts which belong to the ith residue class with respect to x, so are the rows. Therefore, by referring to equations (13) and (14), we have

$$S(b)=(b_0, \ldots, b_{x-1})=S_x^0(a)\vee S_x^1(a)\vee \ldots \vee S_x^{y-1}(a)$$

$$S(c)=(c_0, \ldots, c_{y-1})=S_y^0(a)\vee S_y^1(a)\vee \ldots \vee S_y^{x-1}(a)$$

Now, we have found a set of values for $S(b)$ and $S(c)$. Since $b_i\wedge c_j=1$ implies $a_{(i,j)}=a_k=1$, therefore as we check $S(b)$ and $S(c)$ for $S(a)$, the table's entries should not be changed in order to hold the relation $S(a)=S(b)\wedge S(c)$. This agreement can be obtained iff the following conditions are satisfied:

1) for all non-zero columns, their weights are the same,
2) for all non-zero row's, their weights are the same, and
3) the weight of $s(b)$ is equal to the weight of rows and the weight of $s(c)$ is equal to the weight of columns. (S-1)

To prove the above statement being correct, all we have to do is to prove (S-1) will lead to a statement as follows:

All the entries in the table of Figure 4 is 1 except those in zero columns and zero rows.

Since this proof is trivial, it is omitted. Q. E. D.

[Example 5] $S(a)=1100110101011001110$, $p_a=20$. Let $x=4$, $y=5$. Arrange $S(a)$ to the form of equation (13), we have

$$\left.\begin{array}{r} 1100 \\ 1101 \\ 0101 \\ 1001 \\ \vee)\ 1101 \end{array}\right\} \text{all non-zero columns have weight}=4$$

$$S(b)\ \ 1101 \qquad \text{weight of } S(b)=3$$

Arrange $s(b)$ to the form of equation (14), we have

$$\left.\begin{array}{r} 11001 \\ 10101 \\ 01100 \\ \vee)\ 11101 \end{array}\right\} \text{all non-zero columns have weight}=3$$

$$S(c)=11101 \qquad \text{weight of } S(c)=4$$

By cheching those weights, we find the conditions of Theorem 8 are satisfied. Therefore $S(a)=S(b)\wedge S(c)$.

[Theorem 10] Let $S(a)$ be a periodic sequence. Assume $p_a=xyg$ and g. c. d. $(x, y)=1$. Let $S(b)$ and $S(c)$ have periods $p_b=xg$ and $p_c=yg$. Then

$$S(a)=S(b)\wedge S(c)$$

iff the following conditions are satisfied

$$\left.\begin{array}{ll} & R_g^i(a)=R_g^i(b)\wedge R_g^i(c) \quad \text{for} \quad i=0, 1, \ldots, (g-1) \\ \text{where} & R_g^i(a)=a_i, a_{i+g}, \ldots, a_{i+(ky-1)g}, \\ & R_g^i(b)=b_i, b_{i+g}, \ldots, b_{i+(x-1)g}, \quad \text{and} \\ & R_g^i(c)=c_i, c_{i+g}, \ldots, c_{i+(y-1)g} \end{array}\right\} \quad (18)$$

are periodic sequences. Besides, the expression $s(a)=s(b)\wedge s(c)$ will be unique if $R_g^i(a)\neq S(0)$ for any $i=0, 2, \ldots, (g-1)$. If there are m i's such that $R_g^i(a)=S(0)$ then there exist $(2^x+2^y-1)^m$ pairs of different $S(b)$ and $S(c)$ satisfying $S(a)=S(b)\wedge S(c)$.

[Proof] Following the notations used in proving Theorem 9, for $S(a)=S(b)\wedge S(c)$, we have

$$a_k=b_k\wedge c_k \quad \text{for} \quad k=0, 1, \ldots, (p_a-1) \qquad (19)$$

Since g. c. d. $(p_b, p_c)=g$, b_k and c_k can be divided into g disjoint sets by grouping the subscripts of b's and c's with respect to a residue class of g. Because $a_k=a_{(i,j)}$, therefore, a's will also follow the b's and c's. Mathematically, after this grouping process, we have the following subsequences:

$$\left.\begin{aligned} &R_g^0(a)=a_0,\ a_g,\ a_{2g},\ \ldots\ldots,\ a_{(xy-1)g}\\ &\vdots\\ &R_g^{g-1}(a)=a_{g-1},\ a_{2g-1},\ \ldots\ldots,\ a_{xyg-1}\end{aligned}\right\} \quad (20)$$

$$\left.\begin{aligned} &R_g^0(b)=b_0,\ b_g,\ \ldots\ldots\ldots,\ b_{(x-1)g}\\ &\vdots\\ &R_g^{g-1}(b)=b_{g-1},\ b_{2g-1},\ \ldots\ldots,\ b_{xg-1}\end{aligned}\right\} \quad (21)$$

$$\left.\begin{aligned} &R_g^0(c)=c_0,\ c_g,\ \ldots\ldots\ldots,\ c_{(y-1)g}\\ &\vdots\\ &R_g^{g-1}(c)=c_{g-1},\ c_{2g-1},\ \ldots\ldots,\ c_{yg-1}\end{aligned}\right\} \quad (22)$$

Now, we have g independent classes, namely

$$\{R_g^i(a),\ R_g^i(b),\ R_g^i(c)\} \quad \text{for} \quad i=0,\ 1,\ \ldots\ldots,\ (g-1) \qquad (23)$$

By expanding the scale g times, Theorem 9 can be applied to all classes in equation (23). If $R_g^i(a)\neq S(0)$ for $i=1,2,\ldots\ldots,(g-1)$, Theorem 9 assures the expression is unique. If, for some i, $R_g^i(a)=S(0)$, then either $R_g^i(b)$ or $R_g^i(c)$ or both must be $S(0)$. For $R_g^i(b)=S(0)$, there are 2^y possible values for $R_g^i(c)$. For $R_g^i(c)=0$, there are 2^x possible values for $R_g^i(b)$. Therefor, for any one i such that $R_g^i(a)=S(0)$, we will have total 2^x+2^y-1 pairs of solutions. As a consequence, for m i's such that $R_g^i(a)=S(0)$, we will have $[2^x+2^y-1]^m$ pairs of $S(b)$ and $S(c)$ satisfying $S(a)=S(b)+S(c)$.

[Example 11] $S(a)=1000101000001000101000000100010$, $p_a=30$. Find $S(b)$ and $S(c)$ for $p_b=6$, $p_c=15$ such that $S(a)=S(b)\wedge S(c)$. Solution

$$\because \text{ g. c. d. } (p_a, p_b)=3, \quad \therefore \quad x=2,\ y=5.$$

1) $R_g^0(a)=1010101010$

By applying Theorem 8, we have

```
  10          10101
  10      ∨)  01010
  10          -----
  10          11111
  10
∨)10
-----
  10
```

The relations between the weights are satisfied, so

$$(b_0, b_3)=(1, 0),$$

$$(c_0, c_3, c_6, c_9, c_{12})=(11111)$$

2) $R_g^1(a)=0100010001$

$$\begin{array}{r} 01 \\ 00 \\ 01 \\ 00 \\ +)\ 01 \\ \hline 01 \end{array} \qquad \begin{array}{r} 01000 \\ 10001 \\ +)\ 11001 \\ \hline 11001=(c_1, c_4, c_7, c_{10}, c_{13}) \end{array}$$

3) $R_g^2(a)=000000000$

Therefore, as $(b_2, b_5)=(0,0)$, $(c_2, c_5, c_8, c_{11}, c_{13})$ may have $2^5=32$ possible values. As $(c_2, c_5, c_8, c_{11}, c_{13})=(0,0,0,0,0)$, (b_2, b_5) may have 4 different values. There are total $2^5+2^2-1=35$ pairs of solutions.

From 1), 2) and 3), we have the solution as follows:

$$S(b)=10\text{◊}01\text{◊}$$

$$S(c)=11\text{◊}11\text{◊}10\text{◊}10\text{◊}11\text{◊}$$

where ◊ means optional element subjected to the constrain: either in $S(b)$ or $S(a)$ all optional elements are equal to zero.

IV. CONCLUSION

Theorem 2 is rather a general theorem. It is good for any number system. The theorems deal with decomposition of periodic sequences which may be applied to many number systems with a slight modification required. Those theorems may also be used to decompose finite non-periodic sequences[1,3]. Theorem 9 and Theorem 10 can be used to find $S(b)$ and $S(c)$ such that $S(a)=S(b)\vee S(c)$ for a given $S(a)$, because $\overline{S(a)}=\overline{S(b)}\wedge\overline{S(c)}=\overline{S(b)}\vee\overline{S(c)}$.

One direct application of sequence decomposition is in the data compresion field. Theorem 7 is closely related to generation of sequences by using linear feed back shift-registers[1]. It may be applied to implement some coding and decoding networks. The method shown in Theorems 9 and 10 may extend to formulate $S(a)=f(S(b), S(c))$. For instance, it may be modified to find $S(b)$ and $S(c)$ such that $S(b)\cdot S(c)=S(a)$, where "·" is the componentwise multiplication operator and $S(a)$, $S(b)$ and $S(c)$ are sequences over ordinary number system.

ACKNOWLEDGEMENT

The author would like to thank professor C. L. Liu for his helpful suggestions and constant encouragement.

REFERENCES

1. J. E. Massey, "Shift-register Synthesis and BCH Decoding" IEEE Transactions on Information Theory Vol. IT-15, No. 1, January 1969.
2. Ore; Graph Theory and its application.
3. R. J. Nelson, Introduction To Automata, 1968.