BAZI ÖZEL DEVİRLİ KODLAR

Önceki bölüm devirli kodların genel olarak tanıtılmasına ve bazı özel durumlar için devirli kodlarla kod çözme algoritmalarının verilmesine ayrılmıştı. Bir devirli kodun üreteç polinomu sayesinde birçok özelliğinin belirlenebiliyor olmasına karşın bu kodların minimum uzaklıklarını elde etmek zor olabilmektedir. Öte yandan üreteç polinomu iyi seçilirse, devirli kodun uzaklığı hemen anlaşılabilir ve nispeten daha kolay kod çözme algoritmaları elde edilebilir. Bu bölümde üreteç polinomlarını özel bir biçimde seçerek elde edilen ve az evvel bahsedilen kolaylıkları barındıran BCH kodları, Reed-Solomon Kodları ve kuadratik-kalan kodları tanıtılacaktır.

A - BCH Kodları

Açık halde Bose-Chaudhuri-Hocquenghem olan BCH kodları Hamming kodlarının bir genellemesi olarak daha fazla hata düzeltebilme özelliği ile ilk defa 1959 yılında A. Hocquenghem, 1960 yılında birbirinden bağımsız olarak R.C. Bose ve D.K. Ray-Chaudhuri tarafından ortaya atılmıştır.

A.1. Temel Tanımlar

$f_1(x), f_2(x) \in \mathbb{F}_q[x]$ için $f_1(x)$ ve $f_2(x)$ polinomlarının en küçük ortak katı $\text{ekok}(f_1(x), f_2(x))$, $f_1(x)$ ve $f_2(x)$ in katı olan en küçük dereceli monik polinom olarak tanımlanmıştı. Şimdi elimizde

t adet $f_1(x), \dots, f_t(x) \in \mathbb{F}_q[x]$ polinomları olsun. Bunların en küçük ortak katını $f_1(x), \dots, f_t(x)$ polinomlarının katı olan en küçük dereceli polinom olarak tanımlarız ve bu polinomu $\text{ekok}(f_1(x), \dots, f_t(x))$ ile gösteririz. Kolayca gösterilebilir ki

$$\text{ekok}(f_1(x), \dots, f_t(x)) = \text{ekok}(\text{ekok}(f_1(x), \dots, f_{t-1}(x)), f_t(x))$$

dir. Ayrıca eğer $f_1(x), \dots, f_t(x)$ polinomları

$$f_1(x) = a_1 P_1(x)^{e_{11}} \dots P_n(x)^{e_{1n}}, \dots, f_t(x) = a_t P_1(x)^{e_{t1}} \dots P_n(x)^{e_{tn}}$$

şeklinde indirgenemez çarpanlarına ayrılıyor ise

$$\text{ekok}(f_1(x), \dots, f_t(x)) = P_1(x)^{\text{maks}\{e_{11}, \dots, e_{t1}\}} \dots P_n(x)^{\text{maks}\{e_{1n}, \dots, e_{tn}\}}$$

olur.

Örnek. $f_1(x) = (1+x)^2(1+x+x^4)^3 \in \mathbb{F}_2[x]$, $f_2(x) = (1+x)(1+x+x^2)^2 \in \mathbb{F}_2[x]$ ve $f_3(x) = x^2(1+x+x^4) \in \mathbb{F}_2[x]$ olsun. Buna göre

$$\text{ekok}(f_1(x), f_2(x), f_3(x)) = x^2(1+x)^2(1+x+x^2)^2(1+x+x^4)^3$$

olur.

Lemma. $f(x), f_1(x), \dots, f_t(x) \in \mathbb{F}_q[x]$ olsun. Eğer her $i = 1, \dots, t$ için $f_i \mid f(x)$ ise o zaman $\text{ekok}(f_1(x), \dots, f_t(x)) \mid f(x)$ olur.

Örnek. $f_1(x) = 1+x+x^2 \in \mathbb{F}_2[x]$, $f_2(x) = 1+x+x^4 \in \mathbb{F}_2[x]$ ve $f_3(x) = (1+x+x^2)(1+x^3+x^4) \in \mathbb{F}_2[x]$ polinomları $f(x) = x^{15}-1 \in \mathbb{F}_2[x]$ polinomunu böldüğü için $\text{ekok}(f_1(x), f_2(x), f_3(x)) = (1+x+x^2)(1+x+x^4)(1+x^3+x^4)$ polinomu da $x^{15}-1$ i böler.

α, $\mathbb{F}_{q^m}$ cisminin bir ilkel elemani, $M^{(i)}(x)$ α^i elemanının $\mathbb{F}_q$ üzerindeki minimal polinomu ve $\{s_1, \ldots, s_t\}$ q nun q^m-1 modülüne göre bir tam temsilci kümesi ise

$$x^{q^m-1}-1 = M^{(s_1)}(x) \ldots M^{(s_t)}(x)$$

olacağını daha önce göstermiştik. Dolayısıyla $I \subseteq \mathbb{Z}_{q^m-1}$ ise her $i \in I$ için $M^{(i)}(x) \mid x^{q^m-1}-1$ olur. Böylece $\text{ekok}(M^{(i)}(x))_{i\in I} \mid x^{q^m-1}-1$ bulunur. Bu gözlemi de dikkate alarak aşağıdaki tanımı verebiliriz:

Tanım. α $\mathbb{F}_{q^m}$ cisminin bir ilkel elemanı olmak üzere α^i elemanının $\mathbb{F}_q$ üzerindeki minimal polinomu $M^{(i)}(x)$ ve $\delta \geq 2$ bir tamsayı olsun. Bir $a \in \mathbb{Z}$ için

$$g(x) = \text{ekok}(M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+\delta-2)}(x))$$

polinomu tarafından üretilen q-lu devirli koda uzunluğu $n=q^m-1$ ve tasarlanmış uzaklığı δ olan $\mathbb{F}_q$ üzerinde bir <u>BCH kodu</u> denir. Eğer $a=1$ ise BCH koduna <u>dar anlamlı</u> denir.

Örnek. (i) α, $\mathbb{F}_{2^m}$ cisminin bir ilkel elemanı olsun. Tasarlanmış uzaklığı 2 olan bir ikili BCH kodu $M^{(1)}(x)$ tarafından üretilen ikili devirli koddur. Gösterilebilir ki aslında bu kod bir Hamming kodudur.

(ii) $\alpha \in \mathbb{F}_8$, $1+x+x^3$ polinomunun bir kökü olsun. Buna göre α $\mathbb{F}_8$ cisminin bir ilkel elemanıdır. $M^{(1)}(x) = M^{(2)}(x) = 1+x+x^3$ olduğunu biliyoruz. Böylece 7 uzunluklu dar anlamlı bir ikili BCH kodunun tasarlanmış uzaklığı $\delta=3$ ise bu kod $\text{ekok}(M^{(1)}(x), M^{(2)}(x)) = 1+x+x^3$ tarafından üretilen ikili devirli koddur. Aslında bu kod

$[7,4,3]$- Hamming kodudur.

(iii) (ii) şıkkındaki α için ekok$(M^{(1)}(x), M^{(2)}(x), M^{(4)}(x)) =$ ekok$(1+x, 1+x+x^3) = (1+x)(1+x+x^3)$ tarafından üretilen 7 uzunluklu bir ikili BCH kodu bir $[7,3]$-devirli kodudur. Bu kodun (ii) deki Hamming kodunun dual olduğu kolayca görülebilir.

Örnek. β, $1+x+x^2 \in \mathbb{F}_2[x]$ polinomunun bir kökü olsun. $\mathbb{F}_4 = \mathbb{F}_2[\beta]$. α, $\beta+x+x^2 \in \mathbb{F}_4[x]$ polinomunun bir kökü olsun. O zaman α, $\mathbb{F}_{16}$ cismi nin bir ilkel elemanıdır. Tasarlanmış uzaklığı 4 olan 15-uzunluklu dörtlü BCH kodunun üreteç polinomu

$$g(x) = \text{ekok}(M^{(1)}(x), M^{(2)}(x), M^{(3)}(x)) = 1+\beta x+\beta x^2+x^3+x^4+\beta^2 x^5+x^6$$

polinomudur.

A.2. BCH Kodlarının Parametreleri

BCH kodlarının uzunlukları q^m-1 şeklindedir. Bu kodların önce boyutlarını ele alalım.

Teorem. (i) $g(x) = \text{ekok}(M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+\delta-2)}(x))$ tarafından üretilen ve uzunluğu q^m-1 olan bir q-lu BCH kodunun boyutu α ilkel elemanının seçiminden bağımsızdır.

(ii) Tasarlanmış uzaklığı δ olan q^m-1 uzunluklu bir q-lu BCH kodunun boyutu en az $q^m-1-m(\delta-1)$ dir.

C_i : q nun q^m-1 modülüne göre i yi içeren ç.e.b. kümesi

$S = \bigcup_{i=a}^{a+\delta-2} C_i$

$\Rightarrow$ üreteç polinomu

$$g(x) = \text{ekok}\left(\prod_{i\in C_a}(x-\alpha^i), \prod_{i\in C_{a+1}}(x-\alpha^i), \ldots, \prod_{i\in C_{a+\delta-2}}(x-\alpha^i)\right)$$

$$= \prod_{i\in S}(x-\alpha^i)$$

Dolayısıyla boyut $= q^m - 1 - |S|$

Yani $g(x) = \text{ekok}(M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+\delta-2)}(x))$ tarafından üretilen ve uzunluğu q^m-1 olan q-lu BCH kodunun boyutunu bulmak için $\bigcup_{i=a}^{a+\delta-2} C_i$ kümesinin eleman sayısını belirlemek yeterlidir.

Örnek. 2 nin 15 modülüne göre

$$C_2 = \{1,2,4,8\} \text{ ve } C_3 = \{3,6,12,9\}$$

ç.e.b. kümelerini ele alalım. $g(x) = \text{ekok}(M^{(2)}(x), M^{(3)}(x))$ tarafından üretilen tasarlanmış uzaklığı 3 olan 15 uzunluklu ikili BCH kodunun boyutu

$$15 - |C_2 \cup C_3| = 15 - 8 = 7$$

bulunur.

Örnek. 3 ün 26 modülüne göre

$$C_1 = C_3 = \{1,3,9\}, \quad C_2 = \{2,6,18\}, \quad C_4 = \{4,12,10\}$$

ç.e.b. kümelerini ele alalım. $g(x) = \text{ekok}(M^{(1)}(x), M^{(2)}(x), M^{(3)}(x), M^{(4)}(x))$ tarafından üretilen ve tasarlanmış uzaklığı 5 olan 26 uzunluklu üçlü BCH kodunun boyutu

$$26 - |C_1 \cup C_2 \cup C_3 \cup C_4| = 26 - 9 = 17 > 14 = 2^m - 1 - m(\delta - 1)$$

olur.

Örnek: (i) $t \geq 1$ olmak üzere t ve $2t$, 2 nin $2^m - 1$ modülüne göre aynı ç.e.b. kümelerine düşerler. Bu ise

$$M^{(t)}(x) = M^{(2t)}(x)$$

olması demektir. Dolayısıyla

$$\text{ekok}(M^{(1)}(x), \ldots, M^{(2t-1)}(x)) = \text{ekok}(M^{(1)}(x), \ldots, M^{(2t)}(x))$$

olur. Yani uzunluğu $2^m - 1$ ve tasarlanmış uzaklığı $2t+1$ olan dar anlamlı ikili BCH kodu ile uzunluğu $2^m - 1$ ve tasarlanmış uzaklığı $2t$ olan dar anlamlı ikili BCH kodu aynıdır.

Aşağıdaki tabloda uzunluğu $2^m - 1$ ve tasarlanmış uzaklığı $2t+1$ olan dar anlamlı ikili BCH kodlarının boyutları görülebilir.

n	k	t	n	k	t
7	4	1	63	51	2
15	11	1	63	45	3
15	7	2	63	39	4
15	5	3	63	36	5
31	26	1	63	30	6
31	21	2	63	24	7
31	16	3	63	18	10
31	11	5	63	16	11
31	6	7	63	10	13
63	57	1	63	7	15

(ii) α, $1 + x + x^4 \in \mathbb{F}_2[x]$ polinomunun bir kökü olsun. Buna göre α $\mathbb{F}_{16}$ cisminin bir ilkel elemanıdır. Ayrıca

$$M^{(0)}(x) = 1 + x$$

$$M^{(1)}(x) = M^{(2)}(x) = M^{(4)}(x) = M^{(8)}(x) = 1 + x + x^4$$

$M^{(3)}(x) = M^{(6)}(x) = M^{(12)}(x) = M^{(9)}(x) = 1+x+x^2+x^3+x^4$

$M^{(5)}(x) = M^{(10)}(x) = 1+x+x^2$

$M^{(7)}(x) = M^{(14)}(x) = M^{(13)}(x) = M^{(11)}(x) = 1+x^3+x^4$

bulunur. Buna göre 15-uzunluklu bir dar anlamlı ikili BCH kodu için aşağıdaki tabloyu verebiliriz.

n	k	t	üreteç polinomu
15	11	1	$1+x+x^4$
15	7	2	$(1+x+x^4)(1+x+x^2+x^3+x^4)$
15	5	3	$(1+x+x^4)(1+x+x^2+x^3+x^4)(1+x+x^2)$

Teorem. Eğer $q \neq 2$ ve her $1 \leq e \leq \delta-1$ için $\text{ebob}(q^m-1, e) = 1$ ise o zaman uzunluğu q^m-1 ve tasarlanmış uzaklığı δ olan bir dar anlamlı q-lu BCH kodunun boyutu $q^m-1-m(\delta-1)$ dir.

Örnek. 63 uzunluklu tasarlanmış uzaklığı 3 olan dar anlamlı 4-lü BCH kodunun boyutu $63-3(3-1) = 57$ dir.

Teorem. Tasarlanmış uzaklığı δ olan bir BCH kodunun uzaklığı en az δ dir.

Örnek.(i) α, $1+x+x^3 \in \mathbb{F}_2[x]$ polinomunun bir kökü olmak üzere $\mathcal{C}$ 7 uzunluklu, tasarlanmış uzaklığı 4 olan ve

$$g(x) = \text{ekok}(M^{(0)}(x), M^{(1)}(x), M^{(2)}(x)) = 1+x^2+x^3+x^4$$

tarafından üretilen ikili BCH kodu olsun. Bu durumda

$d(\mathcal{C}) \leq wt(g(x)) = 4$ dür. Ayrıca yukarıdaki teoremden $d(\mathcal{C}) \geq 4$ bulunur. Dolayısıyla $d(\mathcal{C}) = 4$ olur.

(ii) α, $1+x+x^4 \in \mathbb{F}_2[x]$ polinomunun bir kökü olsun. Buna göre α $\mathbb{F}_{16}$ cisminin bir ilkel elemanıdır. 15 uzunluklu ve tasarlanmış uzaklığı 7 olan dar anlamlı ikili BCH kodunu düşünelim. Bu kodun üreteç polinomu

$$\begin{aligned} g(x) &= ekok\left(M^{(1)}(x), M^{(2)}(x), \ldots, M^{(6)}(x)\right) \\ &= M^{(1)}(x)\, M^{(3)}(x)\, M^{(5)}(x) \\ &= 1+x+x^2+x^4+x^5+x^8+x^{10} \end{aligned}$$

olur. Buna göre $d(\mathcal{C}) \leq wt(g(x)) = 7$ dir. Öte yandan yukarıdaki teoreme göre $d(\mathcal{C}) \geq 7$ olur. Böylece $d(\mathcal{C}) = 7$ bulunur.

A-3. BCH Kodları ile Kod Çözme

α $\mathbb{F}_{2^m}$ cisminin bir ilkel elemanı ve $M^{(i)}(x)$ α^i elemanının $\mathbb{F}_2$ üzerindeki minimal polinomu olsun.

$\mathcal{C}$, uzunluğu $n = 2^m - 1$ ve tasarlanmış uzaklığı $\delta = 2t+1$ olan ve $g(x) = ekok\left(M^{(1)}(x), M^{(2)}(x), \ldots, M^{(\delta-1)}(x)\right)$ tarafından üretilen dar anlamlı ikili BCH kodu olsun.

$$H = \begin{bmatrix} 1 & \alpha & (\alpha)^2 & \cdots & (\alpha)^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{\delta-1} & (\alpha^{\delta-1})^2 & \cdots & (\alpha^{\delta-1})^{n-1} \end{bmatrix}$$

olsun. Dikkat edilirse $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ elemanlarının hepsi $g(x)$ in köküdür. Şimdi $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]$ alalım. $c = (c_0, c_1, \ldots, c_{n-1})$ diyelim. Eğer $c \in \mathcal{C}$ ise o zaman $g(x) \mid c(x)$ ve böylece her $1 \le i \le \delta-1$ için $c(\alpha^i) = 0$ olur. Dolayısıyla

$$cH^T = 0$$

olur. Şimdi tersine $cH^T = 0$ olsun. Buna göre her $1 \le i \le \delta-1$ için $c(\alpha^i) = 0$ olur. $M^{(i)}(x)$, α^i nin $\mathbb{F}_q$ üzerindeki minimal polinomu ve $c(x) \in \mathbb{F}_q[x]$ olduğundan $M^{(i)}(x) \mid c(x)$ $(1 \le i \le \delta-1)$ elde edilir. Böylece $g(x) = \text{ekok}\left(M^{(i)}(x)\right)_{i=1}^{\delta-1} \mid c(x)$, yani $c \in \mathcal{C}$ bulunur. Dolayısıyla her $c \in \mathbb{F}_q^{n-1}$ için

$$c \in \mathcal{C} \iff cH^T = 0$$

elde edilir. Buna göre her $c \in \mathbb{F}_q^{n-1}$ için c nin sendromunu $S(c) = cH^T$ olarak tanımlayabiliriz. Her $c_1, c_2 \in \mathbb{F}_q^{n-1}$ için kolayca görülebilir ki $S(c_1 + c_2) = S(c_1) + S(c_2)$ ve $S(c_1) = S(c_2) \iff c_1$ ve c_2 $\mathcal{C}$ nin aynı koseti içindedir.

Kabul edelim ki $w(x) = w_0 + w_1 x + \cdots + w_{n-1} x^{n-1}$ alınan sözcük olsun. Ayrıca kabul edelim ki hata polinomu $e(x)$ in ağırlığı $wt(e(x)) \le t$ olsun. $c(x) = w(x) - e(x)$ yazalım.

$w(x)$ in sendromu $(s_0, s_1, \ldots, s_{\delta-2})$ denirse

$$(s_0, s_1, \ldots, s_{\delta-2}) = (w_0, w_1, \ldots, w_{n-1}) H^T$$

olur. Dikkat edilirse her $i = 0, 1, \ldots, \delta-2$ için

$$s_i = w(\alpha^{i+1}) = e(\alpha^{i+1})$$

olur. (Son eşitliğin nedeni $g(x) \mid c(x)$ ve $g(\alpha^{i+1}) = 0$ olmasıdır.)

Kabul edelim ki $\ell \leq t$ olmak üzere hatalar $i_0, i_1, \ldots, i_{\ell-1}$ basamaklarında meydana gelmiş olsun; yani

$$e(x) = x^{i_0} + x^{i_1} + \cdots + x^{i_{\ell-1}}$$

olsun.

$$\sigma(z) := \prod_{j=0}^{\ell-1} (1 - \alpha^{i_j} z)$$

polinomunu tanımlayalım. $\sigma(z)$ nin köklerini bilirsek i_j hata yerlerini de bulabiliriz. Bunun için önce $\sigma(z)$ nin belirlenmesi gerekiyor.

Teorem. Kabul edelim ki $S(z) = \sum_{i=0}^{\delta-2} S_i z^i$ sendrom polinomu sıfırdan farklı olsun. O zaman

(i) $r(z) \equiv S(z)\sigma(z) \pmod{z^{\delta-1}}$

(ii) $\deg(r(z)) \leq t-1$ ve

(iii) $\text{ebob}(r(z), \sigma(z)) = 1$

olacak şekilde sıfırdan farklı $r(z) \in \mathbb{F}_{2^m}[z]$ polinomu vardır. Ayrıca $u(z) \equiv S(z)v(z) \pmod{z^{\delta-1}}$, $\deg(u(z)) \leq t-1$ ve $\deg(v(z)) \leq t$ olacak şekildeki herhangi iki $u(z)$ ve $v(z)$ polinomu için $\sigma(z) = \beta v(z)$ ve $r(z) = \beta u(z)$ olacak şekilde sıfırdan farklı $\beta \in \mathbb{F}_{2^m}$ vardır.

Yukarıdaki teoremde bahsedilen

$$r(z) \equiv \sigma(z) S(z) \pmod{z^{\delta-1}}$$

denkliğindeki $r(z)$ ve $\sigma(z)$ polinomlarını bulabilmek için aşağıdaki gibi hareket edebiliriz:

Öklid algoritmasını kullanarak

$$z^{\delta-1} = q_1(z)s(z) + r_1(z), \quad \deg(r_1(z)) < \deg(s(z))$$
$$s(z) = q_2(z)r_1(z) + r_2(z), \quad \deg(r_2(z)) < \deg(r_1(z))$$
$$\vdots \qquad\qquad \vdots$$
$$r_{d-2}(z) = q_d(z)r_{d-1}(z) + r_d(z), \quad \deg(r_d(z)) < \deg(r_{d-1}(z))$$
$$r_{d-1}(z) = q_{d+1}(z)r_d(z)$$

eşitliklerini sağlayan $q_i(z)$ ve $r_i(z)$ polinomlarını bulalım. Aşağıdaki polinomları tanımlayalım:

$$y_{-1}(z) = 0, \quad y_0(z) = 1, \quad y_i(z) = y_{i-2}(z) - q_i(z)y_{i-1}(z)$$

$(i = 1, 2, \ldots, d)$.

Tümevarım ile aşağıdakilerin sağlandığını gösterebiliriz:

$r_{-1}(z) = z^{\delta-1}$ ve $r_0(z) = s(z)$ denirse

(i) her $i = -1, 0, \ldots, d$ için $r_i(z) = y_i(z)s(z) \pmod{z^{\delta-1}}$

ve

(ii) her $i = 0, 1, \ldots, d$ için $\deg(y_i(z)) = \delta - 1 - \deg(r_{i-1}(z))$.

Aşağıdaki lemma sayesinde $r(z)$ ve $\sigma(z)$ polinomlarını bulabiliriz.

LEMMA. Kabul edelim ki $s(z) = \sum_{i=0}^{\delta-2} s_i z^i$ sendrom polinomu sıfırdan farklı olsun. O zaman

(i) $r(z) \equiv s(z)\sigma(z) \pmod{z^{\delta-1}}$

(ii) $\deg(r(z)) \leq t-1$ ve

(iii) $\text{ebob}(r(z), \sigma(z)) = 1$ ve (iv) $\sigma(z) = \prod_{j=0}^{\ell-1} (1 - \alpha^{i_j} z)$

koşullarını sağlayan $r(z)$ ve $\sigma(z)$ polinomları için

b, $\deg(r_b(z)) \le t-1$ eşitsizliğini sağlayan en küçük indis olmak üzere

$$\sigma(z) = y_b(0)^{-1} y_b(z)$$

ve

$$r(z) = y_b(0)^{-1} r_b(z)$$

dir.

ÖRNEK. α, $g(x) = 1+x+x^3 \in \mathbb{F}_2[x]$ polinomunun bir kökü olsun. 7 uzunluklu ve tasarlanmış uzaklığı $\delta = 3$ olan dar anlamlı ikili BCH kodunu düşünelim. Bu kodun üreteç polinomu

$$\text{ekok}(M^{(1)}(x), M^{(2)}(x)) = 1+x+x^3 = g(x)$$

olur. (Aslında bu kod bir ikili Hamming kodudur.)

Şimdi $w(x) = 1+x+x^2+x^3$ alınmış olsun. $w(x)$ in sendromu

$$(S_0, S_1) = (w(\alpha), w(\alpha^2)) = (1+\alpha+\alpha^2+\alpha^3,\ 1+\alpha^2+\alpha^4+\alpha^6)$$
$$= (\alpha^2, \alpha^4)$$

bulunur. Bu hesaplamada $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ cisminin Zech logaritma tablosu kullanışlı olur.

i	$z(i)$
∞	0
0	∞
1	3
2	6
3	1
4	5
5	4
6	2

$\mathbb{F}_2(\alpha)$ cisminin Zech logaritma tablosu

$r(z) \equiv \sigma(z)s(z) \pmod{z^2}$ denkliğini çözelim.

Öklid algoritması ile

$$z^2 = (\alpha^3 z + \alpha)(\alpha^4 z + \alpha^2) + \alpha^3$$

$$\alpha^4 z + \alpha^2 = (\alpha z + \alpha^6)\alpha^3$$

bulunur. Buna göre $r_{-1}(z) = z^2$ $r_0(z) = \alpha^4 z + \alpha^2$ ve $r_1(z) = \alpha^3$ olur. $\deg(r_b(z)) \le t-1 = 1-1 = 0$ olacak şekildeki en küçük b, 1 olduğundan $y_1(z)$ yi bulmalıyız.

$$y_1(z) = \overbrace{y_{-1}(z)}^{0} - q_1(z)\overbrace{y_0(z)}^{1} = \alpha^3 z + \alpha$$

$q_1(0) = \alpha$ ve $q_1(0)^{-1} = \alpha^{-1} = \alpha^6$ olduğundan

$\sigma(z) = \alpha^6(\alpha^3 z + \alpha) = \alpha^2 z + 1$ elde edilir. $\sigma(z)$ nin tanımından $e(x) = x^2$ bulunur. Dolayısıyla $w(x)$ sözeüğü

$w(x) - x^2 = 1 + x + x^3 = 1101000$ şeklinde çözülür.

ÖRNEK. α, $x^4 + x + 1 \in \mathbb{F}_2[x]$ polinomunun bir kökü olsun. Bu durumda α, $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ cisminin bir ilkel elemanıdır. 15 uzunluklu ve tasarlanmış uzaklığı $\delta = 5$ olan dar anlamlı ikili BCH kodunu düşünelim.

$$M^{(1)}(x) = M^{(2)}(x) = M^{(4)}(x) = 1 + x + x^4$$

ve

$$M^{(3)}(x) = 1 + x + x^2 + x^3 + x^4$$

olduğundan bu kodun üreteç polinomu

$$\text{ekok}(M^{(1)}(x), M^{(2)}(x), M^{(3)}(x), M^{(4)}(x)) = M^{(1)}(x)M^{(3)}(x) = 1 + x^4 + x^6 + x^7 + x^8$$

olur. $w(x) = 1 + x^3 + x^6 + x^7 + x^{11}$ alınmış olsun. $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ cisminin Zech logaritma tablosu aşağıdaki gibidir.

i	$z(i)$	i	$z(i)$
∞	0	7	9
0	∞	8	2
1	4	9	7
2	8	10	5
3	14	11	12
4	1	12	11
5	10	13	6
6	13	14	3

Buna göre

$$S_0 = w(\alpha) = 1 + \alpha^3 + \alpha^6 + \alpha^7 + \alpha^{12} = 1$$

$$S_1 = w(\alpha^2) = 1 + \alpha^6 + \alpha^{12} + \alpha^{14} + \alpha^9 = 1$$

$$S_2 = w(\alpha^3) = 1 + \alpha^9 + \alpha^3 + \alpha^6 + \alpha^6 = \alpha^4$$

$$S_3 = w(\alpha^4) = 1 + \alpha^{12} + \alpha^9 + \alpha^{13} + \alpha^3 = 1$$

olacağından $w(x)$ in sendromu $S(x) = 1 + x + \alpha^4 x^2 + x^3$ olur. Şimdi $\sigma(z)$ polinomunu bulalım. Öklid algoritması ile

$r_0(z)$ $z^4 = \underbrace{(z + \alpha^4)}_{q_1(z)} S(z) + \underbrace{\alpha^2 z^2 + \alpha z + \alpha^4}_{r_1(z)}$

$S(z) = (\alpha^{13} z + \alpha^7)(\alpha^2 z^2 + \alpha z + \alpha^4) + \underbrace{\alpha^{12}}_{r_2(z)}$

$\alpha^2 z^2 + \alpha z + \alpha^4 = (\alpha^5 z^2 + \alpha^4 z + \alpha^7)\alpha^{12}$

elde edilir. $\deg(r_b(z)) \le t - 1 = 2 - 1 = 1$ olacak şekildeki en küçük b, 2 dir. ($r_2(z) = \alpha^{12}$). Buna göre $y_2(z)$ yi bulmalıyız.

$$y_{-1}(z) = 0, \quad y_0(z) = 1, \quad y_1(z) = -q_1(z) = z + \alpha^4$$

$$y_2(z) = y_0(z) - q_2(z)y_1(z) = 1 + (\alpha^{13}z + \alpha^7)(z + \alpha^4)$$
$$= 1 + \alpha^{13}z^2 + \alpha^2 z + \alpha^7 z + \alpha^{11}$$
$$= \alpha^{13}z^2 + \alpha^{12}z + \alpha^{12}$$

bulunur. $y_2(0)^{-1} = \alpha^3$ olduğundan

$$\sigma(z) = \alpha z^2 + z + 1$$

elde edilir.

$$\sigma(z) = (1 + \alpha^{i_0}z)(1 + \alpha^{i_1}z)$$

olduğunu biliyoruz. $\sigma(z)$ nin $\mathbb{F}_{16}$ içindeki iki kökü α^6 ve α^8 dir. Buna göre $i_0 = 9$ ve $i_1 = 7$ yazılabilir. Böylece $e(x) = x^7 + x^9$ bulunur. $w(x)$ sözcüğü

$$w(x) - e(x) = 1 + x^3 + x^6 + x^9 + x^{12}$$

olarak çözülür.