CODIERUNGSTHEORIE

KURS ZELL AN DER PRAM, FEBRUAR 2005

1. Das Problem

1.1. **Kanalcodierung und Fehlerkorrektur.** Wir wollen eine Nachricht über einen digitalen Kanal, der nur 0 oder 1 übertragen kann, schicken. Wegen Rauschen wird ein Bit mit Wahrscheinlichkeit $p = 0,1$ verfälscht (dh. nur mit Wahrscheinlichkeit $0,9$ korrekt übertragen).

Unsere Nachricht ist ein digitales Bild, bestehend aus Pixeln in einer von 2^5 Farben.

Ziel: Jedes Pixel (5 Bit) soll mit Wahrscheinlichkeit von mindestens $0,95$ korrekt ankommen.

Date: 15. Februar 2005.

Erhard Aichinger und Peter Mayr, Institut für Algebra, Johannes Kepler Universität Linz, erhard@algebra.uni-linz.ac.at, peter.mayr@algebra.uni-linz.ac.at, http://www.algebra.uni-linz.ac.at/.

Bsp. Bild bei unkodierter Übertragung:

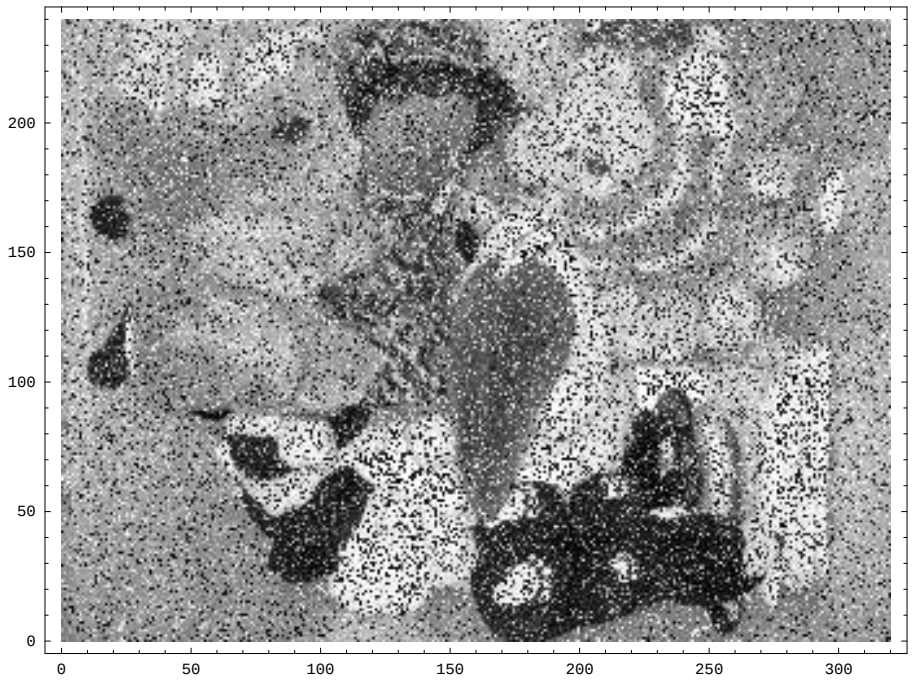
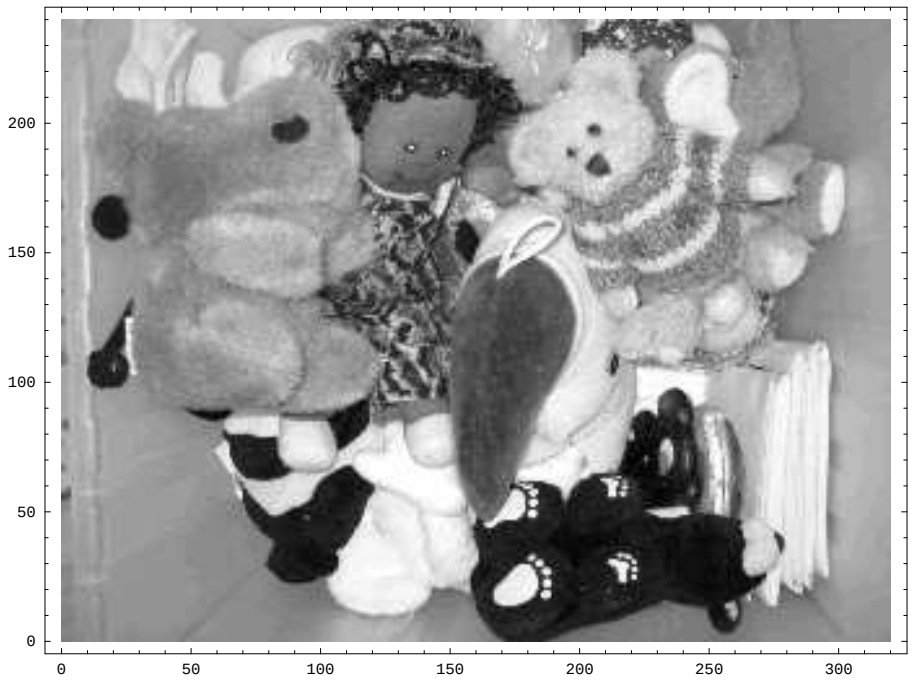


Bild im Original:



2. Einige Begriffe

Beispiel 2.1. 1. Idee: Wiederholung.

Nearest-Neighbor Dekodierung

Übungsaufgaben 2.2.

(1) Die Bitfehler-W. eines binären Kanals sei p. Wir kodieren 0 als 000 und 1 als 111 (3-fach Wiederholungscode).
   (a) Wie hoch ist die W., dass wir ein empfangenes Wort mit Nearest-Neighbor Dekodierung falsch dekodieren?
   (b) Wie hoch ist die W., dass wir 5 Wörter in Folge mit Nearest-Neighbor Dekodierung korrekt dekodieren?
   (c) Wie oft müssten wir jedes Bit wiederholen, damit 5 Wörter in Folge mit Nearest-Neighbor Dekodierung korrekt dekodiert werden können?

Beispiel 2.3. Kodieren Wörter der Länge 3:

(1) 1fach fehlererkennend: Parity check
(2) 1fach fehlerkorregierend: 3fach Wiederholung und linearer $(6, 3, 3)$-Code leisten das selbe.

Definition 2.4. binärer Code über $\mathbb{Z}_2 = \{0, 1\}$ der Länge n, Wort ist Vektor.
Hamming-Distanz zwischen Wörtern $d(u, v) := |\{i \in \{1, \dots, n\} \mid u_i \neq v_i\}|$,
Minimaldistanz $d(C) := \min\{d(u, v) \mid u, v \in C\}$.
Informationsrate $\frac{\log_2(|C|)}{n}$.

Ad Bsp. 2.3: Der 3fach Wiederholungscode hat Länge 9, Minimaldistanz 3 (1 Fehler kann korrigiert werden), Inforate 1/3. Der $(6, 3, 3)$-Code hat Minimaldistanz 3 und Inforate 1/2.

Wir wollen ein empfangenes Wort v zu dem "am wahrscheinlichsten" ausgesandten Codewort c dekodieren.

Maximum-Likelihood Dekodierung: Sei C ein binärer Code der Länge n. Für $c \in C$ und $v \in {\mathbb{Z}_2}^n$, sei $W(v|c)$ die bedingte Wahrscheinlichkeit, dass v empfangen wird, wenn c gesendet wurde.

Wir dekodieren ein empfangenes Wort $v \in {\mathbb{Z}_2}^n$ zu einem Codewort $c \in C$, so dass

$$W(v|c) = \max\{W(v|d) \mid d \in C\}.$$

Dabei ist c nicht notwendigerweise eindeutig.

Ein Kanal, der 0,1 überträgt, heißt *binär symmetrisch* wenn mit W. $p < 1/2$ das Symbol 0 zu 1, und 1 zu 0 verfälscht wird (Bitfehler-W. p).

Übungsaufgaben 2.5.

(1) Für einen binären symmetrischen Kanal mit Bitfehler-W. $p < 1/2$ ergibt die Maximum-Likelihood Dekodierung die Nearest-Neighbor Dekodierung.

(2) Hamming-Distanz erfüllt die Dreiecksungleichung.
(3) Wieviele Fehler kann man für einen Code C mit Minimaldistanz d immer erkennen? Wieviele mit Nearest-Neighbor Dekodierung korrigieren?
(4) Gibt es einen Code mit 8 Codewörtern der Länge 5, der Einfachfehler korrigieren kann?

Definition 2.6. Sei $B_t(x) := \{y \in {\mathbb{Z}_2}^n \mid d(x,y) \leq t\}$.

Ein Code C heißt t-fehlererkennend, wenn $C \cap B_t(c) = \{c\}$ für alle $c \in C$.

Ein Code C heißt e-fehlerkorrigierend, wenn $B_e(c) \cap B_e(c') = \emptyset$ für alle $c, c' \in C$.

Diskrete Kugelpackungen:

Theorem 2.7. ***Hamming Schranke:*** *Sei C ein binärer Code der Länge n mit $d(C) \geq 2e+1$. Dann gilt*

$$|C| \cdot \sum_{i=0}^{e} \left(\begin{array}{c} n \\ i \end{array} \right) \leq 2^n.$$

Definition 2.8. Kanalkapazität eines binären symmetrischen Kanals mit Bitfehler-W. p:

$$k(p) := 1 + p \log_2(p) + (1-p) \log_2(1-p)$$

Theorem 2.9. ***Shannon's Hauptsatz der Kanalkodierung:***
Sei k die Kanalkapazität eines binären symmetrischen Kanals. Sei $\epsilon > 0$ und $0 < r < k$. Für hinreichend großes n gibt es dann einen binären Code der Länge n, dessen Informationsrate mindestens r ist, und für den die Wahrscheinlichkeit einer falschen Dekodierung eines Wortes kleiner als ϵ ist.

3. Lineare Codes

Vgl. Bsp 2.3.

Definition 3.1. Ein binärer linearer Code C ist die Lösungsmenge eines linearen Gleichungssystems. Eine Matrix H über $\mathbb{Z}_2$ so, dass $C = \{x \in {\mathbb{Z}_2}^n \mid Hx = 0\}$, heißt Kontrollmatrix von C.

Ein binärer linearer Code C der Länge n mit 2^k Codeworten und Minimaldistanz d wird als (n, k, d)-Code bezeichnet.

Lemma 3.2. *Für einen linearen Code C gilt $d(C) = \min\{d(c, 0) \mid c \in C\}$.*

Gewicht von v ist $d(v, 0)$.

Beispiel 3.3. Hamming-Code (7,4,3).

Syndrom-Dekodierung Zum empfangenen Wort $v \in {\mathbb{Z}_2}^n$ suchen wir $c \in C$, so dass der Fehler $e = v - c$ minimales Gewicht hat. Es gilt

$$Hv = H(c + e) = Hc + He = He.$$

Dh. v und e haben das gleiche Fehlersyndrom.

Übungsaufgaben 3.4.

(1) Was sagt die Hamming-Schranke über den Hamming-Code (7,4,3)?
(2) Gibt es einen linearen $(7, 4, 4)$-Code?
(3) Finden Sie einen möglichst kurzen binären linearen $(n, 5, 3)$-Code.
    Wie hoch ist die W., damit ein über den bin. symm. Kanal (p = 0.9) übertragenes Wort korrekt dekodieren zu können?