Zusammenfassung Information Theory and Coding

Markus Velm

Inhaltsverzeichnis

1. Einleitung

1.1. Informationstheorie

Bit: binary unit → Einheit für Information

bit: binary digit → bit als binäres Symbol

Informationgehalt

je unwahrscheinlicher ein Symbol x auftritt, desto mehr Information enhält es:

$$I(x) = ld\left(\frac{1}{P(x)}\right) - ld(P(x))$$

P: Wahrscheinlichkeit eines Symbols
I: Informationsgehalt $[I] = Bit$

Entropie

gemittelter Informationsgehalt einer Quelle X:

$$H(X) = \sum_i P(x_i) \cdot I(x_i) = -\sum_i P(x_i) \cdot ld(P(x_i))$$

H: Entropie $[H] = Bit/Symbol$

Entscheidungsgehalt

Entropie wird maximal, wenn alle Symbole gleichwahrscheinlich sind → Entscheidungsgehalt

$$H_0 = ld(N)$$

H_0: Entscheidungsgehalt $[H_0] = Bit/Symbol$
N: Anzahl der Symbole eines Alphabets

Redundanz

$$R = H_0 - H$$

$$r = \frac{R}{H_0}$$

R: Redundanz $[R] = Bit/Symbol$
r: relative Redundanz

1.2. Quellcodierung

1.2.1. Huffman-Code

ist **Präfixcode:** ein Codewort ist niemals Anfang eines anderen Codewortes

Codebaum aufbauen:

1. Ordne die Symbole nach Auftrittswahrscheinlichkeit
2. Fasse Symbole mit niedrigster Wahrscheinlichkeit zu einem Symbol zusammen und addiere die Wahrscheinlichkeiten
3. Wiederhole bis nur ein Symbol übrig bleibt

Beschrifte die Pfade mit 1 und 0
→ Codewort ergibt sich, indem man von Wurzel bis zum Blatt geht

1.2.2. Arithmetische Codierung

Codierung eines Wortes (oder Textes) durch Zahl

Endezeichen notwendig, da keine natürliche Terminierung des Codes

1.3. Kanalmodell

1.4. Kanalkapazität

1.5. Shannon-Theoreme

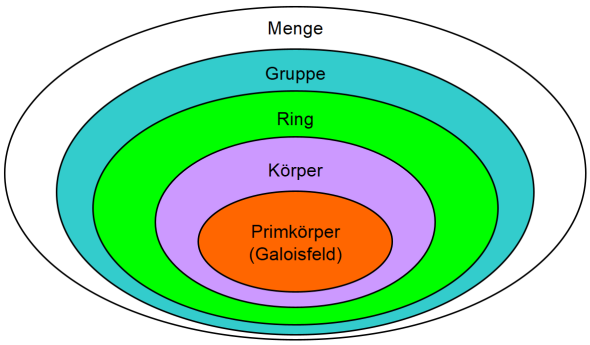
2. Blockcodes

Code beschrieben durch $C(n, k, d)$

n: Länge Codewort
k: Länge Informationswort
d: Mindestabstand

3. Galois-Felder

3.1. Algebraische Strukturen



Menge

Verbund von Elementen, welche keine Operationen beinhalten (Möbel können eine Menge sein, es kann aber nicht Tisch + Stuhl gerechnet werden)

Halbgruppe

Menge A mit Verknüpfung »+« ist eine Halbgruppe, wenn

- Abgeschlossenheit ($+$ zweier Elemente von A ergibt wieder ein Element von A)
- Assoziativität (Reihenfolge der Operation mit $+$ spielt keine Rolle, $a + (b + c) = (a + b) + c$)
- Existenz eines neutralen Elements (Element a + neutrales Element n ergibt wieder Element a)

Gruppe

Halbgruppe plus

- Existenz eines additiven inversen Elements ($a+b = n$)

Abelsche oder kommutative Gruppe

Gruppe plus

- Kommutativität (Reihenfolge der Operanden spielt keine Rolle, $a + b = b + a$)

Ring

abelsche Gruppe plus

- Abgeschlossenheit bezüglich »·«
- Assoziativität bezüglich »·«
- Distributivität ($a \cdot (b + c) = a \cdot b + a \cdot c$)

Körper

Ring plus

- Kommutativität bezüglich »·«($a \cdot b = b \cdot a$)
- Neutrales Element bezüglich »·«
- Inverses Element bezüglich »·«für jedes Element

Primkörper/Galois-Feld

Körper, indem Addition und Multiplikation $\mod p$ gerechnet wird (p muss dabei eine Primzahl sein)
$\hookrightarrow GF(p)$

3.2. Eigenschaften Galois-Felder

Primitives Element

Element α, welches durch ihre $p-1$ Potenzen alle Elemente (außer 0) des $GF(p)$ erzeugt

Bsp. $GF(5), \alpha = 2$:

$2^0 = 1 \mod 5 = 1$
$2^1 = 2 \mod 5 = 2$
$2^2 = 4 \mod 5 = 4$
$2^3 = 8 \mod 5 = 3$

ab hier zykische Wiederholung:
$2^4 = 16 \mod 5 = 1$

4. Reed-Solomon-Code

4.1. Wunsch und Idee

Wunsch

Konstruktion eines Codes mit vorgegebener Korrekturfähigkeit
→ Vorgabe des Mindestabstandes d

$$e = \left\lfloor \frac{d-1}{2} \right\rfloor$$
$$d = 2e - 1$$

bei linearem Code ist Mindestabstand = Mindestgewicht

→ Codeworte haben mind. d von 0 verschiedene Koeffizienten

d'Alembert: Polynom vom Grad n hat n komplexe (oder höchstens n reelle) Nullstellen; auch im Galois-Feld

Idee

Konstruktion des Informationswortes als Polynom $A(x)$ mit Grad $k-1$ (damit höchstens $k-1$ Nullstellen)

Im $GF(p)$ mit Ordnung $n = p-1$ kann man $A(x)$ an n Stellen auswerten, danach wiederholen sich die Werte

→ Auswertung des Polynoms für verschiedene x (bzw. α^i) ergeben die Koeffizienten a_i des Polynoms $a(x)$

$a_i = A(\alpha^i)$ IDFT

von diesen sind höchstens $k-1$ Null (weil $grad(A(x)) = k-1$)
von diesen sind also mind. $n-(k-1)$ von Null verschieden
→ Mindestgewicht d

$d = n - (k-1) = n - k + 1$

4.2. Codierung

Verschiedene Möglichkeiten aus einem Informationswort ein Codewort zu generieren

4.2.1. IDFT (nicht systematisch)

$a_i = A(\alpha^i)$
$A(x)$: Informationswort
a_i: Koeff. des Codewortes

4.2.2. Generatorpolynom (nicht systematisch)

$a_i = g(x) \cdot i(x)$

mit Generatorpolynom

$g(x) = \prod_{i=k}^{n-1}(x - \alpha^{-i})$

$g(x)$: Generatorpolynom
$i(x)$: Informationspolynom

4.2.3. Polynomdivision (systematisch)

Informationswort ist Teil des Codewortes (an den hohen Potenzen)

$a^*(x) = i_{k-1}x^{n-1} + i_{k-2}x^{n-2} + ... + i_1x^{n-k+1} + i_0x^{n-k}$

jedes Codewort muss durch Generatorpolynom teilbar sein
→ ist für $a^*(x)$ i.A. nicht der Fall

$$\frac{a^*(x)}{g(x)} = b(x) + \frac{rest(a^*(x))}{g(x)}$$
$$\rightarrow \frac{a^*(x) - rest(a^*(x))}{g(x)} = b(x)$$
$$a(x) = a^*(x) - rest(a^*(x))$$

$rest(a^*(x))$: Divisionsrest

4.2.4. Über Prüfpolynom (systematisch)

Prüfpolynom:

$$h(x) = \prod_{i=0}^{k-1}(x - \alpha^{-i})$$

Produkt aus Generator- und Prüfpolynom ist 0

$g(x) \cdot h(x) = 0$

4.3. Decodierung

Idee:

Addition des Fehlerpolynoms $f(x)$ mit t Koeffizienten (d.h. t Fehler sind auf dem Kanal aufgetreten) zum gesendeten Codewort $a(x)$

im Zeitbereich:

$r(x) = a(x) + f(x)$

im Frequenzbereich:

$R(x) = A(x) + F(x)$

gedanklich wird ein Polynom $c(x)$ aufgestellt, welches t Nullen an den Fehlerstellen hat

Da die Koeffizienten von $c(x)$ die Auswertung ihrer Fouriertransformierten $C(x)$ ist, ist der Grad von $C(x)$ t

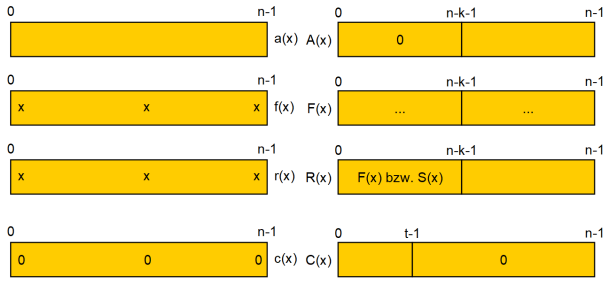
Da $c(x)$ gerade dort 0 ist, wo $f(x)$ ungleich 0, ist das Produkt $f_i \cdot c_i$ immer 0 (Achtung, keine Polynommultiplikation gemeint, sondern punktweise Multiplikation)

$f_i \cdot c_i = 0$

wenn Zeitbereich = 0 → Frequenzbereich = 0

$F(x) \cdot C(x) = 0$

Achtung: hier Polynommultiplikation/ Faltung/ Filterung gemeint
↪ Aufstellen der Schlüsselgleichungen



4.3.1. Schlüsselgleichungen

beschreiben, dass Faltung von $C(x)$ und $F(x)$ Null sind (Achtung: zyklische Faltung, siehe Abschnitt 3)

F_0 bis F_{n-k-1} (bzw. F_{d-2}) sind bekannt, da diese direkt an den Syndromstellen von $R(x)$ stehen

Alle C-Koeff. sind unbekannt, außer C_{t-1}, dieser wird zu 1 gesetzt

$C_{t-1} = 1$

da Anzahl der Fehler (t) unbekannt sind, muss ausprobiert werden, welche minimale Anzahl an Fehlern die Schlüsselgleichungen erfüllt

Berlekamp-Massey-Algorithmus

effizientes Verfahren zur Lösung der Schlüsselgleichungen

Euklidscher Algorithmus

Suche des ggT zweier Zahlen

Kann zur Lösung der Schlüsselgleichungen verwendet werden

4.4. Horner-Schema

5. Erweiterungskörper

Erweitern des Grundkörpers (z.B. 2) mit Exponent (z.B. 4) $\rightarrow GF(2^4)$

primitives Element wird zu primitivem Polynom, z.B. $p(x) = x^4 + x + 1$

6. BCH-Codes

A. Hilfreiches

A.1. Inverse in Galois-Feldern

Additive Inverse

gegeben: -3 in $GF(5)$

gesucht: additive Inverse

bedeutet: $3 + x \mod 5 = n = 0$

$x = 2$, da $3 + 2 = 5$ und $5 \mod 5 = 0$

daher: $-3 = 2$

n: neutrales Element der Addition ($= 0$)

oder: mit Tabelle

gegebene Zahl als Index behandeln, passenden Wert raussuchen

Index	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
Wert	0	1	2	3	4	0	1	2	3	4	0	1

Multiplikative/modulare Inverse

gegeben: 2^{-1} in $GF(7)$

gesucht: multiplikative Inverse

bedeutet: $2^1 \cdot x \mod 7 = n = 1$

$x = 4$, da $2^1 \cdot 4 = 8$ und $8 \mod 7 = 1$

daher: $2^{-1} = 4$

oder: mit Logarithmentafel

gegebene Potenz als Index behandeln, passenden Wert raussuchen

Index	-3	-2	-1	0	1	2	3	4	5	6
Wert	1	2	4	1	2	4	1	2	4	1

A.2. ABC/PG-Formel

ABC/ PQ-Formel

ABC: $ax^2 + bx + c = 0$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

PQ: $x^2 + px + q$

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

B. Polynome

B.1. Polynommultiplikation

B.2. Polynomdivision

C. Lineare Algebra

Matrix-Multiplikation

$$A \cdot B = \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}_{3,2} \begin{pmatrix} g & h \\ i & j \end{pmatrix}_{2,2} = \begin{pmatrix} ag + bi & ah + bj \\ cg + di & ch + dj \\ eg + fi & eh + fj \end{pmatrix}_{3,2}$$

$$\vec{v} \cdot \vec{w}^T = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \cdot (d \quad e \quad f) = \begin{pmatrix} a \cdot d & a \cdot e & a \cdot f \\ b \cdot d & b \cdot e & b \cdot f \\ c \cdot d & c \cdot e & c \cdot f \end{pmatrix}$$

Skalarprodukt:

$$\vec{v}^T \cdot \vec{w} = (a \quad b \quad c) \cdot \begin{pmatrix} d \\ e \\ f \end{pmatrix} = a \cdot d + b \cdot e + c \cdot f$$

bei komplexen Vektoren: $\vec{v}^H \cdot \vec{w}$

Transponieren

Zeilen werden Spalten, Spalten werden Zeilen

$$A^T = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix}^T = \begin{pmatrix} a & d \\ b & e \\ c & f \end{pmatrix}$$

Invertieren

für 2x2-Matrizen:

$$A^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

Diagonale Matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Spalten der Matrix sind Eigenvektoren

1; -5; 3 sind die Eigenwerte der Eigenvektoren

Hermitesche Matrix

nur für quadratische Matrizen

$$A = A^H = (A^*)^T = \begin{pmatrix} 1 & 5-j & 3j \\ 5+j & 2 & 3-2j \\ -3j & 3+2j & 3+4j \end{pmatrix}$$

Eigenvektoren von hermiteschen Matrizen sind orthogonal

Unitäre Matrix

$A \cdot A^H = k \cdot I$

k: Skalierungsfaktor (bei skaliert unitären Matrizen)

Toeplitz-Struktur

Eine Matrix hat Toeplitz-Struktur, wenn alle Diagonalen parallel zur Hauptdiagonalen, die gleichen Elemente enthalten:

$$T = \begin{pmatrix} 0 & -2 & -5 & -3 \\ 1 & 0 & -2 & -5 \\ 2 & 1 & 0 & -2 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

Hermitesche Toeplitz-Matrizen sind positiv oder negativ definit, abhängig vom Vorzeichen der Elemente auf der Hauptdiagonalen

Vandermonde-Matrix

Spalten: Indezes gleich
Zeilen: Potenzen gleich

$$S = \begin{pmatrix} 1 & 1 & ... & 1 \\ x_0^1 & x_1^1 & ... & x_{N-1}^1 \\ x_0^2 & x_1^2 & ... & x_{N-1}^2 \\ ... & ... & ... & ... \\ x_0^{N-1} & x_1^{N-1} & ... & x_{N-1}^{N-1} \end{pmatrix}$$

Determinante

nur für quadratische Matrizen

für 2×2-Matrix:

$$det(A) = det\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = a \cdot d - b \cdot c$$

für 3×3-Matrix:

$$det(C) = det\left[\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}\right]$$

$$= a \cdot det\left[\begin{pmatrix} e & f \\ h & i \end{pmatrix}\right] - b \cdot det\left[\begin{pmatrix} d & f \\ g & i \end{pmatrix}\right] + c \cdot det\left[\begin{pmatrix} d & e \\ g & h \end{pmatrix}\right]$$

Rang einer Matrix

Eine Matrix hat vollen Rang, wenn die Determinante ungleich 0 ist

Ist die Determinante gleich 0, ist die Matrix/das Gleichungssystem überbestimmt

Eigenvektoren/ Eigenwerte

Eigenvektoren einer Matrix werden bei einer Matrixtransformation nur in ihrer Länge geändert, nicht in ihrer Richtung

Faktor, um den ein Eigenvektor gedehnt oder gestaucht wird, ist der zum Eigenvektor zugehöriger Eigenwert λ

$A\vec{v} = \lambda\vec{v}$

$(A - \lambda I)\vec{v} = \vec{0}$

A: Matrix
$\vec{v}$: Eigenvektor
λ: Eigenwert(e)
I: Einheitsmatrix

Eigenwerte von positiv (oder negativ) definiten Matrix sind immer positiv (oder negativ)

D. Digitale Signalverarbeitung

Diskretisierung und Fensterung

Diskretisierung ○—● Periodische Fortsetzung
Diskretisierung ●—○ Periodische Fortsetzung
Begrenzung → Leck-Effekt

Fourier-Transformation (kontinuierlich)

$$X(f) = \int_{-\infty}^{\infty} x(t) \cdot e^{-j2\pi ft}\, dt$$

DFT

$$X(n) = \sum_{k=0}^{N-1} x(k) \cdot e^{-j2\pi \frac{nk}{N}}$$

n: Frequenzindex
k: Zeitindex

Auflösung DFT

$$\Delta f = \frac{f_a}{N} = \frac{1}{t_a \cdot N} = \frac{1}{\Delta t}$$

Δf: spektrale Auflösung
f_a: Abtastfrequenz
t_a: Abtastrate
N: Anzahl Abtastwerte
Δt: Messdauer

Fensterung

Fensterung im Zeitbereich → Multiplikation mit Fensterfunktion ○—● Faltung mit zur Fensterfunktion zugehörigem Spektrum

Dirichlet-Kern

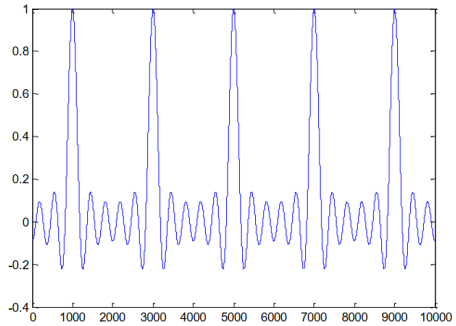
abgetastete Rechteckfunktion ○—● Dirichlet-Kern

Definition der Dirichlet-Kerns der Länge $N + 1$:

$$D(x) = \sum_{n=-\frac{N}{2}}^{\frac{N}{2}} e^{jnx} = \frac{\sin\left(\left(\frac{N+1}{2}\right)x\right)}{\sin\left(\frac{x}{2}\right)}$$

$x = 2\pi f T_a$

Bsp: 11:



Eigenschaften:

Hauptwert hat Höhe $N+1$

Nullstellen, bei $f = \frac{f_a}{N+1} \cdot k$ für $k \in \mathbf{N}$

Hauptwert periodisch mit f_a

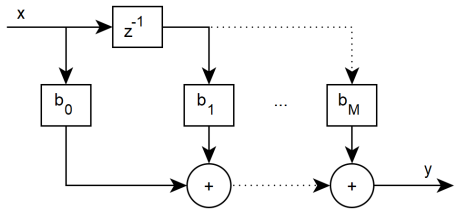
z-Transformation

$z = e^{j2\pi \frac{f}{f_a}}$

$$H(f) = H(z)\Big|_{z=e^{j2\pi \frac{f}{f_a}}}$$

Reiner FIR-Filter

kanonische Form

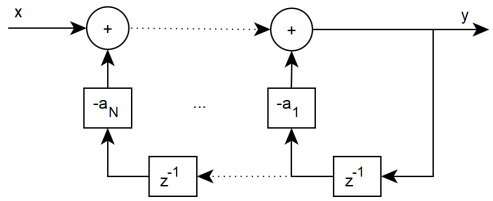


$$H(z) = \frac{Y(z)}{X(z)} = b_0 + b_1 \cdot z^{-1} + ... + b_M \cdot z^{-M}$$

$$y(t) = b_0 \cdot x(t) + b_1 \cdot x(t-1) + ... + b_M \cdot x(t-M)$$

Reiner IIR-Filter

kanonische Form



$$H(z) = \frac{1}{1 + a_1 \cdot z^{-1} + ... + a_N \cdot z^{-N}}$$

$$y(t) = x(t) - a_1 \cdot y(t-1) - ... - a_n \cdot y(t-N)$$