$1 \le R \le n$

$a = (a_0, ..., a_{k-1}) \in K^k$ Information

$\xi_1, ..., \xi_n$ verbinden Elemente aus K

$A = a_0 + a_1 X + ... + a_{k-1} X^{k-1} \in K_k[X]$

$y = (A(\xi_1), ..., A(\xi_n)) = \mathrm{val}_{\xi_1,...,\xi_n}(A)$

$y \sim> \tilde{y} \in K^n$

$RS_{\xi_1,...,\xi_n}(n,k) = \left\{ y \in K^n \middle| y = \mathrm{val}_{\xi_1,...,\xi_n}(A),\ A \in K^k[X] \right\}$

Unterraum der Dimension k von K^n

Bezeichnung für $y = (y_1, ..., y_n) \in K^n$, $x = (x_1, ..., x_n) \in K^n$

$d(x,y) := \left| \{ i \in \{1, ..., n\} \} \middle| x_i \ne y_i \right|$ **Hammingdistanz**

6.1. $d(x,y) = d(y,x)$

$d(x,y) = 0 \Rightarrow x = y$

$C \subseteq K^n$ (Code)

$d_C \overset{\text{def.}}{=} \min \{ d(x,y) | x \ne y \text{ aus } C \}$ **Minimumdistanz**

$w(x) := d(x,0)$ Gewicht von $x \in K^n$

$d(x,y) = w(x-y)$

Sei C ein Unterraum von K^n (linearer Code)

$d_C = \min \{ w(x) | x \ne 0 \text{ aus } C \}$

6.2. Satz

Sei $C = RS(n,k)$, dann ist $d_C = n - k + 1$

Beweis: 1) $A = \prod_{i=1}^{k-1} (X - \xi_i) \in K^k[X]$

$y = \mathrm{val}\, A \Rightarrow w(y) = n - (k-1)$

$y_1 = ... = y_{k-1} = 0,\ y_k, ..., y_n \ne 0$

2) Sei $y \in C$ und $w(y) \le n - k$, $y = \mathrm{val}\, A$

$\Rightarrow A$ hat mindestens $n - (n-k) = k$ Nullstellen

$\mathrm{grad}\, A \le k \Rightarrow A = 0 \Rightarrow y = 0$

Allgemeine Betrachtung

$C \subseteq K^n$ (Code)

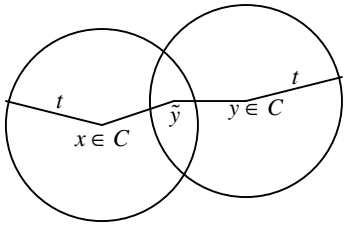
$y \in C \overset{\sim>}{\underset{\text{Kanal}}{}} \tilde{y} \in K^n$

Voraussetzung: $\exists t \in \mathbb{N}$ mit $d(y,\tilde{y}) \le t \quad 1 \le t \le n$

6.3. Ist $d_C \ge 2t+1$, so kann (prinzipiell) decodiert werden.

Genauer: $\exists!\ x \in C$ mit $d(x,\tilde{y}) \le t$, nämlich $x = y$

Beweis:



$$d(x,y) \le \underbrace{d(x,\tilde{y})}_{\le t} + \underbrace{d(y,\tilde{y})}_{\le t} \quad \Rightarrow \quad d(x,y) \le 2t$$

$n - k = 2t \quad d_C \ge 2t+1$

$y \sim> \tilde{y} \quad d(y,\tilde{y}) \le t$

Decodierung von $\tilde{y}$

1) Bestimme $B \in K_n[X]$ mit $\text{val}_{\xi_1,\dots,\xi_n} B = \tilde{y}$

$\left(B = \prod_{\xi_1,\dots,\xi_n} \tilde{y}\right) \qquad B(\xi_i) = \tilde{y}_i$

B Empfangspolynom

2) Bezeichnung: $E := B - A$ Fehlerpolynom

$F = \{i \in \{1,\dots,n\} \mid y_i + \tilde{y}_i\}$ Fehlerstellenmenge $|F| \le t$

$R = \{i \in \{1,\dots,n\} \mid y_i = \tilde{y}_i\} \quad |R| \ge n - t$

$P := \prod_{i \in F} (X - \xi_i)$ Fehlerstellenpolynom $\text{grad}\, P \le t$

$i \in R \ \Leftrightarrow\ E(\xi_i) = 0 \ \Leftrightarrow\ (X - \xi_i)$ Teiler von E

$B(\xi_i) - A(\xi_i) = \tilde{y}_i - y_i$

6.3. a) $\text{ggT}(E,N) = \prod_{i \in R} (X - \xi_i)$, wobei $N = \prod_{i=1}^{n} (X - \xi_i)$

b) $P = \dfrac{N}{\text{ggT}(E,N)}$

c) Sei $Q := \dfrac{E}{\text{ggT}(E,N)}$. Dann ist $PE = QN = \text{kgV}(E,N)$

6.4. $A = B - \underbrace{\frac{QN}{P}}_{E}$

3) Berechne P, Q mit Hilfe des erweiterten Algorithmus.
In jedem Schritt (Division) wird ein Rest R_i und ein
Polynom P_i, Q_i berechnet $Q_i N = P_i E + R_i$

6.5. Ist $R_i \neq 0$, so ist grad $R_i \geq n - t$
Ist grad $R_i < n - t$, so ist $R_i = 0$
Setze $P = P_i$, $Q := -Q_i$

4) Problem B aber nicht $E = B - A$ ist bekannt
Sei $B = \sum_{i=0}^{n-1} b_i X^i$, $E = \sum_{i=0}^{n-1} e_i X^i$

6.6. $b_i = e_i$ für $i = k, k+1, ..., n-1$

$$i = \underbrace{k, k+1, ..., k + (2t-1)}_{2t \text{ Zahlen}}$$

Die letzten $2t$ Koeffizienten von B sind die von E

z.B. die 1. Division:
grad $\underset{n}{N} : \underset{n-1}{E}$
Multipliziere E mit X und subtrahiere $e_{n-1} N$
$\Rightarrow E_1$ i.A. grad $E_1 = n - 1$
höchster Koeffizient ist e_{n-2} von E_1 (wenn $N = X^n - 1$)
subtrahiere geeignetes Vielfaches von E_1 von E_2

5) P und Q seien berechnet
Praxisnah:
$$P(\xi_i) = 0 \Leftrightarrow i \in F$$

Bestimme die Nullstellen von $P \Rightarrow F$
$\Rightarrow R$, $|R| \geq n < t \geq k \Rightarrow A$
Besser: $E = \frac{QN}{P}$
$$E(\xi_i) = B(\xi_i) - A(\xi_i) = \tilde{y}_i - y_i \quad i \in F$$
$$\tilde{y}_i - y_i \quad E(\xi_i) = \frac{Q(\xi_i) N(\xi_i)}{\underbrace{P(\xi_i)}_{=0}}$$
ξ_i ist eine einfache Nullstelle von P

Regel von de l'Hopital

$$\frac{(QN)'}{P'} = \frac{Q'N + N'Q}{P'}$$

$$E(\xi_i) = \frac{Q'(\xi_i)N(\xi_i) + N'(\xi_i)Q(\xi_i)}{\underbrace{P'(\xi_i)}_{\neq 0}} = \frac{N'(\xi_i)Q(\xi_i)}{P'(\xi_i)} \Rightarrow y_i$$

$\Rightarrow y = (y_1, ..., y_n)$ ist rekonstruiert $\overset{\text{Interpolation}}{\sim>}$ A

In der Praxis K endlicher Körper ($= GF(2^8)$)

K^* ist eine zyklische Gruppe. $|K^*| = n$

$K^* = \{1, \beta, \beta^2, ..., \beta^{n-1}\}$

$\xi_1 = 1, \xi_2 = \beta, ..., \xi_i = \beta^{(i-1)}, ..., \xi_n = \beta^{(n-1)}$

$\eta_1 = 1, \eta_2 = \beta^{-1}, ..., \eta_i = \beta^{-(i-1)}, ..., \eta_n = \beta^{-(n-1)}$

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

$\bar{n} = \underbrace{1 + ... + 1}_{n} \in K$

zu 5.8. $y = (y_1, ..., y_n) \in K^n$

$\Phi_y = y_1 + y_2 X + ... + y_n X^{n-1} \in K_n[X]$

$k(\Pi y) = \frac{1}{n} \text{val}_{\eta_1, ..., \eta_n}(\Phi_y)$

6.7. $y \in RS_{\xi_1, ..., \xi_n}(n, k) \Leftrightarrow \text{grad}\,\Pi y < k$

$\Leftrightarrow \Phi_y(\eta_{k+1}) = ... = \Phi_y(\eta_n) = 0$

$\Leftrightarrow \underbrace{(X - \eta_{k+1})(X - \eta_{k+2})...(X - \eta_n)}_{G \text{ Generatorpolynom grad } G = n-k}$ teilt Φ

$\Leftrightarrow \exists A \in K_k[X]$ mit $\Phi_y = AG$