No. 42
79-6

Switching Functions Constructed by Galois Extension Fields

June 1979

Iwaro Takahashi

University of Tsukuba

list of symbols

$x \in K$: element x belongs to set K

$L \supseteq K$: set L includes set K

$|K|$: the size of set K

GF(q): Galois(or finite) field of size q

$GF(2^m)$: extention field of order m over GF(2)

$j \equiv k \pmod{n}$: integers j and k have the same residue if they are divided by n

number of pages 15

number of tables 5

running heads

1. Introduction
2. The reduction to one function
3. Complex analysis in information processing
4. Frobenius cycles in switching functions
5. Computational procedure

A1. General theorems in Galois switching functions

A2. Computations in Galois fields

Abstruct

Every digital information processing is essentially represented by a set of n functions of m variables on $\{0,1\}$. We propose a method to reduce such a set of functions to one polynomial of one variable on $GF(2^N)$ (extension field over GF(2)). Such polynomials have remarkable properties based on Frobenius-transforms, which are to serve for effective designs and productions of switching circuits.

1. Introduction

We can say that with appropriate coding systems every digital information processing is essentially to determine the set of functions

$$y_j = f_j(x_0, x_1, \ldots, x_{m-1}),\ j=0,1,\ldots,n-1\ ,\ x_i, y_j \in \{0,1\}\ . \quad (1.1)$$

It is well known that given a truth table, say table I, we can construct the set of Boolean functions $f_j(x_0,x_1,x_2)$ $(j=0,1)$ representing the truth table. These are $n(=2)$ functions on $m(=3)$ variables.

We propose a method to construct one function on one variable representing any given truth table, by introducing extension fields over GF(2) (§2,§3). Further we show that the function (a kind of switching function) has a remarkable property based on Frobenius cycles in extension fields (§4). This will serve to designs or productions of switching circuits for various digital information processings.

2. The reduction to one function

For brevity first we treat the case $m=n$ in (1.1). In this case we can take both $x=(x_0,\ldots,x_{m-1})$ and $y=(y_0,\ldots,y_{n-1})$ as elements in $GF(2^n)$, the extension field of order n over GF(2). And we can reduce (1.1) to

$$y = f(x),\quad x,y \in GF(2^n)\ . \quad (2.1)$$

Then, as a special case of theorem 3 or theorem 6, we have

Theorem 1 Any function f(x) on $GF(2^n)$ can be represented as a polynomial of order $r=2^n-1$, that is

$$f(x) = a_0+a_1x+\ldots+a_rx^r,\quad a_i \in GF(2^n)\ . \quad (2.2)$$

And the coefficients $a_i(i=0,\ldots,r)$ are determined by

$$a_0 = f(0)$$
$$a_i = \sum_{x \in GF(2^n)} x^{r-i} f(x) , \quad 1 \leqslant i \leqslant r \qquad (2.3)$$

(note that $x^0=1$ even if $x=0$) -----

Every non zero element of $GF(2^n)$ can be represented by a power α^j of a primitive element α (of $GF(2^n)$), and at the same time this can be written by a polynomial of α

$$x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1} , \quad x_i \in GF(2) \qquad (2.4)$$

if the minimal polynomial over GF(2) of α is given. Thus we can take the set of coefficients of (2.4) $(x_0,x_1,\ldots,x_{n-1})$ as a content of the truth table.

Eample 1 A truth table (a correspondence (x_0,x_1,x_2) to (y_0,y_1,y_2)) is given in table II. Let α be the primitive element of $GF(2^3)$ and $\alpha^3+\alpha+1$ be the minimal polynomial of α. Then α^j can be represented as left hand of table II. And the switching function $y=f(x)$ of table II can be written as

table II

$$f(x)= 1+\alpha^2x+\alpha x^2+\alpha x^3+\alpha^3x^4+\alpha^2x^6 \qquad (2.5)$$

($a_0=\alpha^0=1$, $a_1=\alpha^2$, $a_2=\alpha$, $a_3=\alpha$, $a_4=\alpha^3$, $a_5=0$, $a_6=\alpha^2$, $a_7=0$)

by theorem 1. (In table II (000) is represented by α^∞ formaly.)

3. Complex analysis in information processing

The following theorem is a well known result on finite fields theories, so the proof can be omitted (see for example [1]).

Theorem 2 $GF(2^N)$ has one and only one subfield $GF(2^M)$ iff $M|N$ (M divides N). And if α is a primitive element of the $GF(2^N)$ then

$$\beta = \alpha^v, \quad v= (2^N-1)/(2^M-1) \qquad (3.1)$$

is a primitive element of the $GF(2^M)$. -----

Based on the above theorem we can proceed to the general case where m is not necessarily equal to n. In this case instead of (2.1) we have

$$y = f(x), \quad x \in GF(2^m), \quad y \in GF(2^n) . \tag{3.2}$$

Let l be the least common multiple of m and n, and consider a $GF(2^l)$, then the $GF(2^l)$ has the unique $GF(2^m)$ and $GF(2^n)$ in itself . Thus we have

Theorem 3 Any function f(x) in (3.2) can be represented as the polynomial

$$f(x) = a_0 + a_1 x + \ldots + a_r x^r \quad (r = 2^m - 1) \tag{3.3}$$
$$x \in GF(2^m), \quad f(x) \in GF(2^n), \quad a_i \in GF(2^l) \quad (0 \leqslant i \leqslant r)$$

where coefficients a_i (i=0,...,r) are determined by

$$a_0 = f(0)$$
$$a_i = \sum_{x \in GF(2^m)} x^{r-i} f(x) , \quad 1 \leqslant i \leqslant r . \tag{3.4}$$

The proof of this theorem will be stated in §A1. Formally theorem 3 is almost same as theorem 1, but the meaning of the former are quite new. $x \in GF(2^m)$ and $y \in GF(2^n)$ are (coded) informations about the real world, ~~that is these are in an imaginary~~ but $a_0, a_1, \ldots, a_r \in GF(2^l)$ have no longer any meanings of the real world, that is these are in an imaginary world. Thus the informations about real world are to be processed through an imaginary world. In this sence theorem 3 might be called a kind of complex analysis in information processing theories.

Example 2 A truth table is given in table III with m=3, n=2. Thus l must be 6, and let α be a primitive element in $GF(2^6)$ and its minimal polynomial (over GF(2)) be $\alpha^6 + \alpha + 1$. Then $\beta = \alpha^9$ and

table II

$\gamma=\alpha^{21}$ are primitive elements in $GF(2^3)$ and $GF(2^2)$ respectively, and minimal polynomials (over GF(2)) of β and γ will be easily found as $\beta^3+\beta^2+1$ and $\gamma^2+\gamma+1$ respectively. Thus every content in truth table is represented by β^i or γ^j such as in table Ⅲ.

By (3.4) we can calculate the coefficients $a_i(i=0,\ldots,7)$ and construct the desired function

$$y=f(x)=\alpha^{43}x+\alpha^{58}x^2+\alpha^{39}x^3+\alpha^{46}x^4+\alpha^{30}x^5+\alpha^{57}x^6 \qquad (3.5)$$

Example 3 Truth table is given in table Ⅳ (m=4, n=2). In this case l=m=4 and let α be a primitive element of $GF(2^4)$ and its minimal polynomial be $\alpha^4+\alpha+1$. Thus $\beta=\alpha^5$ is primitive in $GF(2^2)$ and its minimal polynomial is $\beta^2+\beta+1$. Like (3.5) we can construct the desired function

$$y=f(x)=\alpha x+\alpha^6x^3+\alpha^4x^4+\alpha^7x^6+\alpha^{13}x^9+\alpha^9x^{12} \qquad (3.6)$$

4. Frobenius cycles in switching functions

Polynomials in theorem 3, say (3.5) and (3.6), have remarkable properties connected with Frobenius cycles. This is based on the following theorem fundamental on finite fields.

Theorem 4 Let $L=GF(q^l)$ be an extension field of $K=GF(q)$ (q being an prime power). Any $\theta\in L$ is in K iff

$$\theta^q=\theta \qquad (4.1)$$

proof First let $\theta\in K$. If $\theta=0$ then clealy $\theta^q=\theta$, so let us consider the case $\theta\neq0$. Let $K^*=K-\{0\}=\{\theta,\theta_2,\theta_3,\ldots,\theta_{q-1}\}$, and if $\theta_i\neq\theta_j$ then $\theta\theta_i\neq\theta\theta_j$, so $\{\theta^2,\theta\theta_2,\theta\theta_3,\ldots,\theta\theta_{q-1}\}$ is equal to K^*. So we have $\theta\theta_2\theta_3\ldots\theta_{q-1}=\theta^2(\theta\theta_2)(\theta\theta_3)\ldots(\theta\theta_{q-1})$, therfore $\theta^{q-1}=1$, that is θ satisfies (4.1).

Conversely let us assume that $\theta \in L$ satisfies (4.1). Let α be a primitive element of L, then θ can be written as

$$\theta = a_0+a_1\alpha+\ldots+a_{l-1}\alpha^{l-1} \quad , \quad a_i \in K \quad . \tag{4.2}$$

Thus taking q-th power of (4.2) we have

$$\theta = a_0+a_1\alpha^q+\ldots+a_{l-1}\alpha^{(l-1)q}$$

because of (4.1) and the fact that q=0 in L. Continuing this procedure up to $q^{(l-1)}$-th power, we have

$$\theta = a_0+a_1\alpha^{q^2}+\ldots+a_{l-1}\alpha^{(l-1)q^2}$$

$$\ldots$$

$$\theta = a_0+a_1 q^{l-1}+\ldots+a_{l-1}(l-1)q^{l-1} .$$

Subtracting (4.2) from each of these formulae, we have

$$\begin{aligned}
0 &= a_1(\alpha^q-\alpha)+\ldots+a_{l-1}(\alpha^{(l-1)q}-\alpha^{l-1}) \\
0 &= a_1(\alpha^{q^2}-\alpha)+\ldots+a_{l-1}(\alpha^{(l-1)q^2}-\alpha^{l-1}) \\
&\ldots \\
0 &= a_1(\alpha^{q^{l-1}}-\alpha)+\ldots+a_{l-1}(\alpha^{(l-1)q^{l-1}}-\alpha^{l-1}) .
\end{aligned} \tag{4.3}$$

The determinant of the coefficient matrix $(\alpha^{iq^j}-\alpha^i)$ is equal to the so called Van der Monde determinant, which is well known to be not equal to zero. Thus we have $a_1=\ldots=a_{l-1}=0$, so $\theta=a_0 \in K$. -----

In general, when a finite field L has a subfield K ($\subseteq$L), the transformation

$$\theta \longrightarrow \theta^q \quad \text{for any } \theta \in L \quad (|K|=q) \tag{4.4}$$

is called K-Frobenius transformation. Thus theorem 4 states that $\theta \in$L is invariant by K-Frobenius transformation iff $\theta \in K$. Further $\{\theta,\theta^q,\theta^{q^2},\ldots,\theta^{q^{i-1}}\}$ is called a K-Frobenius cycle if $\theta^{q^i}=\theta$ and $\theta^{q^j} \neq \theta$ for j<i, and the sum of whole elements of a K-Frobenius cycle

including θ is called a trace of θ and written as

$$tr(\theta)= \theta+\theta^q+\theta^{q^2}+\ldots+\theta^{q^{i-1}} . \tag{4.5}$$

Clealy $tr(\theta^{q^j})=tr(\theta)$.

Theorem 5 Let $GF(2^n)=GF(q)=K$, then coefficiemts $a_o,a_1,\ldots,a_r$ in (3.3) satisfy the following condition

$$a_j= a_i^q \iff j= iq \ (\mathrm{mod}(2^m-1)) \quad (\iff \text{means iff}) \tag{4.6}$$

Specifically we have

$$a_o^q= a_o \tag{4.7}$$

proof Let us take L and K as $GF(2^1)$ and $GF(2^n)$ in theorem 3 respectively. For any $x(\in GF(2^m))$ $f(x)\in GF(2^n)$, so from theorem 4 we have $f(x)^q=f(x)$, that is

$$a_o^q+a_1^q x^q+a_2^q x^{2q}+\ldots+a_r^q x^{rq}= a_o+a_1x+a_2x^2+\ldots+a_rx^r \tag{4.8}$$

For $x\in GF(2^m)$ we have

$$x^k= x^i \iff k=i \ (\mathrm{mod}(2^m-1)) ,$$

so from (4.8) we have (4.6). -----

From theorem 5 we can say that if a_ix^i is a term in (3.3) then its GF(q)-Frobenius transform $a_i^q x^{iq}$ can also be found in (3.3) $(q=2^n)$, consequently whole terms in (3.3) are decomposed into several GF(q)-Frobenius cycles.

Example 4 All terms in (3.5) are decomposed into two $GF(2^2)$-Frobenius cycles

$$\{x, x^4, x^{16}\}, \{x^3, x^{12}, x^{48}\}, \{x^7, x^{28}, x^{112}\},$$

$$\{\alpha^{43}x, \alpha^{46}x^4, \alpha^{58}x^2\}, \{\alpha^{39}x^3,\alpha^{30}x^5,\alpha^{57}x^6\} . \tag{4.9}$$

Thus f(x) in (3.5) can be written as

$$f(x)= tr(\alpha^{43}x)+tr(\alpha^{39}x^3) \tag{4.10}$$

Example 5 All terms in (3.6) are decomposed into three $GF(2^2)$-Frobenius cycles

$$\{\alpha x, \alpha^4 x^4\},\ \{\alpha^6 x^3, \alpha^9 x^{12}\},\ \{\alpha^7 x^6, \alpha^{13} x^9\}\ . \qquad (4.11)$$

Thus f(x) in (3.6) can be written as

$$f(x) = \mathrm{tr}(\alpha x) + \mathrm{tr}(\alpha^6 x^3) + \mathrm{tr}(\alpha^7 x^6)\ . \qquad (4.12)$$

Thus instead of (3.5) and (3.6) we have only to bear (4.10) and (4.12) respectively, in order to find values of f(x) for given x. By this we can remarkably reduce the size of memory and amounts of calculations of coefficients of desired polynomials.

5. Computational procedure

In actual computation, say in table I or table III, given $(x_0, x_1, x_2)(=x)$ we are to find corresponding (y_0, y_1) by calculations in (4.10). These procedures are as follows;

i) find β^i corresponding to (x_0, x_1, x_2). It is PE-transform (§A2.).

In our case it requres about $2^m/m$ memories and only a little amounts of computations, or 2^m (at maximum) units of computations without memories (§A2.)

ii) find $x = \beta^i = \alpha^{9i} = \alpha^j$

iii) find two arguments

$$\alpha^{43} x = \alpha^{43+j} = \alpha^r\ ,\quad \alpha^{39} x^3 = \alpha^{39+3j} = \alpha^s \qquad (5.1)$$

of function tr() in (4.10).

iv) calculate $\mathrm{tr}(\alpha^r)$ and $\mathrm{tr}(\alpha^s)$ and take the sum of them to get (y_0, y_1).

For iv) it is necessary to get the minimal polynomial of α over $GF(2^n)$. In our case, it is easily found to be

$$\alpha^3 + \alpha^2 + \gamma^2\alpha + \gamma \qquad (5.2)$$

Thus for example if $(x_0,x_1,x_2)=(1,1,0)$ is given, this is found to be β^5 by PE-transform. $x=\beta^5=\alpha^{45}$.

$\alpha^{43}x = \alpha^{43+45} = \alpha^{25}$, $\quad \alpha^{39}x^3 = \alpha^{39+135} = \alpha^{48}$

$$\begin{aligned} tr(\alpha^{25}) &= \alpha^{25}+\alpha^{37}+\alpha^{22} \\ &= (\gamma^2+\gamma\alpha+\gamma^2\alpha^2) + (1+\gamma^2\alpha^2) + \gamma\alpha \quad (\text{EP-transform by (5.2)}) \\ &= \gamma \end{aligned}$$

$$\begin{aligned} tr(\alpha^{48}) &= \alpha^{48}+\alpha^{3}+\alpha^{12} \\ &= (\gamma^2+\gamma^2\alpha)+(\gamma+\gamma^2\alpha+\alpha^2)+(1+\alpha^2) \quad (\text{EP-transform by (5.2)}) \\ &= 0 . \end{aligned}$$

Thus $f(x)= tr(\alpha^{25})+tr(\alpha^{48})= \gamma =(0,1)=(y_0,y_1)$.

A1. General theorems in Galois switching functions

Here as a generalization of theorem 1 we will demonstrate the following theorem on a general Galois field GF(q) (q being a prime power).

Theorem 6 Any function on GF(q)

$$y= f(x) \ , \quad x,y \in GF(q) \tag{A1.1}$$

can be represented by a polynomial of order r=q-1

$$f(x)= a_o-a_1x-a_2x^2-\ldots-a_rx^r \ , \ r=q-1, \ a_i \in GF(q) \ , \tag{A1.2}$$

where

$$a_o= f(0) \ , \ a_i= \sum_{t \in GF(q)} t^{r-i}f(t) \ , \ 1 \leqslant i \leqslant r \tag{A1.3}$$

proof It suffices to show that if we put $a_i (0 \leqslant i \leqslant r)$ calculated by (A1.3) for any given function f() on GF(q) into the right hand of (A1.2) then the value of the latter is equal to f(x).

$$\begin{aligned} \text{right hand of (A1.2)} &= a_o-\sum_{i=1}^{r} a_i x^i \\ &= f(0)- \sum_{i=1}^{r}\Big(\sum_{t \in GF(q)} t^{r-i}f(t)\Big)x^i \\ &= f(0)- \sum_{t \in GF(q)} \Big(\sum_{i=1}^{r} t^{r-i}x^i\Big)f(t) \end{aligned} \tag{A1.4}$$

If x=0 then (A1.4) is clearly equal to f(x), so let us suppose $x \neq o$. If t=x then

$$\sum_{i=1}^{r} t^{r-i}x^i=\sum_{i=1}^{r} x^r= rx^r= -1 \tag{A1.5}$$

because $x^r= x^{q-1}=1$ for non zero x and r=q-1=-1 in GF(q). If $t \neq x$ and $t \neq 0$ then

$$\sum_{i=1}^{r} t^{r-i}x^i= t^r\sum_{i=1}^{r}(t^{-1}x)^i= 0 \tag{A1.6}$$

because for any element θ in GF(q) $\sum_{i=1}^{q-1}\theta^i = 0$. If t=0 then

$$\sum_{i=1}^{r} t^{r-i}x^i = t^0x^r = 1 \quad \text{(note that } t^0 = 1 \text{ even if } t=0) \qquad \text{(A1.7)}$$

So (A1.4) is equal to $f(0)-(f(0)-f(x)) = f(x)$.

Proof of theorem 3 We can demonstrate theorem 3 by the almost same way as theorem 6.

Put $a_i (0 \leqslant i \leqslant r)$ of (3.4) into the right hand of (3.3) then

$$\text{right hand of (3.3)} = f(0)+\sum_{t\in GF(2^m)}\left(\sum_{i=1}^{r} t^{r-i}x^i\right)f(t) \qquad \text{(A1.8)}$$

If x=0, (A1.8) becomes f(0), so consider the case $x\neq 0$.

$$\sum_{i=1}^{r} t^{r-i}x^i = \begin{cases} 1 & \text{if } t=x \\ 1 & \text{if } t\neq x,\ t=0 \\ t^r\sum_{i=1}^{r}(t^{-1}x)^i = t^r s(s^r-1)/(s-1) & \text{if } t\neq x,\ t\neq 0 \end{cases}$$

where $s=t^{-1}x$. Now s belongs to $GF(2^m)$ so $s^r-1=0$. Therefore we have

right hand of (3.3) $= f(0)+(f(0)+f(x)) = f(x)$. -----

Further let us generalize theorem 6 to the case of m-variable functions for wider applications.

Theorem 7 Any m-variable function on GF(q)

$$y = f(x_1,x_2,\ldots x_m) \quad (x_1,x_2,\ldots x_m,\ y \in GF(q)) \qquad \text{(A1.9)}$$

can be represented by an m-variable polynomial

$$f(x_1,x_2,\ldots,x_m) = \sum_{i_1=0}^{r}\sum_{i_2=0}^{r}\cdots\sum_{i_m=0}^{r} a_{i_1i_2\ldots i_m}x_1^{i_1}x_2^{i_2}\ldots x_m^{i_m} \qquad \text{(A1.10)}$$

$(r=q-1,\ a_{i_1i_2\ldots i_m}\in GF(q))$

where

$$
\left.\begin{aligned}
a_{oo\ldots o} &= f(0,0,\ldots,0)\\
a_{io\ldots o} &= -\sum_x x^{r-i} f(x,0,\ldots,0)\\
a_{oi\ldots o} &= -\sum_x x^{r-i} f(0,x,\ldots,0)\\
&\cdots\cdots\cdots\cdots\\
a_{oo\ldots i} &= -\sum_x x^{r-i} f(0,0,\ldots,x)
\end{aligned}\right\} \quad (1\leqslant i\leqslant r)
$$

$$
\left.\begin{aligned}
a_{ijo\ldots o} &= (-1)^2 \sum_x \sum_y x^{r-i} y^{r-j} f(x,y,0,\ldots,0)\\
a_{ioj\ldots o} &= (-1)^2 \sum_x \sum_y x^{r-i} y^{r-j} f(x,0,y,\ldots,0)\\
&\cdots\cdots\cdots\cdots\cdots\\
a_{o\ldots oij} &= (-1)^2 \sum_x \sum_y x^{r-i} y^{r-j} f(0,0,\ldots,x,y)
\end{aligned}\right\} \quad (1\leqslant i,j\leqslant r) \qquad \text{(A1.11)}
$$

$$
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
$$

$$
a_{i_1 i_2 \ldots i_m} = (-1)^m \sum_{x_1} \sum_{x_2} \cdots \sum_{x_m} x_1^{r-i_1} x_2^{r-i_2} \cdots x_m^{r-i_m} f(x_1,x_2,\ldots,x_m)
$$

$(1\leqslant i_1, i_2, \ldots, i_m \leqslant r)$

where in $\sum_x$, $\sum_x \sum_y \ldots$, x,y... run all over GF(q).

proof Let us demonstrate the case m=2, and it is only a formal task to extend it to the general case.

$$
\text{right hand of (A1.9)} = \sum_{i=0}^{r} \sum_{j=0}^{r} a_{ij} x_1^i x_2^j
$$

$$
= a_{oo} + \sum_{i=1}^{r} a_{io} x_1^i + \sum_{j=1}^{r} a_{oj} x_2^j + \sum_{i=1}^{r} \sum_{j=1}^{r} a_{ij} x_1^i x_2^j
$$

$$
= f(0,0) - \sum_{i=1}^{r} \Big(\sum_x x^{r-i} f(x,0) \Big) x_1^i - \sum_{j=1}^{r} \Big(\sum_x x^{r-j} f(0,x) \Big) x_2^j
$$

$$
+ \sum_{i=1}^{r} \sum_{j=1}^{r} \Big(\sum_x \sum_y x^{r-i} y^{r-j} f(x,y) \Big) x_1^i x_2^j \qquad \text{(A1.12)}
$$

It can be easily found by investigating the proof of theorm 6 that the second and third terms in the right hand of (A1.12) are equal to $f(0,0)-f(x_1,0)$ and $f(0,0)-f(0,x_2)$ respectively. So we hav

$$\text{right hand of (A1.9)} = f(0,0)-(f(0,0)-f(x_1,0))-(f(0,0)-f(0,x_2)) + \sum_{i=1}^{r}\sum_{j=1}^{r}\Big(\sum_{x}\sum_{y} x^{r-i}y^{r-j}f(x,y)\Big)x_1^i x_2^j \quad . \quad (A1.13)$$

Here if $x_1=0$ or $x_2=0$ then the last term of (A1.13) is equal to zero, and (A1.13) is clearly equal to $f(x_1,x_2)$. So let us suppose $x_1\neq 0$ and $x_2\neq 0$. Let L be the last term of (A1.13) then

$$L=\sum_{x}\sum_{y}\Big(\sum_{i=1}^{r} x^{r-i}x_1^i\Big)\Big(\sum_{j=1}^{r} y^{r-j}x_2^j\Big)f(x,y) \quad . \quad (A1.14)$$

By the same reasoning as the proof in theorem 6, we have

$$\sum_{i=1}^{r} x^{r-i}x_1^i = \begin{cases} -1 & \text{if } x=x_1 \\ 0 & \text{if } x\neq x_1,\ x\neq 0 \\ 1 & \text{if } x=0 \end{cases}$$

$$\sum_{j=1}^{r} y^{r-j}x_2^j = \begin{cases} -1 & \text{if } y=x_2 \\ 0 & \text{if } y\neq x_2,\ y\neq 0 \\ 1 & \text{if } y=0 \end{cases} \quad .$$

Consequently we have

$$L= f(0,0)-f(x_1,0)-f(0,x_2)+f(x_1,x_2) \quad (A1.15)$$

which proves that (A1.12) is equal to $f(x_1,x_2)$.

A2. Computations in Galois fields

In general let $GF(q^N)$ and θ be an extension field of order N over $GF(q)$ (q being a prime power) and its primitive element respectively. Then if we know the minimal polynomial of θ, then as (2.4) we have

$$\theta^j = z_0+z_1\theta+\ldots+z_{N-1}\theta^{N-1}, \quad z_i \in GF(q), \quad 0\leqslant j\leqslant q^N-2 \qquad (A2.1)$$

Let us call it EP-transform to find $(z_0,z_1,\ldots,z_{N-1})$ from θ^j.

It is well known the amount of computation for EP-transform is of order log(j) which relieve us from exponential amounts of computations. (for example let j=100. Expanding 100 in binary number , we have $100=2^6+2^5+2^2=(2^4+2^3+1)2^2=((2+1)2^2+1)2^2$. So we have $\theta^{100}=((((\theta^2\theta)^2)^2\theta)^2)^2$, and it takes 8 multiplications to get θ^{100}.)

On the contrary let it be called PE-transform to get j from $(z_0,z_1,\ldots,z_{N-1})$. If N is comparavely small it is advisable to search all j=0,1,2,... untill to get the given $(z_0,z_1,\ldots,z_{N-1})$, ~~If N is~~ because it takes one shift operation (ordinary 10^{-9}second) to get θ^{j+1} from θ^j with appropriate circuits. Otherwise it is suitable to utilize the following relation between i and k

$$\theta^i+\theta^k = 1 \qquad (A2.2)$$

If i and k satisfy (A2.2) then let us write i=f(k), and of course we can also write k=f(i).

An example of (A2.2) is given in table V (for $GF(2^5)$ with minimal polynomial $\theta^5+\theta^2+1$), where each column ~~is~~ consists of a GF(2)-Frobenius cycle. So we have only to bear initial relations(with parentheses in the table) for which the amount of memory is of order $2^N/N$ in general.

Now let us find j for $(z_0,z_1,z_2,z_3,z_4)=(1,1,1,0,1)$ in $GF(2^5)$ using table V.

$\theta^4+\theta^2+\theta+1=\theta^j$, $\theta^4+\theta^2+\theta=\theta^k$ $(j=f(k))$

$\theta^3+\theta+1=\theta^{k-1}$, $\theta^3+\theta=\theta^l$ $(k-1=f(l))$

$\theta^2+1=\theta^{l-1}$

therefore

$l-1=f(2)=5$, $l=6$

$k-1=f(6)=27$, $k=28$, $j=f(28)=26$ //

References

[1] Blake,I.F. and Mullin,R.C. (1975), "The Mathematical Theory of Coding" Academic Press

Table I

x_0	x_1	x_2	y_0	y_1
0	0	0	0	0
1	0	0	1	0
0	1	0	1	0
0	0	1	1	0
1	0	1	0	1
1	1	1	1	1
1	1	0	0	1
0	1	1	0	1

Table II

x	x_0	x_1	x_2	y_0	y_1	y_2	y
α^{∞}	0	0	0	1	0	0	α^0
α^0	1	0	0	0	1	0	α^1
α^1	0	1	0	0	0	1	α^2
α^2	0	0	1	0	1	1	α^4
α^3	1	1	0	1	1	0	α^3
α^4	0	1	1	1	0	1	α^6
α^5	1	1	1	0	0	0	α^{∞}
α^6	1	0	1	1	1	1	α^5

Table III

x	x_0	x_1	x_2	y_0	y_1	y
$0=\beta^{\infty}$	0	0	0	0	0	$\gamma^{\infty}=0$
$1=\beta^0$	1	0	0	1	0	$\gamma^0=1$
$\alpha^9=\beta^1$	0	1	0	1	0	$\gamma^0=1$
$\alpha^{18}=\beta^2$	0	0	1	1	0	$\gamma^0=1$
$\alpha^{27}=\beta^3$	1	0	1	0	1	$\gamma^1=\alpha^{21}$
$\alpha^{36}=\beta^4$	1	1	1	1	1	$\gamma^2=\alpha^{42}$
$\alpha^{45}=\beta^5$	1	1	0	0	1	$\gamma^1=\alpha^{21}$
$\alpha^{54}=\beta^6$	0	1	1	0	1	$\gamma^1=\alpha^{21}$

Table IV

x	x_0	x_1	x_2	x_3	y_0	y_1	y
0	0	0	0	0	0	0	$\beta^{\infty}=0$
1	1	0	0	0	0	1	$\beta^{0}=1$
α	0	1	0	0	0	1	$\beta^{0}=1$
α^2	0	0	1	0	0	1	$\beta^{0}=1$
α^3	0	0	0	1	0	1	$\beta^{0}=1$
α^4	1	1	0	0	1	0	$\beta=\alpha^5$
α^5	0	1	1	0	1	0	$\beta=\alpha^5$
α^6	0	0	1	1	1	0	$\beta=\alpha^5$
α^7	1	1	0	1	1	1	$\beta^2=\alpha^{10}$
α^8	1	0	1	0	1	0	$\beta=\alpha^5$
α^9	0	1	0	1	1	0	$\beta=\alpha^5$
α^{10}	1	1	1	0	1	1	$\beta^2=\alpha^{10}$
α^{11}	0	1	1	1	1	1	$\beta^2=\alpha^{10}$
α^{12}	1	1	1	1	0	0	$\beta^{\infty}=0$
α^{13}	1	0	1	1	1	1	$\beta^2=\alpha^{10}$
α^{14}	1	0	0	1	1	0	$\beta=\alpha^5$

Table V

$(\theta^1+\theta^{18}=1)$	$(\theta^3+\theta^{29}=1)$	$(\theta^7+\theta^{22}=1)$
$\theta^2+\theta^5=1$	$\theta^6+\theta^{27}=1$	$\theta^{14}+\theta^{13}=1$
$\theta^4+\theta^{10}=1$	$\theta^{12}+\theta^{23}=1$	$\theta^{28}+\theta^{26}=1$
$\theta^8+\theta^{20}=1$	$\theta^{24}+\theta^{15}=1$	$\theta^{25}+\theta^{21}=1$
$\theta^{16}+\theta^9=1$	$\theta^{17}+\theta^{30}=1$	$\theta^{19}+\theta^{11}=1$