On Algebraic Soft Decision Decoding of Cyclic Binary Codes

Vladimir B. Balakirsky

Euler Institute for Discrete Mathematics
and its Applications (EIDMA)
c/o Eindhoven University of Technology
5600 MB Eindhoven
The Netherlands

Data transmission over a symmetric channel

Suppose that there is a discrete memoryless channel defined by the conditional probability distributions

$$\Big(W_x(y), y \in \mathcal{Y} \stackrel{\triangle}{=} \{0, \ldots, 2L-1\} \Big), \; x = 0, 1$$

in a sense that

$$W(\mathbf{y}|\mathbf{x}) \stackrel{\triangle}{=} \prod_{j=0}^{n-1} W_{x_j}(y_j)$$

is the conditional probability to receive the vector $\mathbf{y} = (y_0, \ldots, y_{n-1}) \in \mathcal{Y}^n$ when the vector $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in \{0,1\}^n$ was sent. We will assume that the $2 \times (2L)$ matrix of crossover probabilities has the form

$$\mathbf{W} = \left[\begin{array}{cccccc} q(0) & \ldots & q(L-1) & p(L-1) & \ldots & p(0) \\ p(0) & \ldots & p(L-1) & q(L-1) & \ldots & q(0) \end{array} \right]$$

where

$$\begin{cases} q(y) > p(y) \geq 0, \text{ for all } y \in \{0, \ldots, L-1\} \\ \sum_{y=0}^{L-1} (p(y) + q(y)) = 1. \end{cases}$$

Example. Let $L = 2$ and

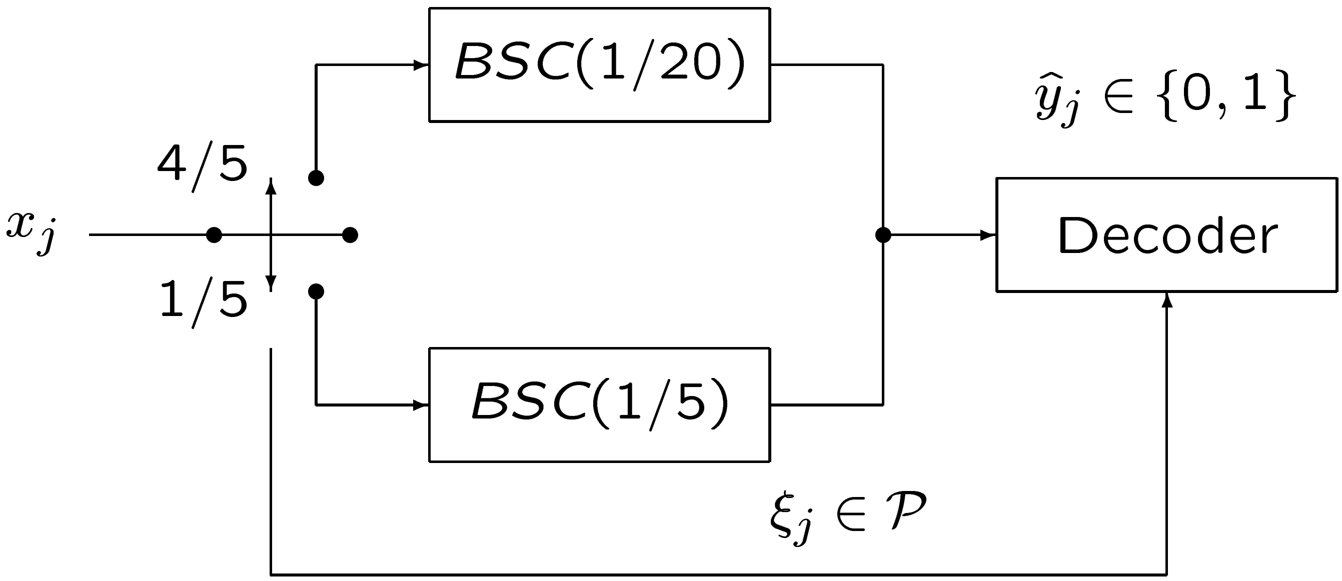
$$\mathbf{W} = \begin{bmatrix} 0.76 & 0.16 & 0.04 & 0.04 \\ 0.04 & 0.04 & 0.16 & 0.76 \end{bmatrix}.$$

Then

$$\mathcal{P} = \{1/20, 1/5\}$$

and

$$\begin{bmatrix} \pi(1/20) & \pi(1/5) \end{bmatrix} = \begin{bmatrix} 4/5 & 1/5 \end{bmatrix}.$$



Comments.

Consider the system of data transmission where the j–th code bit is transmitted either over a $BSC(1/20)$, or over a $BSC(1/5)$. The selection is made by a jammer who chooses the first channel with probability $4/5$ and the second channel with probability $1/5$. The jammer also informs the decoder about his choice by sending him $\xi_j \in \{1/20, 1/5\}$. These operations are independently repeated for all $j = 1, \ldots, n$. The decoder has to construct an estimate of the transmitted codeword for a given vector of pairs $((\widehat{y}_1, \xi_1), \ldots, (\widehat{y}_n, \xi_n))$. This problem coincides with the problem of estimating the transmitted codeword for a given vector $(y_1, \ldots, y_n)$ received at the output of the channel having the matrix of crossover probabilities $\mathbf{W}$, since there are component–wise one–to–one mappings $0 \leftrightarrow (0, 1/20)$, $1 \leftrightarrow (0, 1/5)$, $2 \leftrightarrow (1, 1/5)$, $3 \leftrightarrow (1, 1/20)$ that translate $(y_1, \ldots, y_n)$ to the vector of pairs $((\widehat{y}_1, \xi_1), \ldots, (\widehat{y}_n, \xi_n))$.

Conclusion.

Transmission of a binary codeword over a symmetric channel defined by the $2 \times (2L)$ matrix $\mathbf{W}$ can be represented as transmission over a time–varying binary symmetric channel whose crossover probability belongs to a certain set. This set is uniquely determined by the matrix $\mathbf{W}$. There is also side information at the decoder. As a result, the decoder knows the crossover probability of the binary symmetric channel at each time instant. The difference in the performance of the soft decision decoding compared to the hard decision decoding is due to the fact that the decoder makes use of this side information.

The error vector of the time–varying binary symmetric channel is a binary vector, which belongs to the same space as the codewords. Thus, metric properties of the space and different algebraic tools developed for binary symmetric channels can be used.

Example. *Consider the* $(15, 7)$ *BCH code having the parity–check matrix*

$$\mathbf{H} = \left[\begin{array}{cccc} \alpha^0 & \alpha^1 & \ldots & \alpha^{14} \\ (\alpha^0)^3 & (\alpha^1)^3 & \ldots & (\alpha^{14})^3 \end{array} \right]$$

where $\alpha \in GF(2^4) : \alpha^0 + \alpha^1 + \alpha^4 = 0.$

Let

$$y_j = \begin{cases} 0, & \text{if } j \notin \{0, 1, 9, 13\} \\ 1, & \text{if } j \in \{0, 1\} \\ 3, & \text{if } j \in \{9, 13\}. \end{cases}$$

Denote

$$\hat{y}_j = \begin{cases} 0, & \text{if } j \notin \{9, 13\} \\ 1, & \text{if } j \in \{9, 13\} \end{cases}$$

and

$$\begin{aligned} \mathcal{J}_{1/20} &= \{2, \ldots, 14\} \\ \mathcal{J}_{1/5} &= \{0, 1\}. \end{aligned}$$

Let

$$X_{i,\xi} \triangleq \sum_{j \in \mathcal{J}_\xi :\, x_j = 1} (\alpha^i)^j$$

$$S_{i,\xi} \triangleq \sum_{j \in \mathcal{J}_\xi :\, \hat{y}_j = 1} (\alpha^i)^j.$$

Then, for $i = 1, \ldots, 4$,

$$\sum_{j \in \mathcal{J}_{1/20} :\, e_j = 1} (\alpha^i)^j = (\alpha^9)^i + (\alpha^{13})^i + X_{i,1/20}$$

$$\sum_{j \in \mathcal{J}_{1/5} :\, e_j = 1} (\alpha^i)^j = X_{i,1/5}$$

and

$$X_{i,1/20} + X_{i,1/5} = 0.$$

Problem. *Assign a valid vector*

$$\mathbf{e} = (e_0, \ldots, e_{14}) \in \{0, 1\}^{15}$$

which minimizes the function

$$\begin{aligned} Cost \ \stackrel{\triangle}{=}\ & c_{1/20} \left| \{ j \in \mathcal{J}_{1/20} : e_j = 1 \} \right| \\ & + c_{1/5} \left| \{ j \in \mathcal{J}_{1/5} : e_j = 1 \} \right| \end{aligned}$$

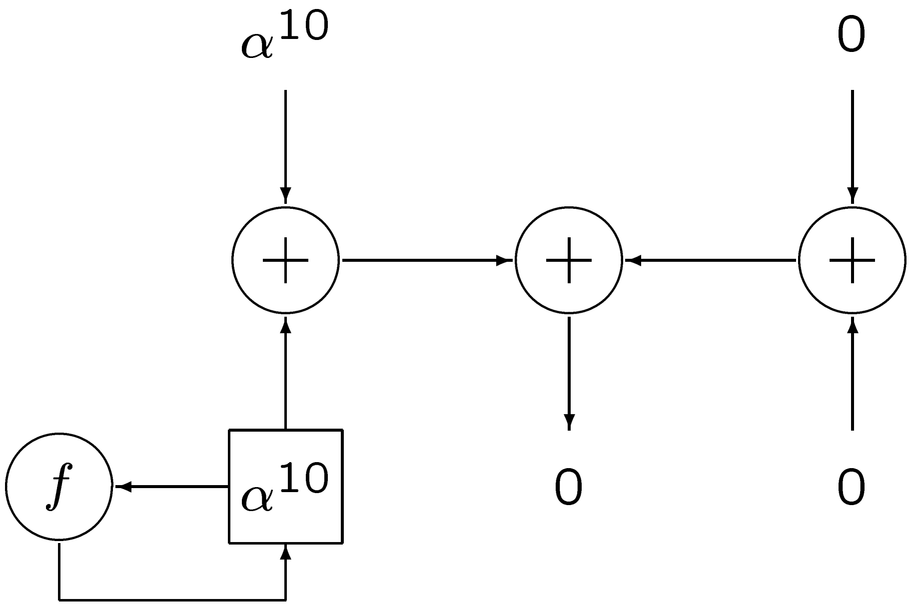
where

$$\begin{aligned} c_{1/20} &= \log \frac{19/20}{1/20} = 4.25\ldots \\ c_{1/5} &= \log \frac{4/5}{1/5} = 2. \end{aligned}$$

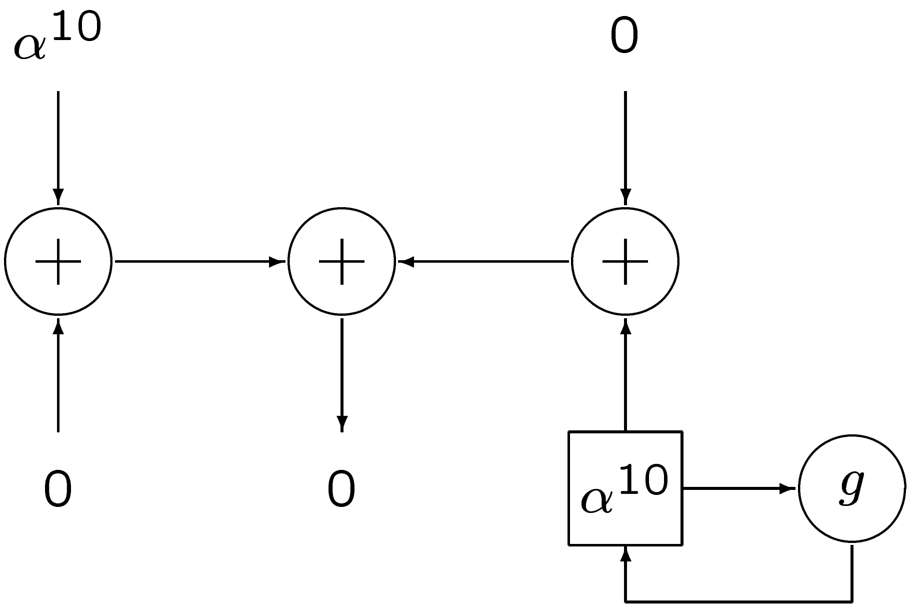
(The vector $\mathbf{e}$ *is a valid vector if and only if* $\hat{\mathbf{y}} \oplus \mathbf{e}$ *is a codeword).*

$i = 1$; $\alpha^9 + \alpha^{13} = \alpha^{10} \notin \{0, \alpha^0, \alpha^1, \alpha^0 + \alpha^1\}$.

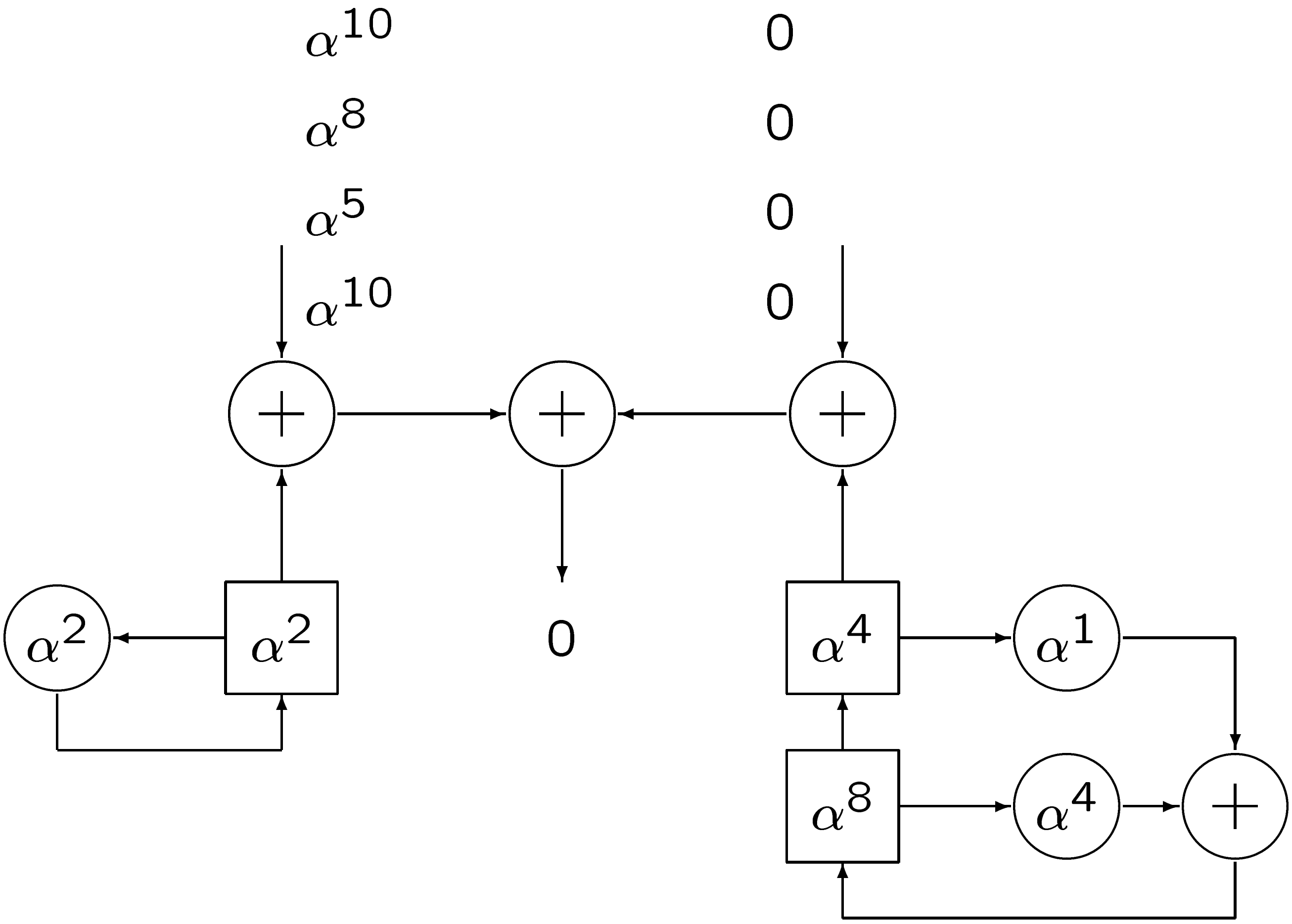
Valid scheme, $Cost = 4.25$:



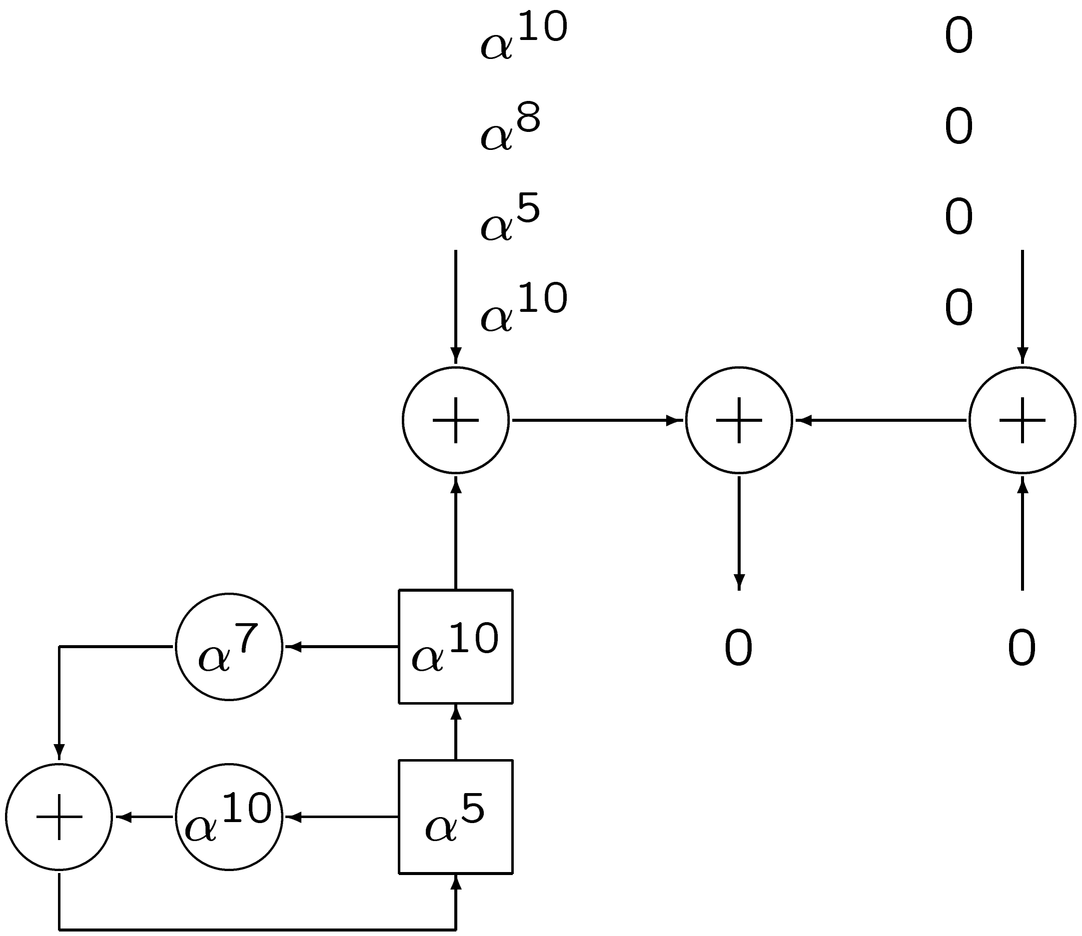
Non–valid scheme, $Cost = 2$:



Optimal scheme, $Cost = 4.25 + 2 \cdot 2 = 8.25$.



Non–optimal scheme, $Cost = 2 \cdot 4.25 = 8.5$.



Proposition. *Let*

$$S_t = \sum_{i=1}^{L} f_i S_{t-i}, \quad \textit{for all } t = L+1, \ldots, j$$

and

$$f^*(z) \triangleq \sum_{i=0}^{L} f_i z^{L-i}.$$

Then

$$S_j = \sum_{i=0}^{L-1} r_i^{(j-1)} S_{i+1}$$

where $r_0^{(j-1)}, \ldots, r_{L-1}^{(j-1)}$ *are coefficients of the polynomial*

$$r^{(j-1)}(z) \triangleq \mathsf{R}_{f^*(z)}[\, z^{j-1}\,]$$

and $\mathsf{R}_{f^*(z)}[\, z^{j-1}\,]$ *denotes the remainder of the division of the polynomial* z^{j-1} *by the polynomial* $f^*(z)$.

Example. Let $\alpha \in GF(2^4) : \alpha^0 + \alpha^1 + \alpha^4 = 0$ and

$$(S_1, \ldots, S_4) = (\alpha^{10}, \alpha^5, \alpha^8, \alpha^{10})$$

Then

$$f(z) = \alpha^0 + \alpha^{10} z + \alpha^7 z^2$$

and

$$f^*(z) = \alpha^0 z^2 + \alpha^{10} z + \alpha^7.$$

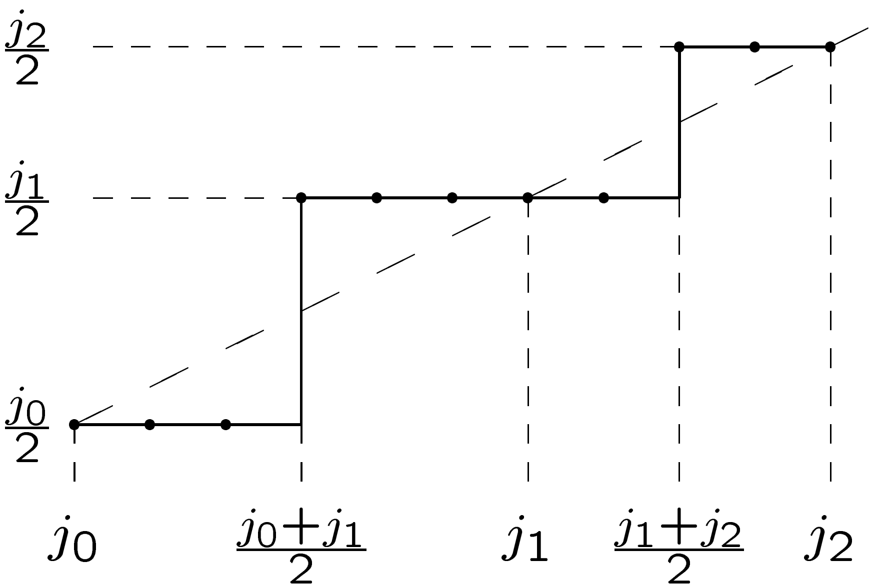
Furthermore,

$$z^5 = (\alpha^0 z^3 + \alpha^{10} z^2 + \alpha^{13} z^1 + \alpha^0) f^*(z) + (\alpha^0 z + \alpha^7).$$

Thus,

$$S_6 = \alpha^0 \cdot \alpha^5 + \alpha^7 \cdot \alpha^{10} = \alpha^1.$$

Properties of the linear complexity profile of a given sequence $S_1, S_2, \ldots$



Lemma. *Let* $i_1 \stackrel{\triangle}{=} (j_0+j_1)/2$ *and* $i_2 \stackrel{\triangle}{=} (j_1+j_2)/2$. *For all* $j \in \{i_2, \ldots, j_2\}$,

$$F_j(z) = G(z)F_{j_1}(z) + \alpha^h z^{i_2-i_1} F_{j_0}(z)$$

where $0 \leq \deg G(z) \leq j_2 - i_2 - 1$, *the first* $j - i_2$ *coefficients of* $G(z)$ *are uniquely determined by* $S_{i_2+1}, \ldots, S_j$, *and* h *is uniquely determined by* S_{i_2}.

Example. Let $\widehat{y}_9 = \widehat{y}_{13} = 1$ and $\widehat{y}_j = 0$ for all $j \notin \{9, 13\}$;

$$(S_1, \ldots, S_4) = (\alpha^{10}, \alpha^5, \alpha^8, \alpha^{10})$$

is the syndrome sequence.

Then

$$\begin{aligned} F_2(z) &= \alpha^0 + \alpha^{10} z \\ F_4(z) &= \alpha^0 + \alpha^{10} z + \alpha^7 z^2 \\ &= (\alpha^0 + \alpha^9 z)(\alpha^0 + \alpha^{13} z) \end{aligned}$$

and the sequence $(S_1, \ldots, S_5)$ for some non–zero element S_5 is generated by the polynomial

$$F_5(z) = (\alpha^0 + gz) F_4(z) + \alpha^h z^2 F_2(z)$$

where $g \in GF(2^4)$ and $h \in \{0, \ldots, 14\}$.

Let $\mathsf{R}^j[F(z)]$ denote the remainder of the division of the polynomial $F(z)$ by the polynomial $\alpha^0 + \alpha^j z$.

Remaiders of the division :

$$F_4(z) = \alpha^0 + \alpha^{10} z + \alpha^7 z^2, \;\; F_2(z) = \alpha^0 + \alpha^{10} z.$$

j	$\mathrm{R}^j[F_4(z)]$	$\mathrm{R}^j[\,z^2\,]$	$\mathrm{R}^j[F_2(z)]$	h	
0	α^{13}	α^0	α^5	8	$\odot$
1	α^{13}	α^{13}	α^7	8	$\odot$
2	α^6	α^{11}	α^2	8	$\odot$
3	α^3	α^9	α^9	0	
4	α^2	α^7	α^{13}	12	
5	α^3	α^5	α^{10}	3	$\ominus$
6	α^8	α^3	α^1	4	
7	α^6	α^1	α^{14}	6	
8	α^{14}	α^{14}	α^8	7	
9	0	α^{12}	α^4	—	
10	α^2	α^{10}	0	—	
11	α^{14}	α^8	α^3	3	$\ominus$
12	α^0	α^6	α^6	3	$\ominus$
13	0	α^4	α^{11}	—	
14	α^8	α^2	α^{12}	9	

The valid polynomials

$$F_5(z) = (\alpha^0 + gz)F_4(z) + z^h F_2(z), \text{ where}$$

$$F_4(z) = \alpha^0 + \alpha^{10}z + \alpha^7 z^2, \;\; F_2(z) = \alpha^0 + \alpha^{10}z.$$

Note that $S_6 = (\alpha^9)^6 + (\alpha^{13})^6 = \alpha^1$ **is known.**

g	h	Factors of $F_5(z)$			$\widehat{S}_6$
0	3	$\alpha^0 + \alpha^5 z$	$\alpha^0 + \alpha^{11} z$	$\alpha^0 + \alpha^{12} z$	α^1
0	8	$\alpha^0 + \alpha^0 z$	$\alpha^0 + \alpha^1 z$	$\alpha^0 + \alpha^2 z$	α^1
α^0	11	$\alpha^0 + \alpha^1$	$\alpha^0 + \alpha^3 z$	$\alpha^0 + \alpha^6 z$	α^9
α^1	9	$\alpha^0 + \alpha^1 z$	$\alpha^0 + \alpha^6 z$	$\alpha^0 + \alpha^8 z$	α^9
α^2	1	$\alpha^0 + \alpha^0 z$	$\alpha^0 + \alpha^6 z$	$\alpha^0 + \alpha^{11} z$	α^4
α^3	1	$\alpha^0 + \alpha^1 z$	$\alpha^0 + \alpha^3 z$	$\alpha^0 + \alpha^{12} z$	α^{14}
α^4	4	$\alpha^0 + \alpha^3 z$	$\alpha^0 + \alpha^8 z$	$\alpha^0 + \alpha^{14} z$	α^3
α^5	7	$\alpha^0 + \alpha^2 z$	$\alpha^0 + \alpha^6 z$	$\alpha^0 + \alpha^{14} z$	α^7
α^7	11	$\alpha^0 + \alpha^4 z$	$\alpha^0 + \alpha^5 z$	$\alpha^0 + \alpha^{14} z$	α^4
α^8	10	$\alpha^0 + \alpha^0 z$	$\alpha^0 + \alpha^3 z$	$\alpha^0 + \alpha^7 z$	α^2
α^9	14	$\alpha^0 + \alpha^7 z$	$\alpha^0 + \alpha^{12} z$	$\alpha^0 + \alpha^{14} z$	α^3
α^{11}	6	$\alpha^0 + \alpha^4 z$	$\alpha^0 + \alpha^8 z$	$\alpha^0 + \alpha^{12} z$	α^{12}
α^{13}	4	$\alpha^0 + \alpha^1 z$	$\alpha^0 + \alpha^4 z$	$\alpha^0 + \alpha^7 z$	α^7
α^{13}	5	$\alpha^0 + \alpha^2 z$	$\alpha^0 + \alpha^3 z$	$\alpha^0 + \alpha^5 z$	α^2