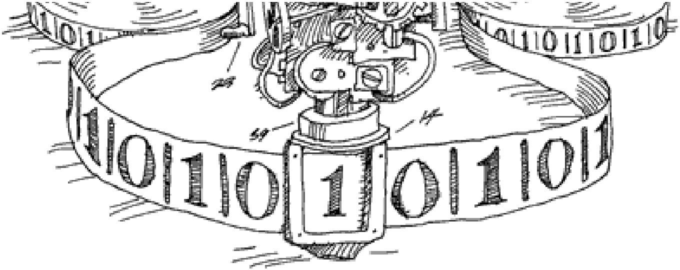
Karlsruher Institut für Technologie

Theoretische Grundlagen der Informatik

Tutorium 11

Institut für Kryptographie und Sicherheit



Unäre vs. binäre Kodierung

Karlsruher Institut für Technologie

Warum ist das unäre Partitionproblem in *P* und das binäre in *NP*?

- Beispielinstanz: 32, 128, 64, 256, 32
  - Unäre Eingabelänge: $32 + 128 + 64 + 256 + 32 = 512$
  - Binäre Eingabelänge: $5 + 7 + 6 + 8 + 5 = 31$
- Ein Algorithmus der beispielsweise deterministisch $2 \cdot$ *Summe der Zahlen* Schritte benötigt ist für unäre Kodierung polynomiell, für binäre Kodierung allerdings exponentiell

TSP in NP

TSP Enscheidungsproblem

Gegeben: Ein Graph $G = (V, V \times V)$, eine Gewichtungsfunktion $d : V \times V \rightarrow \mathbb{N}$ und ein Parameter k
Gesucht: Besitzt G einen einfacher Kreis $C = (v_1, v_2, ..., v_n, v_1)$, sodass $n = |V|$ und $\sum_{(u,v) \in C} d(u, v) \leq k$.

TSP Optimierungsproblem

Gegeben: Ein Graph $G = (V, V \times V)$ und eine Gewichtungsfunktion $d : V \times V \rightarrow \mathbb{N}$
Gesucht: Minimales k, sodass G einen einfacher Kreis $C = (v_1, v_2, ..., v_n, v_1)$ besitzt, mit $n = |V|$ und $\sum_{(u,v) \in C} d(u, v) \leq k$.

Fuuuuusion

Gegeben: Ein Graph $G = (V, V \times V)$ und eine Gewichtungsfunktion $d : V \times V \rightarrow \mathbb{N}$
Gesucht: Besitzt G einen einfacher Kreis $C = (v_1, v_2, ..., v_n, v_1)$, sodass $n = |V|$ und $\sum_{(u,v) \in C} d(u, v)$ minimal.

TSP in NP

TSP Enscheidungsproblem

Gegeben: Ein Graph $G = (V, V \times V)$, eine Gewichtungsfunktion $d : V \times V \to \mathbb{N}$ und ein Parameter k
Gesucht: Besitzt G einen einfacher Kreis $C = (v_1, v_2, ..., v_n, v_1)$, sodass $n = |V|$ und $\sum_{(u,v) \in C} d(u, v) \leq k$.

- Orakel rät eine Lösung als Folge von Kanten
- Wir überpüfen ob Kantenzahl $\leq |V|$
- Wir überprüfen ob Kantenfolge einen einfachen Kreis bildet
- Wir überprüfen ob Summe der Kantengewichte $\leq k$

Überprüfung offensichtlich in polynomieller Zeit. Bilden daraus eine Funktion $TSP_E : (V, d, k) \rightarrowtail bool$ abbildet. Die Funktion ist nichtdeterministisch und benötigt polynomielle Laufzeit.

TSP in NP

Karlsruher Institut für Technologie

TSP Optimierungsproblem

Gegeben: Ein Graph $G = (V, V \times V)$ und eine Gewichtungsfunktion $d : V \times V \rightarrow \mathbb{N}$

Gesucht: Minimales k, sodass G einen einfacher Kreis $C = (v_1, v_2, ..., v_n, v_1)$ besitzt, mit $n = |V|$ und $\sum_{(u,v) \in C} d(u, v) \leq k$.

Zu zeigen: $TSP_O \in NP \Leftrightarrow \exists$ nichtdet. TM, die TSP_O in Polyzeit löst.

- Berechne $s = \sum_{u,v \in V} d(u, v)$
- Verwende binäre Suche für $k \in 1, .., s$ um minimales k zu finden, sodass $TSP_E((V, V \times V), d, k) == True$
- Gebe gefundenes k aus.

Laufzeit: $|V|^2 + \log_2(s) \cdot P_n$

- Falls d unär in Eingabe kodiert: $\leq |V|^2 + \log_2(n) \cdot P_n \leq n^2 + P(n) \cdot n$
- Falls d binär in Eingabe kodiert: $\leq |V|^2 + \log_2(2^n) \cdot P_n \leq n^2 + P(n) \cdot n$

TSP in NP

Fuuuuusion

Gegeben: Ein Graph $G = (V, V \times V)$ und eine Gewichtungsfunktion $d : V \times V \to \mathbb{N}$
Gesucht: Besitzt G einen einfacher Kreis $C = (v_1, v_2, ..., v_n, v_1)$, sodass $n = |V|$ und $\sum_{(u,v)\in C} d(u, v)$ minimal.

- Gebe „Ja“ aus.

Kolmogorow

Beispiel: Das Wort, das aus 1000 Nullen besteht (Alphabet: ASCII)

Kolmogorow

Karlsruher Institut für Technologie

0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000

Kolmogorow

Eine Beschreibung eines Wortes w ist ein Programm bei dessen Ausführung das Wort erzeugt wird. Die Länge dieses Programmes ist dann ein d(w).

```
Program Nullfolge (n)
 begin
  for i:= 1 to n
   print “0”
 end
```

Kolmogorow

Eine minimale Beschreibung eines Wortes w heißt Kolmogorow-Komplexität $K(w)$

- Also: $\forall d(w) : |d(w)| \geq |K(w)|$
- Die Länge von $K(w)$ ist abhängig von der Struktur von w

Falls $|K(w)| \geq |w|$ heißt das Wort unkomprimierbar.

Die Kolmogorow-Komplexität ist nicht entscheidbar aber semi-entscheidbar.

Kolmogorow

Eine minimale Beschreibung eines Wortes w heißt Kolmogorow-Komplexität $K(w)$

- Also: $\forall d(w) : |d(w)| \geq |K(w)|$
- Die Länge von $K(w)$ ist abhängig von der Struktur von w

Falls $|K(w)| \geq |w|$ heißt das Wort unkomprimierbar.

Die Kolmogorow-Komplexität ist nicht berechenbar aber rekursiv aufzählbar.

Kolmogorow Komplexität: Aufgabe (B7 A1)

1. Beweisen Sie, dass $K(x)$ nicht berechenbar ist!
2. Beweisen Sie, dass die Menge der nichtkomprimierbaren Strings $\mathcal{L}$ nicht rekursiv aufzählbar ist!
3. Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität von 0^n an!
4. Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität der Binärdarstellung der n-ten Primzahl p an!
5. Sei x ein Palindrom. Geben sie eine möglichst gute obere Schranke für $K(x)$ an!
6. Sei π_n die Kreiszahl π bis zur n-ten Nachkommastelle entwickelt. Geben Sie eine möglichst gute obere Schranke für π_n an.

Multiple Choice

Die Kolmogorov-Komplexität einer Zeichenkette $x \in \{0, 1\}^n$ ist immer größer als $log_2(n)$

Multiple Choice

Das Hamilton-Kreis Problem ist NP-vollständig

Multiple Choice

In der Klasse NP liegen nicht-entscheidbare Probleme

Multiple Choice

Das Vertex-Cover Problem ist NP-vollständig

Multiple Choice

Semi-entscheidbare Sprachen sind unter Komplementbildung abgeschlossen

Multiple Choice

Nichtdeterministische endliche Automaten sind echt mächtiger als deterministische

Multiple Choice

Zu jeder CH-2-Sprache gibt es eine CH-1-Grammatik

Multiple Choice

Um zu zeigen, dass ein Problem Π NP-vollständig ist, genügt es, ein NP-schweres Problem auf Π zu reduzieren.

Shannonscher Informationsbegriff

- Jede Information bzw. Nachricht besitzt eine Quelle
  - Oft randomisiert a.k.a. Zufallsquellen
  - Wenn alle gesendete Nachrichten unabhängig voneinander sind, ist die Quelle gedächtnislos
- Es gibt immer einen Empfänger, der die Nachrichten beobachtet
- Je unvorhersehbarer die Nachricht, desto mehr Informationsgehalt
  - Wird deshalb auch manchmal Überraschungswert genannt
- Entropie ist ein Begriff für die Dichte der Informationen

Etwas genauer

- Informationsgehalt soll nicht negativ sein
- Ein sicheres Ergebnis (p = 1) enthält keine Information
- Informationen von unabhängigen Nachrichten sollen sich addieren
- Kleine Änderungen der Wahrscheinlichkeit $\Rightarrow$ kleine Änderung des Informationsgehalts
- $I(x) = -log_b(p(x)) = log_b(\frac{1}{p(x)})$ erfüllt diese Bedingungen
  - Meist wird als Basis b = 2 verwendet

- Entropie ist entsprechend definiert
  $H(X) = \sum_{x \in X} (p(x) \cdot log_2(\frac{1}{p(x)})) = \sum_{x \in X} (p(x) \cdot I(x))$

Beispiele

- Zufallsquelle 1: p(A) = $\frac{1}{2}$, p(B) = $\frac{1}{2}$
- I(A) = $log_2(\frac{1}{0.5}) = log_2(2) = 1$ = I(B)
- H(X) = $(p(A) \cdot I(A)) + (p(B) \cdot I(B)) = 0.5 + 0.5 = 1$

- Zufallsquelle 2: p(A) = $\frac{1}{16}$, p(B) = $\frac{15}{16}$
- I(A) = $log_2(\frac{1}{0.0625}) = log_2(16) = 4$
- I(B) = $log_2(\frac{1}{0.9375}) = log_2(\frac{16}{15}) = 0.0931\ldots$
- H(X) = $(p(A) \cdot I(A)) + (p(B) \cdot I(B))$
  $= (\frac{1}{16} \cdot 4) + (\frac{15}{16} \cdot 0.0931) = \frac{1}{4} + 0.873 = 0.337$

Aufgabe B11 A1

1. Wie groß sind der Informationsgehalt und die Entropie, wenn eine Quelle mit dem Alphabet $\{0, 1\}$ nur aus dem Zeichen 0 bestehende Folgen sendet?
2. An einer Quelle mit n Zeichen tritt jedes Zeichen gleichverteilt auf. Wie groß sind der Informationsgehalt und die Entropie eines einzelnen Zeichens?
3. Berechnen Sie die Entropie des Wurfes eines idealen Würfels mit 8 Seiten, dessen Wahrscheinlichkeit für jede Seite $p = \frac{1}{8}$ ist!
4. Was ist der Unterschied zwischen den beiden Folgen, die aus verschiedenen gedächtnislosen Quellen mit der gleichen Wahrscheinlichkeit für 0 und 1 gesendet werden, wenn man sie unter dem Aspekt Entropie und Ordnung betrachtet?
   4.1 ...10101010101010101010...
   4.2 ...01101100110111000010...

Übertragung von Information

Daten können über einen Kanal von der Quelle zu einem Empfänger gesendet werden. Dieser Kanal ist in der Regel nicht störungsfrei, dass heißt die gesendeten Daten können ungleich zu den empfangenen sein. Ein gestörter Kanal kann durch seine Übertragungswahrscheinlichkeiten $P(r|q)$, welche angeben wie wahrscheinlich es ist, dass r beim Empfänger ankommt, wenn q aus der Quelle gesendet wurde, charakterisiert werden.
Damit ergibt sich der Zusammenhang

$$P(R = r) = \sum_{q \in Q} P(Q = q) P(R = r | Q = q)$$

und für die Wahrscheinlichkeit das r und q gleichzeitig auftreten:

$$P(Q = q, R = r) = P(Q = q) P(R = r | Q = q).$$

Einige Definitionen

Totalinformation oder auch Verbundentropie H(Quelle Q, Empfänger R) ist die gesamte von Quelle und Empfänger erzeugte Entropie

$$H(Q,R) = -\sum_{q\in Q}\sum_{r\in R} P(Q=q, R=r)\log(P(Q=q,R=r))$$

Äquivokation H(Quelle $Q|$ Empfänger R) gibt dem Entropieverlust durch die Übertragung an.

$$H(Q|R) = H(Q,R) - H(R)$$

Fehlinformation H(Empfänger $R|$ Quelle Q) entspricht dem anscheinenden Entropiegewinn durch die Übertragung.

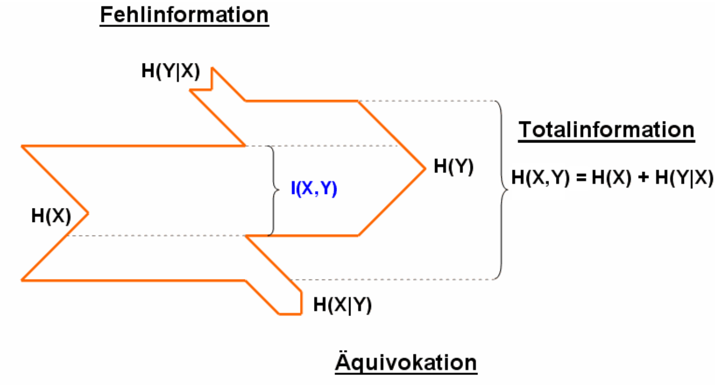
$$H(R|Q) = H(Q,R) - H(Q)$$

Transinformation I(Quelle Q, Empfänger R) ist die richtig empfangene Informationsmenge.

$$I(Q,R) = H(Q) - H(Q|R) = H(R) - H(R|Q) = H(Q) + H(R) - H(Q,R)$$

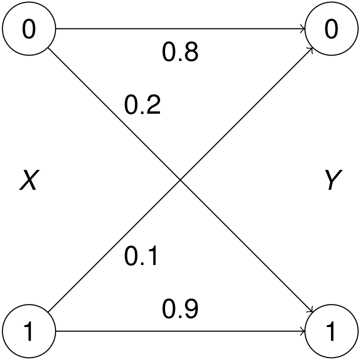
Bild zur Veranschaulichung

Karlsruher Institut für Technologie

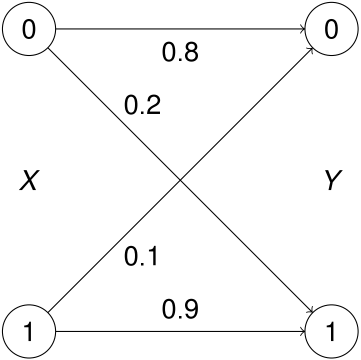


Aufgabe B11 A2

Studieren Sie den Fall eines asymmetrischen binären Kanals mit Quelle X und Empfänger Y. Die Übertragungswahrscheinlichkeiten $P(Y|X)$ seien durch das folgende Diagramm gegeben:

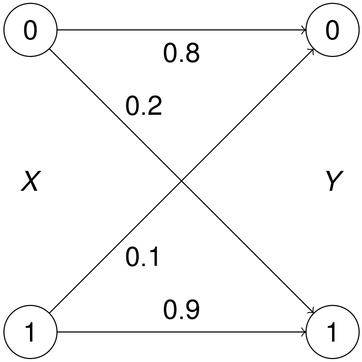


Aufgabe B11 A2



1. Wie groß ist die Wahrscheinlichkeit dafür, dass die Bitkette “1100” als “1001” übertragen wird?
2. Wenn die Entropie der Quelle $H(X) = 1$ bit ist, wie groß ist dann $H(Y)$?
3. Wie groß muss $H(X)$ sein, damit $H(Y) = 1$ bit gilt?

Aufgabe B11 A2



1. Wie groß ist die Verbundentropie $H(X, Y)$ des Übertragungssystems? Gehen Sie ab dieser Teilaufgabe von der Situation der 2. Teilaufgabe aus!
2. Wie groß ist die sog. Irrelevanz $H(Y|X)$? Und wie groß ist die sog. Äquivokation $H(X|Y)$?
3. Wie groß ist schließlich die Transinformation $I(X; Y)$?

Aufgabe B11 A4

Gegeben sei eine gedächtnislose Quelle Q, die mit Wahrscheinlichkeit $p_0 = \frac{1}{4}$ eine 0 und mit Wahrscheinlichkeit $p_1 = \frac{3}{4}$ eine 1 sendet. Gegeben sei zudem ein Empfänger R, der die Zeichen von Q zu empfangen versucht. Dieser Empfänger empfängt eine 0 immer richtig. Sendet die Quelle Q jedoch eine 1, so empfängt R mit Wahrscheinlichkeit $\frac{1}{2}$ eine 1 und mit Wahrscheinlichkeit $\frac{1}{2}$ eine 0.

1. Berechnen Sie die Information $I(0)$ und $I(1)$ bezüglich der Quelle Q!
2. Berechnen Sie die Entropie der Quelle Q!
3. Die Quelle Q sendet die Zeichenfolge 0110. Wie hoch ist der Informationsgehalt dieser Zeichenfolge?
4. Berechnen Sie die Totalinformation $H(Q, R)$, die Fehlinformation $H(R|Q)$, die Äquivokation $H(Q|R)$ und die Transinformation $I(Q; R)$!

Huffman-Codierung

Die Huffman-Codierung ist ein Algorithmus zur verlustfreien Datenkompression.

Problemdefinition

- Gegeben
  - Ein Alphabet $A = \{a_0, a_1, ..., a_n\}$ der Größe n
  - Gewichte $W = \{w_0, w_1, ..., w_n\}$ für alle $a \in A$.
    Meist die Wahrscheinlichkeit, dass ein Zeichen auftritt.
- Gesucht
  - Eine binäre Codierung für alle Zeichen aus A, sodass die erwartete Code-Wortlänge in Bezug auf die Gewichte minimal ist.

Huffman-Codierung

Die Huffman-Codierung ist ein Algorithmus zur verlustfreien Datenkompression.

Problemdefinition

- Gegeben
  - Ein Alphabet $A = \{a_0, a_1, ..., a_n\}$ der Größe n
  - Gewichte $W = \{w_0, w_1, ..., w_n\}$ für alle $a \in A$.
    Meist die Wahrscheinlichkeit, dass ein Zeichen auftritt.
- Gesucht
  - Eine binäre Codierung für alle Zeichen aus A, sodass die erwartete Code-Wortlänge in Bezug auf die Gewichte minimal ist.

Lässt sich sowohl auf konkrete Wörter anwenden als auch auf Quellen, von denen man weiß, wie wahrscheinlich sie welches Zeichen sendet.

Huffman-Codierung Beispiel

Gegeben sei das Wort abacabadabacaba. Wie lautet eine Huffman-Codierung?

Huffman-Codierung Beispiel

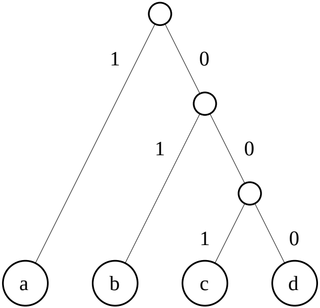
Gegeben sei das Wort **abacabadabacaba**. Wie lautet eine Huffman-Codierung?

- #a = 8
- #b = 4
- #c = 2
- #d = 1

Huffman-Codierung Beispiel

Gegeben sei das Wort abacabadabacaba. Wie lautet eine Huffman-Codierung?

- #a = 8
- #b = 4
- #c = 2
- #d = 1



Aufgabe B11 A3

Karlsruher Institut für Technologie

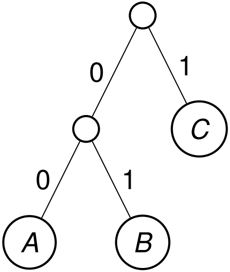
Gegeben sei eine Quelle mit Alphabet $\{A, B, C, D\}$ und mit den folgenden Wahrscheinlichkeiten:
$P(A) = \frac{1}{2}, P(B) = \frac{1}{4}, P(C) = \frac{1}{8}, P(D) = \frac{1}{8}$

- Berechnen Sie die Entropie der Quelle!
- Erstellen Sie eine entsprechende Huffman-Codierung!
- Was ist die mittlere Codewortlänge? Gibt es einen Zusammenhang zur Entropie?

Aufgabe B11 A3

Gegeben sei eine Quelle mit Alphabet $\{A, B, C, D\}$ und mit den folgenden Wahrscheinlichkeiten:
$P(A) = \frac{1}{2}, P(B) = \frac{1}{4}, P(C) = \frac{1}{8}, P(D) = \frac{1}{8}$

- Gegeben sei der folgende Huffman-Baum:



Dekodieren Sie 01101110110010101 1! Ist der Huffman-Code geeignet?

Bis zum nächsten Mal!

Kolmogorov Directions

WHEN PEOPLE ASK FOR STEP-BY-STEP DIRECTIONS, I WORRY THAT THERE WILL BE TOO MANY STEPS TO REMEMBER, SO I TRY TO PUT THEM IN MINIMAL FORM.

Lizenzen