C1/4 - Mathematik von RS-Codes

Merovius

July 12, 2012

Sei $\mathbb{F}_2 := \{0, 1\}$ mit den Operationen $+, \cdot$, gegeben durch

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Sei $\mathbb{F}_2 := \{0, 1\}$ mit den Operationen $+, \cdot$, gegeben durch

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{F}_2$ ist ein Körper, d.h. wir können wie gewohnt addieren, subtrahieren, multiplizieren und dividieren.

Sei $\mathbb{F}_2 := \{0, 1\}$ mit den Operationen $+, \cdot$, gegeben durch

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{F}_2$ ist ein Körper, d.h. wir können wie gewohnt addieren, subtrahieren, multiplizieren und dividieren.
Eine Besonderheit ist:

$$\forall a \in \mathbb{F}_2 \colon a + a = 0$$

Wir können jetzt Polynome über $\mathbb{F}_2$ betrachten:

$$\mathbb{F}_2[T] := \left\{ \sum_{i=0}^{n} a_i T^i \mid n \in \mathbb{N}, a_i \in \mathbb{F}_2 \right\}$$

Wir können jetzt Polynome über $\mathbb{F}_2$ betrachten:

$$\mathbb{F}_2[T] := \left\{ \sum_{i=0}^{n} a_i T^i \mid n \in \mathbb{N}, a_i \in \mathbb{F}_2 \right\}$$

Durch Koeffizientenweise Addition und die „natürliche“ Multiplikation erhalten wir einen Ring

Wir können jetzt Polynome über $\mathbb{F}_2$ betrachten:

$$\mathbb{F}_2[T] := \left\{ \sum_{i=0}^{n} a_i T^i \mid n \in \mathbb{N}, a_i \in \mathbb{F}_2 \right\}$$

Durch Koeffizientenweise Addition und die „natürliche“ Multiplikation erhalten wir einen Ring
Auch hier gilt: $\forall f \in \mathbb{F}_2 : f + f = 0$

Wir können jetzt Polynome über $\mathbb{F}_2$ betrachten:

$$\mathbb{F}_2[T] := \left\{ \sum_{i=0}^{n} a_i T^i \mid n \in \mathbb{N}, a_i \in \mathbb{F}_2 \right\}$$

Durch Koeffizientenweise Addition und die „natürliche“ Multiplikation erhalten wir einen Ring
Auch hier gilt: $\forall f \in \mathbb{F}_2 : f + f = 0$
Wir können Polynome auswerten und erhalten so eine Polynomfunktion:

$$f : \mathbb{F}_2 \to \mathbb{F}_2$$

$$x \mapsto f(x) = \sum_{i=0}^{n} a_i x^i$$

Wir haben auf $\mathbb{F}_2$ eine Division mit Rest:

$$\forall f, g \in \mathbb{F}_2[T] : \exists q, r \in \mathbb{F}_2[T] : f = q \cdot g + r, \deg(r) < \deg(g)$$

Wir haben auf $\mathbb{F}_2$ eine Division mit Rest:

$$\forall f, g \in \mathbb{F}_2[T] : \exists q, r \in \mathbb{F}_2[T] : f = q \cdot g + r, \deg(r) < \deg(g)$$

Ist f *irreduzibel* (d.h. es existieren keine $h, g \in \mathbb{F}_2[T]$ mit $\deg(h), \deg(g) > 1$ und $f = gh$), dann können wir bezüglich f „reduzieren“:

$$g \sim h \Leftrightarrow \exists q \in \mathbb{F}_2[T] : h = qf + g$$

und erhalten so einen Körper $K := {}^{\mathbb{F}_2[T]}/_{f}$, mit $2^{\deg(f)}$ Elementen.

Wir haben auf $\mathbb{F}_2$ eine Division mit Rest:

$$\forall f, g \in \mathbb{F}_2[T] : \exists q, r \in \mathbb{F}_2[T] : f = q \cdot g + r, \deg(r) < \deg(g)$$

Ist f *irreduzibel* (d.h. es existieren keine $h, g \in \mathbb{F}_2[T]$ mit $\deg(h), \deg(g) > 1$ und $f = gh$), dann können wir bezüglich f „reduzieren“:

$$g \sim h \Leftrightarrow \exists q \in \mathbb{F}_2[T] : h = qf + g$$

und erhalten so einen Körper $K := {}^{\mathbb{F}_2[T]}/_{f}$, mit $2^{\deg(f)}$ Elementen. Immer noch gilt $\forall f \in K : f + f = 0$.

Wir haben auf $\mathbb{F}_2$ eine Division mit Rest:

$$\forall f, g \in \mathbb{F}_2[T] : \exists q, r \in \mathbb{F}_2[T] : f = q \cdot g + r, \deg(r) < \deg(g)$$

Ist f *irreduzibel* (d.h. es existieren keine $h, g \in \mathbb{F}_2[T]$ mit $\deg(h), \deg(g) > 1$ und $f = gh$), dann können wir bezüglich f „reduzieren“:

$$g \sim h \Leftrightarrow \exists q \in \mathbb{F}_2[T] : h = qf + g$$

und erhalten so einen Körper $K := {}^{\mathbb{F}_2[T]}/_{f}$, mit $2^{\deg(f)}$ Elementen.
Immer noch gilt $\forall f \in K : f + f = 0$.
Wir betrachten jetzt $R := K[T]$, also den Polynomring mit Koeffizienten in K.

Jedes Wort unserer Nachricht betrachten wir jetzt als ein Element von K.

Jedes Wort unserer Nachricht betrachten wir jetzt als ein Element von K.
Uns interessiert hauptsächlich $n = 8$ ($n = 16, \ldots$), dann interpretieren wir `uint8_t` (`uint16_t`,...) als Elemente von $\mathbb{F}_2[T]$ (und damit von K):

$$b_7 \ldots b_0 \mapsto \sum_{i=0}^{7} b_i T^i$$

Theorem

Sei $f \in K[T]$ *ein Polynom,* $\deg(f) < n$. *Seien* $a_1, \ldots, a_n \in K$, *sodass* $f(a_i) = 0$, *für* $i = 1, \ldots, n$. *Dann ist* $f = 0$

Theorem

Sei $f \in K[T]$ ein Polynom, $\deg(f) < n$. *Seien $a_1, \ldots, a_n \in K$, sodass $f(a_i) = 0$, für $i = 1, \ldots, n$. Dann ist $f = 0$*

Daraus folgt, dass, wenn man die Werte eines Polynoms an n Stellen vorgibt, dass dann auch das Polynom eindeutig ist.

Theorem

Sei $f \in K[T]$ ein Polynom, $\deg(f) < n$. Seien $a_1, \ldots, a_n \in K$, sodass $f(a_i) = 0$, für $i = 1, \ldots, n$. Dann ist $f = 0$

Daraus folgt, dass, wenn man die Werte eines Polynoms an n Stellen vorgibt, dass dann auch das Polynom eindeutig ist.
Das Polynom f, mit $\deg(f) < n$, welches an den Stellen $x_1, \ldots, x_n$ die Werte $y_1, \ldots, y_n$ annimmt, ist gegeben durch

$$f = \sum_{i=0}^{n} y_i \underbrace{\prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{T - x_j}{x_i - x_j}}_{=:L_i}$$

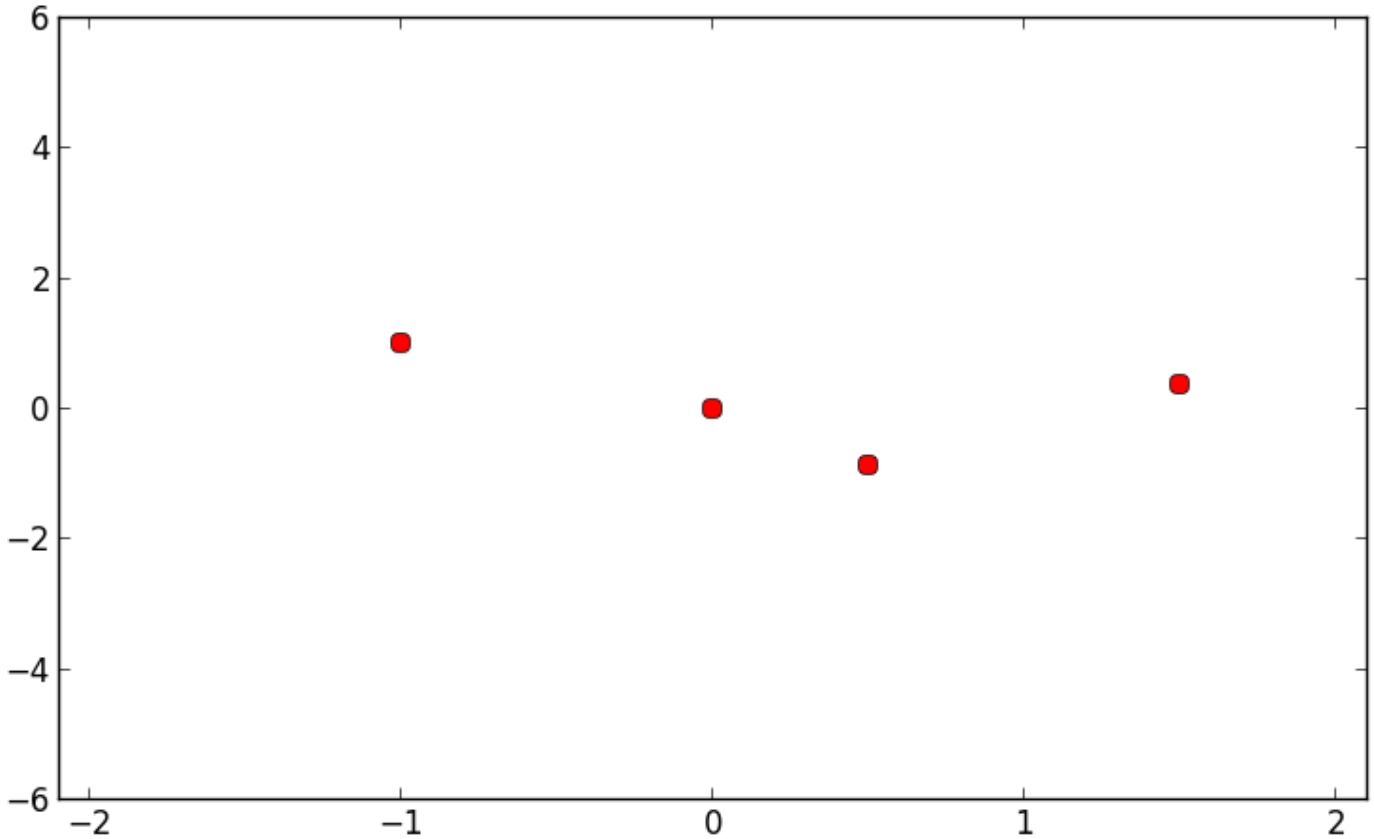
Theorem

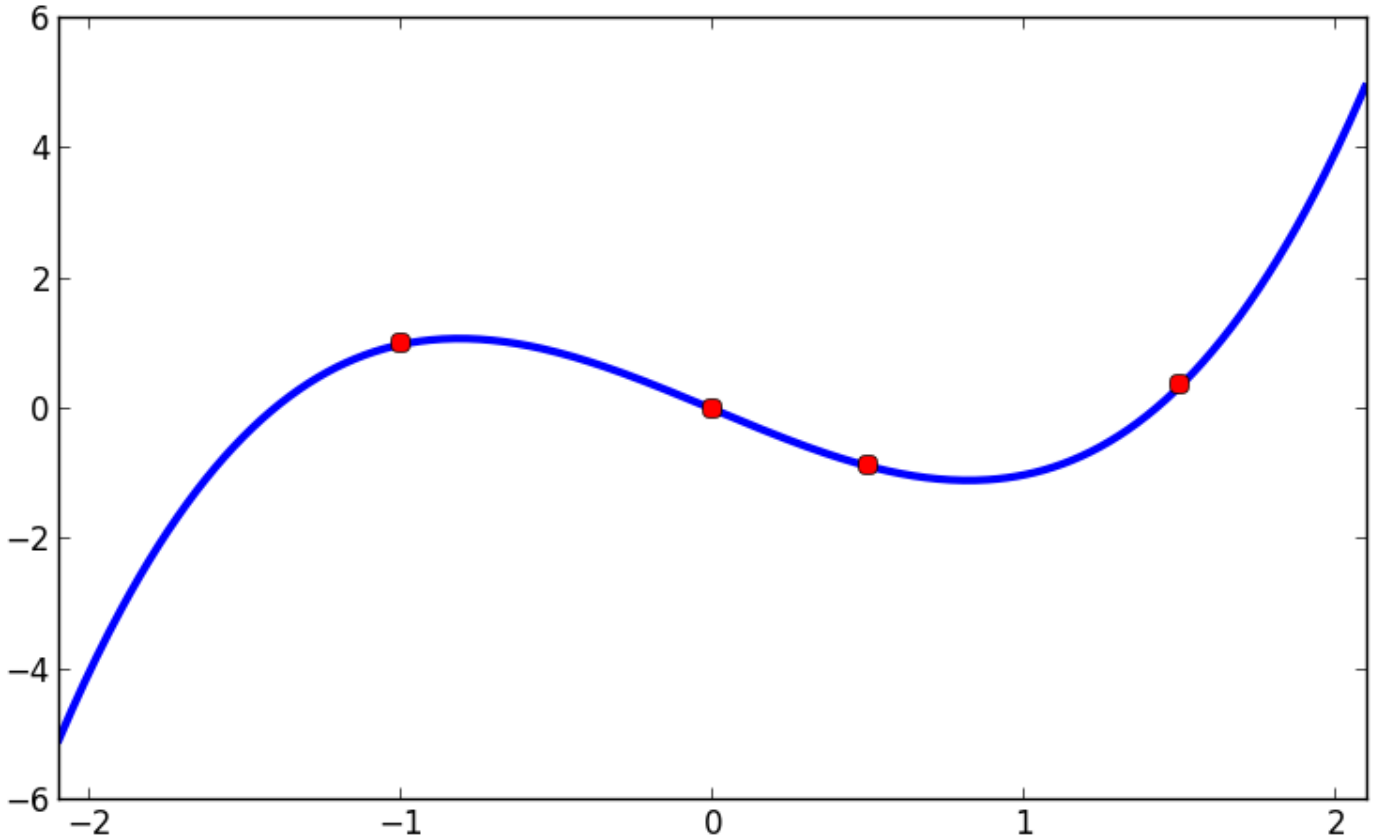
Sei $f \in K[T]$ ein Polynom, $\deg(f) < n$. Seien $a_1, \ldots, a_n \in K$, sodass $f(a_i) = 0$, für $i = 1, \ldots, n$. Dann ist $f = 0$

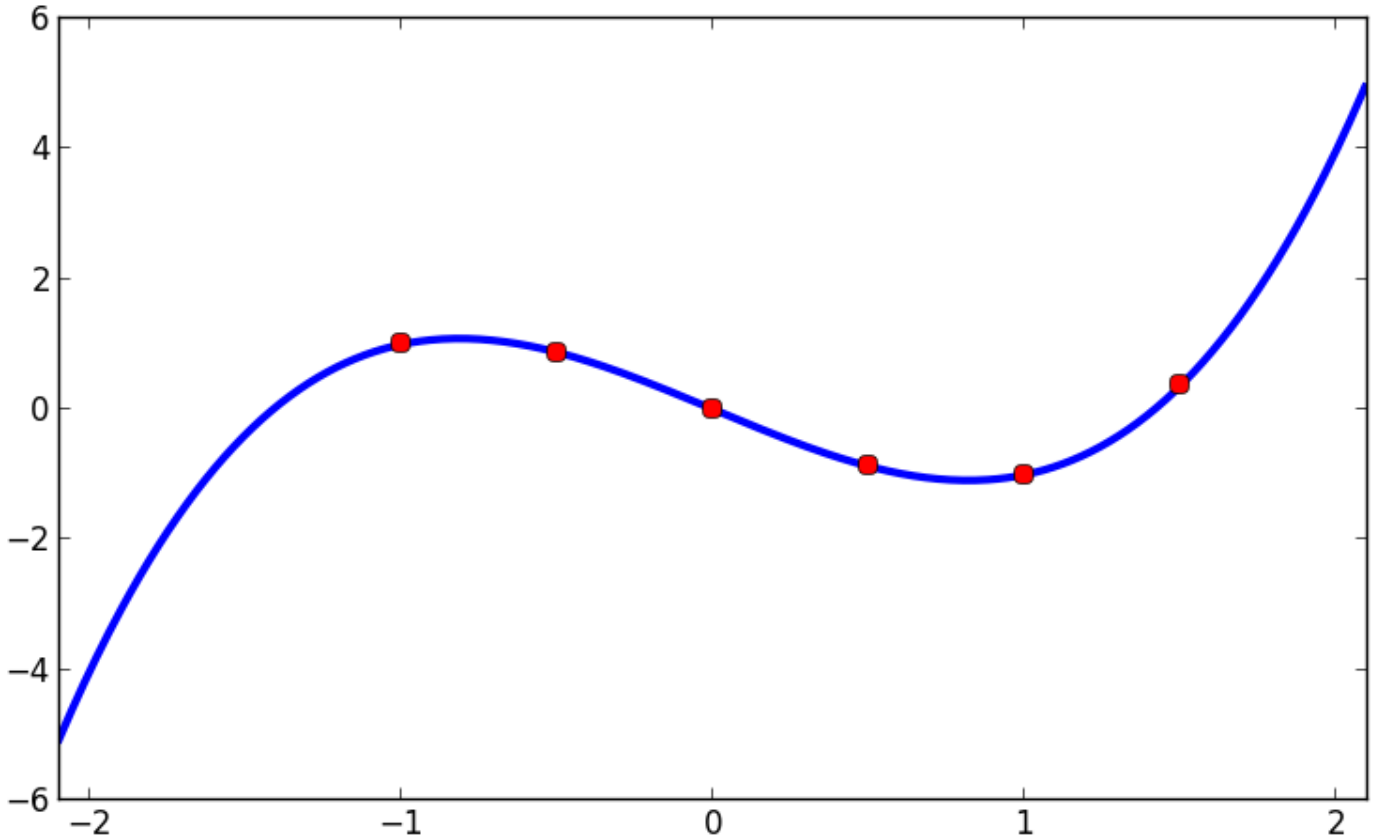
Daraus folgt, dass, wenn man die Werte eines Polynoms an n Stellen vorgibt, dass dann auch das Polynom eindeutig ist.
Das Polynom f, mit $\deg(f) < n$, welches an den Stellen $x_1, \ldots, x_n$ die Werte $y_1, \ldots, y_n$ annimmt, ist gegeben durch

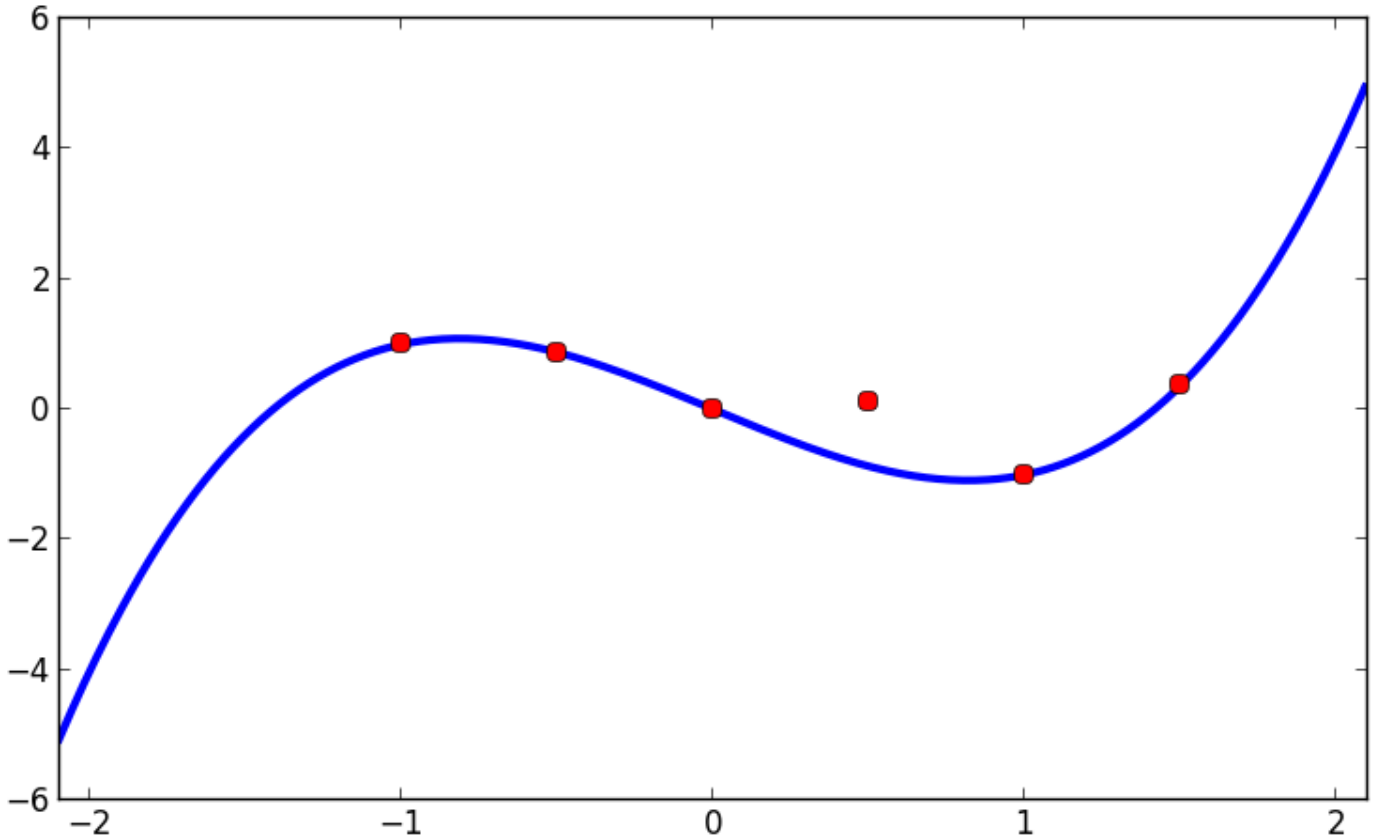
$$f = \sum_{i=0}^{n} y_i \underbrace{\prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{T - x_j}{x_i - x_j}}_{=:L_i}$$

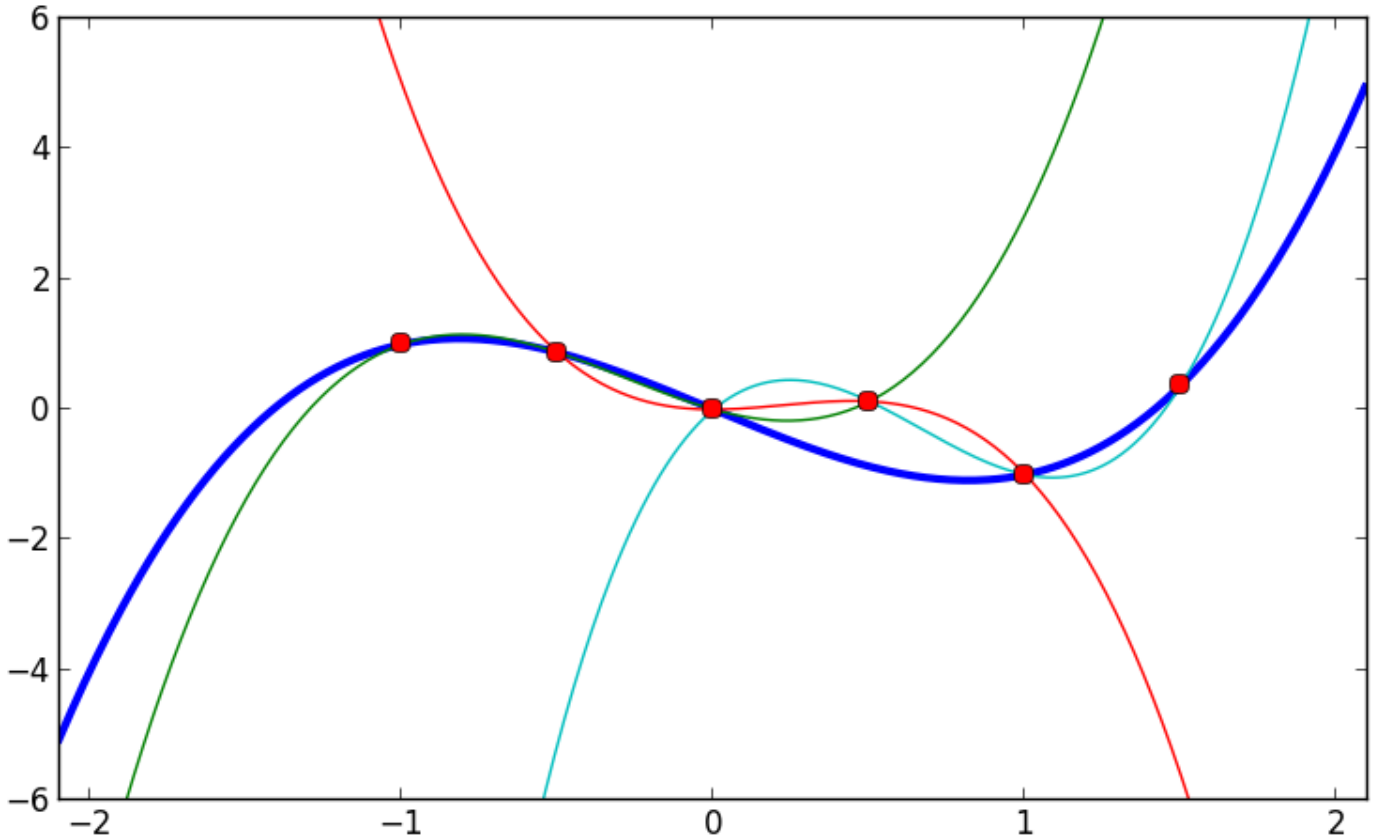
Wir interpretieren unsere Nachrichten als Polynome, die Eindeutigkeitseigenschaften geben uns dann die Fehlerkorrektureigenschaften.

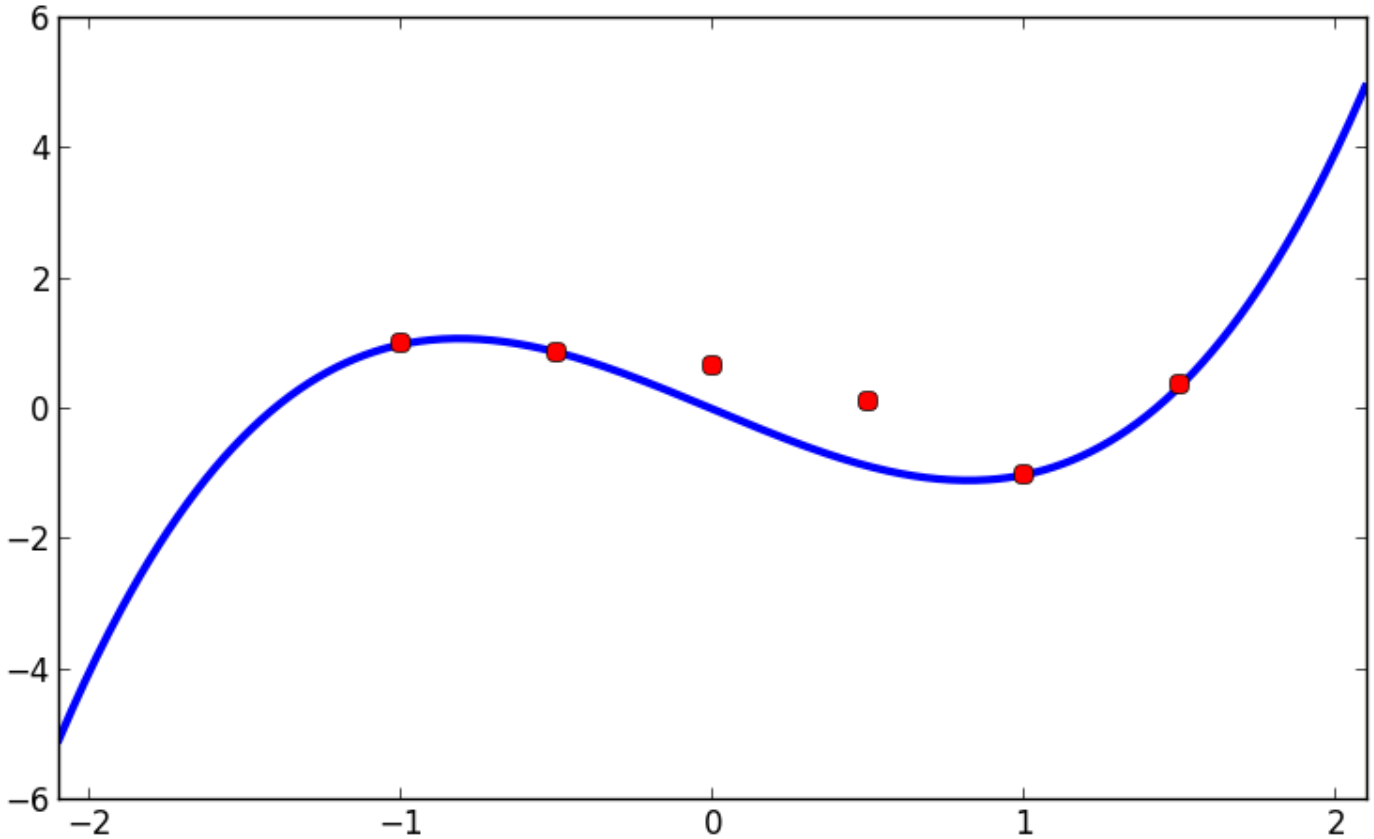

6
4
2
0
−2
−4
−6
−2
−1
0
1
2

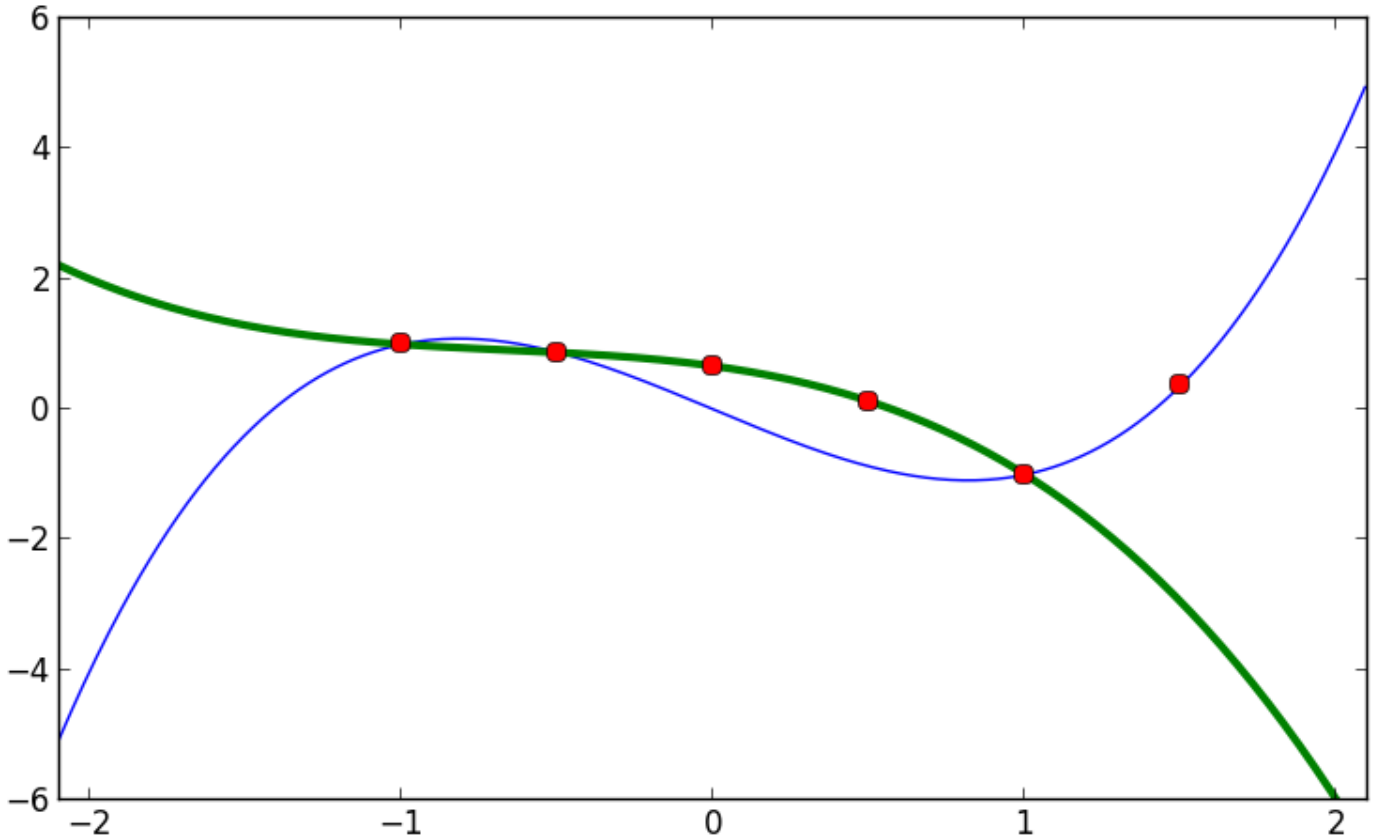

6
4
2
0
−2
−4
−6
−2
−1
0
1
2


6
4
2
0
−2
−4
−6
−2
−1
0
1
2


6
4
2
0
−2
−4
−6
−2
−1
0
1
2


6
4
2
0
−2
−4
−6
−2
−1
0
1
2


6
4
2
0
−2
−4
−6
−2
−1
0
1
2


6
4
2
0
−2
−4
−6
−2
−1
0
1
2

Allgemein: Wir übermitteln ein Polynom vom Grad m, indem wir es an $m + k$ Punkten auswerten und die Werte übertragen.

Allgemein: Wir übermitteln ein Polynom vom Grad m, indem wir es an $m + k$ Punkten auswerten und die Werte übertragen.
Wir dekodieren, indem wir versuchen, ein Polynom vom Grad m durch $m + \frac{k}{2}$ Punkte zu legen.

Allgemein: Wir übermitteln ein Polynom vom Grad m, indem wir es an $m + k$ Punkten auswerten und die Werte übertragen.
Wir dekodieren, indem wir versuchen, ein Polynom vom Grad m durch $m + \frac{k}{2}$ Punkte zu legen.

- Bis zu k Ausfälle können korrigiert werden.

Allgemein: Wir übermitteln ein Polynom vom Grad m, indem wir es an $m + k$ Punkten auswerten und die Werte übertragen.
Wir dekodieren, indem wir versuchen, ein Polynom vom Grad m durch $m + \frac{k}{2}$ Punkte zu legen.

- Bis zu k Ausfälle können korrigiert werden.
- Bis zu $\frac{k}{2}$ Fehler können korrigiert werden.

Allgemein: Wir übermitteln ein Polynom vom Grad m, indem wir es an $m + k$ Punkten auswerten und die Werte übertragen.
Wir dekodieren, indem wir versuchen, ein Polynom vom Grad m durch $m + \frac{k}{2}$ Punkte zu legen.

- Bis zu k Ausfälle können korrigiert werden.
- Bis zu $\frac{k}{2}$ Fehler können korrigiert werden.

Offensichtlich muss $m + k \leq \#K$ gelten.

Allgemein: Wir übermitteln ein Polynom vom Grad m, indem wir es an $m + k$ Punkten auswerten und die Werte übertragen.
Wir dekodieren, indem wir versuchen, ein Polynom vom Grad m durch $m + \frac{k}{2}$ Punkte zu legen.

- Bis zu k Ausfälle können korrigiert werden.
- Bis zu $\frac{k}{2}$ Fehler können korrigiert werden.

Offensichtlich muss $m + k \leq \#K$ gelten.
Diese Formulierung ist mitlerweile veraltet.

Definition

Sei

$$f = \sum_{i=0}^{n-1} f_i T^i,$$

α eine primitive n-te Einheitswurzel.
Dann heißt

$$g = \sum_{i=0}^{n-1} f(\alpha^i) T^i = \sum_{i,j=0}^{n-1} f_j \alpha^{ij} T^i$$

die *diskrete Fouriertransformierte* von f.

Definition

Sei

$$f = \sum_{i=0}^{n-1} f_i T^i,$$

α eine primitive n-te Einheitswurzel.
Dann heißt

$$g = \sum_{i=0}^{n-1} f(\alpha^i) T^i = \sum_{i,j=0}^{n-1} f_j \alpha^{ij} T^i$$

die *diskrete Fouriertransformierte* von f.

Die diskrete Fouriertransformation lässt sich umkehren per

$$g \mapsto \frac{1}{n} \sum_{i=0}^{n-1} g(\alpha^{-i}) T^i$$

Polynomwerte $\mapsto$ Koeffizienten.

Polynomwerte $\mapsto$ Koeffizienten.

$$g := \prod_{i=1}^{k} (T - \alpha^i)$$

Polynomwerte $\mapsto$ Koeffizienten.

$$g := \prod_{i=1}^{k} (T - \alpha^i)$$

$$f \mapsto s = (f \cdot X^k) - (f \cdot X^k \mod g)$$

Polynomwerte $\mapsto$ Koeffizienten.

$$g := \prod_{i=1}^{k} (T - \alpha^i)$$

$$f \mapsto s = (f \cdot X^k) - (f \cdot X^k \mod g)$$

$$\Rightarrow s \mod g = (f \cdot X^k - f \cdot X^k) \mod g = 0$$

Polynomwerte $\mapsto$ Koeffizienten.

$$g := \prod_{i=1}^{k} (T - \alpha^i)$$

$$f \mapsto s = (f \cdot X^k) - (f \cdot X^k \mod g)$$

$$\Rightarrow s \mod g = (f \cdot X^k - f \cdot X^k) \mod g = 0$$

Unsere Codeworte sind also Polynome, die durch g teilbar sind.

Angenommen, es ist ein Fehler aufgetreten:

$$\hat{s} = s + e$$

Angenommen, es ist ein Fehler aufgetreten:

$$\hat{s} = s + e$$

Zur Fehlererkennung setzen wir α^i mit $i = 1, \ldots, k$ ein:

$$\hat{s}(\alpha^i) = s(\alpha^i) + e(\alpha^i)$$

und da $g \mid s \Rightarrow s(\alpha^i) = 0$:

$$S_i := \hat{s}(\alpha^i) = e(\alpha^i)$$

(*Syndrome*)

Angenommen, es ist ein Fehler aufgetreten:

$$\hat{s} = s + e$$

Zur Fehlererkennung setzen wir α^i mit $i = 1, \ldots, k$ ein:

$$\hat{s}(\alpha^i) = s(\alpha^i) + e(\alpha^i)$$

und da $g \mid s \Rightarrow s(\alpha^i) = 0$:

$$S_i := \hat{s}(\alpha^i) = e(\alpha^i)$$

(*Syndrome*) $\rightarrow$ Tabelle aller möglichen Syndrome mit Fehlerstellen.

Angenommen, es ist ein Fehler aufgetreten:

$$\hat{s} = s + e$$

Zur Fehlererkennung setzen wir α^i mit $i = 1, \ldots, k$ ein:

$$\hat{s}(\alpha^i) = s(\alpha^i) + e(\alpha^i)$$

und da $g \mid s \Rightarrow s(\alpha^i) = 0$:

$$S_i := \hat{s}(\alpha^i) = e(\alpha^i)$$

(*Syndrome*) $\rightarrow$ Tabelle aller möglichen Syndrome mit Fehlerstellen.
Nur möglich für kleine Körper.

Idee: Löse die *Key-equations*:

- $\mathrm{ggT}(\sigma, \omega) = 1$
- $\deg(\omega) < |E| = \deg(\sigma) \leq \frac{k}{2}$
- $\sigma S \cong \omega \mod T^k$

wobei

$$S = \prod_{i=1}^{k} S_i T^i$$

$$e = \sum_{i=1}^{k} e_i T^i, E := \{k \mid e_k \neq 0\}$$

Idee: Löse die *Key-equations*:

- $\mathrm{ggT}(\sigma, \omega) = 1$
- $\deg(\omega) < |E| = \deg(\sigma) \leq \frac{k}{2}$
- $\sigma S \cong \omega \mod T^k$

wobei

$$S = \prod_{i=1}^{k} S_i T^i$$

$$e = \sum_{i=1}^{k} e_i T^i, E := \{k \mid e_k \neq 0\}$$

Man kann zeigen: Lösen σ, ω die Key-equations, gilt:

$$\sigma = \sum_{i \in E} (1 - \alpha_i T)$$

$$\omega = \sum_{i \in E} e_i \prod_{j \in E, j \neq i} (1 - \alpha^j T)$$

Man kann zeigen: Lösen σ, ω die Key-equations, gilt:

$$\sigma = \sum_{i \in E} (1 - \alpha_i T)$$

$$\omega = \sum_{i \in E} e_i \prod_{j \in E, j \neq i} (1 - \alpha^j T)$$

$$\Rightarrow \sigma(\alpha^{-k}) = 0 \Leftrightarrow k \in E \Rightarrow \omega(\alpha^{-k}) = e_k$$

Möglichkeiten, Key-equations zu lösen:

1. LGS lösen (nicht sehr effizient)
2. Euklidischer Algorithmus (nicht parallelisierbar)
3. Berlekamp-Massey-Algorithmus (komplex)