Für $j = 0,...,n-1$ sei

$N_0 := 1$

$N_j := \prod_{i=1}^{j}(X - \xi_i)$, $\operatorname{grad} N_i = j$

$N = N_n = \prod_{i=1}^{n}(X - \xi_i)$

5.4. $N_j(\xi_i) = 0 \quad \Leftrightarrow \quad j \le j$

Ansatz: $A = \alpha_0 + \alpha_1 N_1 + ... + \alpha_{n-1} N_{n-1}$, $\operatorname{grad} A = n$

$\alpha_0 + \alpha_1(X - \xi_1) + \alpha_2(X - \xi_2) + ... + \alpha_{n-1}(X - \xi_{n-1})$

$v_1 = A(\xi_1) = \alpha_0 N_0$

$v_2 = A(\xi_2) = \alpha_0 + \alpha_1(\xi_2 - \xi_1) \Rightarrow \alpha_1 = \frac{1}{\xi_2 - \xi_1}(v_2 - v_1)$

$\vdots$

$v_j = A(\xi_j) = \left(\sum_{i=0}^{j-2} \alpha_i N_i(\xi_j)\right) + \alpha_{j-1} N_{j-1}(\xi_j) \quad \Rightarrow \quad a_{j-1} = ...$

$\vdots$

$v_n = A(\xi_n) = \sum_{i=0}^{n-1} \alpha_i N_i(\xi_n) + \alpha_{n-1} \underbrace{N_{n-1}(\xi_n)}_{\neq 0} \quad \Rightarrow \quad a_{n=...}$

$1, N_1, ..., N_{n-1}$ (Newton-)Basis von $K_n[X]$

Bezüglich dieser Basis gehört zu val die Matrix:

$$V = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ * & \mu_1 & 0 & \vdots \\ \vdots & * & \ddots & \vdots \\ * & \cdots & * & \mu_{n-1} \end{pmatrix}, \quad \mu_i = N_i(\xi_{i+1}) \neq 0$$

$$v = \operatorname{val} A = V \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{n-1} \end{pmatrix}$$

$$V^{-1} = \begin{pmatrix} 1 & & & 0 \\ & \mu_1^{-1} & & \\ & & \ddots & \\ * & & & \mu_{n-1}^{-1} \end{pmatrix}$$

$$\begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = \underbrace{V^{-1} \cdot v}_{\Pi v \text{ ist das Polynom } A}$$

$K_n[X]$ mit val $A = v$

Voraussetzung 1: $\xi_i^n = 1 \quad \forall i = 1,..,n$

$$N = (X - \xi_1)\cdots(X - \xi_n) \overset{!}{=} X^n - 1$$

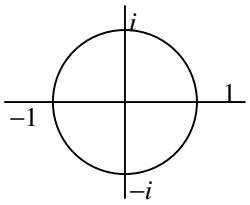
denn $\xi_i^n - 1 = 0$

ξ_i ist Nullstelle von $X^n - 1$

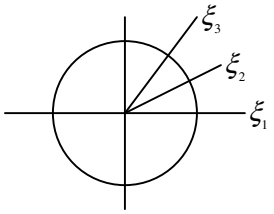
Bemerkungen:

$K = \mathbb{C}$, $\xi_1,...,\xi_n$ die n-ten Einheitswurzeln

$n = 4$



Allgemein:



n "Tortenstücke"

$1 = \xi_1$

$\xi_2 = \cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}$

$\xi_3 = \xi_2^{\,2}$

$K = \mathbb{R}$

$n = 2$

$\xi_1 = 1,\ \xi_2 = -1$

Sei K ein endlicher Körper, dann ist K^* eine zyklische Gruppe der Ordnung n

$\xi_1,...,\xi_n$ sind die Elemente $\neq 0$ in K

$|K| = 2^8 = 256$

$K = \mathrm{GF}(2^8)$ (Galousfeld)

$n = 255$

Unter der Voraussetzung 1 bilden $\xi_1,...,\xi_n$ eine zyklische Gruppe der Ordnung n

d.h. Es existiert ein $\beta \in \{\xi_1,...,\xi_n\}$, so dass jedes ξ_i eine Potenz von β ist

Sei Œ $\xi_1 = \beta^0 = 1,\ \xi_2 = \beta,\ \xi_3 = \beta^2,...,\xi_n = \beta^{n-1}$

Eine kleine Rechnung: $n \in \mathbb{N}$ (nach Voraussetzung : $|E_n| = n$)

$E_n = \{\lambda \in K \mid \lambda^n = 1\}$ Gruppe der n-ten Einheitswurzeln in K

5.6. $\lambda \in E_n$ und $i, j \in \{0,...,n-1\}$

a) $$\sum_{k=0}^{n-1} \lambda^k = \begin{cases} 0 & falls \quad \lambda \neq 1 \\ \overline{n} & falls \quad \lambda = 1 \end{cases}$$

$$n = \underbrace{1+1+...+1}_{n}$$

b) $$\sum_{k=0}^{n-1} \lambda^{ki} \lambda^{-kj} = \begin{cases} 0 & falls \quad i \neq j \\ \overline{n} & falls \quad i = j \end{cases}$$

Beweis von a)

$$s := 1 + \lambda + \lambda^2 + ... + \lambda^{n-1}$$

$$\lambda \cdot s = \lambda + \lambda^2 + ... + \lambda^{n-1} + \cancel{\lambda^n}_{1} = s$$

zu b) $$\sum_{k=0}^{n-1} \lambda^{ki} \lambda^{-kj} = \sum_{k=0}^{n-1} \underbrace{\lambda^{k(i-j)}}_{\left(\lambda^{(i-j)}\right)^k \in E_n} = 0 \quad \text{falls} \quad i \neq j$$

5.7. Das Produkt der Vandermonden Matrizen $\mathrm{Vand}_{\xi_1,...,\xi_n}(n,n)$ und $\mathrm{Vand}_{\eta_1,...,\eta_n}(n,n)$ ist die Diagonalmatrix $\begin{pmatrix} n & & 0 \\ & \ddots & \\ 0 & & n \end{pmatrix}$

$$\eta_i = \beta_i^{-1} = \left(\beta^{i-1}\right)^{-1} = \beta^{-(i-1)} = ... \quad i = 1,...,n$$

$$V = \mathrm{Vand}_{\xi_1,...,\xi_n}(n,n) = \begin{pmatrix} 1 & \xi_1^1 & \cdots & \xi_1^{n-1} \\ & \ddots & & \\ 1 & \xi_i^1 & & \xi_i^{n-1} \\ & & & \end{pmatrix} \quad i\text{-te Zeile}$$

$$\mathrm{Vand}_{\eta_1,...,\eta_n}(n,n) = \begin{pmatrix} & \eta_1^{j-1} & \\ & \eta_2^{j-1} & \\ & \vdots & \\ & \eta_n^{j-1} & \end{pmatrix} \quad j\text{-te Spalte}$$

$$\sum_{k=1}^{n} \xi_i^{(k-1)} \eta_k^{(j-1)} = \sum_{k=1}^{n} \beta^{(k-1)(i-1)} \beta^{(k-1)(j-1)}$$

$$\sum_{k=1}^{n-1} \beta^{k(i-1)} \beta^{-(j-1)k} = \begin{cases} 0 & falls \quad i \neq j \\ \overline{n} & falls \quad i = j \end{cases}$$

Voraussetzung 2: $\overline{n} \neq 0$

$\Rightarrow$ Die Matrix $W := \frac{1}{\overline{n}} \cdot \mathrm{Vand}_{\eta_1,\ldots,\eta_n}(n,n)$ ist die zu $\mathrm{Vand}_{\xi_1,\ldots,\xi_n}(n,n)$ inverse Matrix

Erinnerung: $A = \sum_{i=1}^{n} a_i X^{i-1} \in K_n[X]$, $\kappa(A) = (a_1,..,a_n)$ Koeffiziententupel

$\kappa: K_n[X] \to K^n$ Isomorphismus

$v \in K^n$, Πv das Polynom A in $K_n[X]$ mit $\mathrm{val}\, A = N$

$v = (v_1,\ldots,v_n) \in K^n$

$\Theta(v) := \sum_{i=1}^{n} v_i X^{i-1} \in K_n[X]$

5.8. Satz

$$\kappa(\Pi v) = \frac{1}{\overline{n}} \cdot \left(\mathrm{val}_{\eta_1,\ldots,\eta_n}\, \Theta(v)\right)$$

Beweis: $a := \kappa(\Pi v) = (a_1,\ldots,a_n)$

$v = V \cdot a$

$\mathrm{val}_{\eta_1,\ldots,\eta_n}\, \Theta(v) = (\overline{n} \cdot W) \cdot v = \overline{n} \cdot \underbrace{W \cdot V}_{=1_n} \cdot a = \overline{n} \cdot a$

6. Reed-Solomon-Codes

$1 \leq k \leq n$

1) Eine Information $a = (a_1,..,a_k) \in K^k$

Seien $\xi_1,\ldots,\xi_n$ verschiedene Stützstellen im K

$A = a_1 + a_2 X + \ldots + a_k X^{k-1} \in K_k[X]$

$y := (A(\xi_1),\ldots,A(\xi_n)) = \mathrm{val}\, A \in K^n$

$C = \{\mathrm{val}\, A \mid A \in K_k[X]\}$ ist Unterraum der Dimension k von K^n

=**Reed-Solomon-Code** $= \mathrm{RS}_{\xi_1,\ldots,\xi_n}(n.k)$

Beispiel:

$y \in C$

$a \xrightarrow{\text{coded}} y \xrightarrow{\text{durch gestörten Kanal}} \hat{y} \in K^n$

Aufgabe: Rekonstruiere y (und dann a) aus $\hat{y}$

Annahme: Höchstens t Stellen von $\hat{y}$ sind falsch