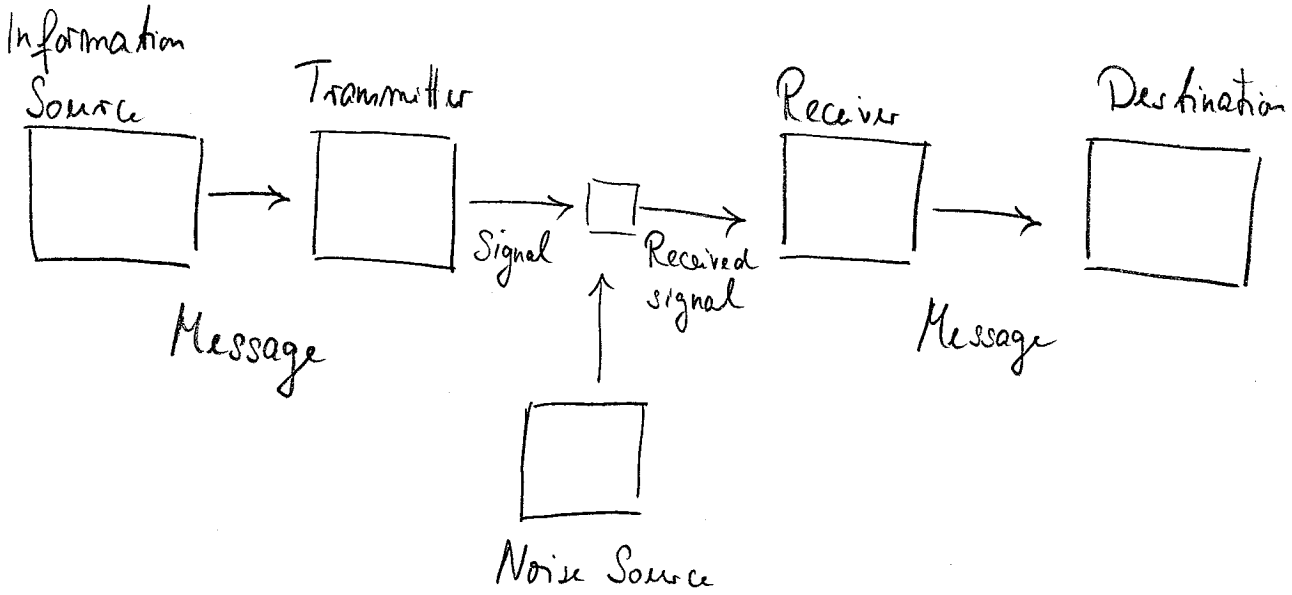
Figure 1 in der Originalarbeit von Shannon:

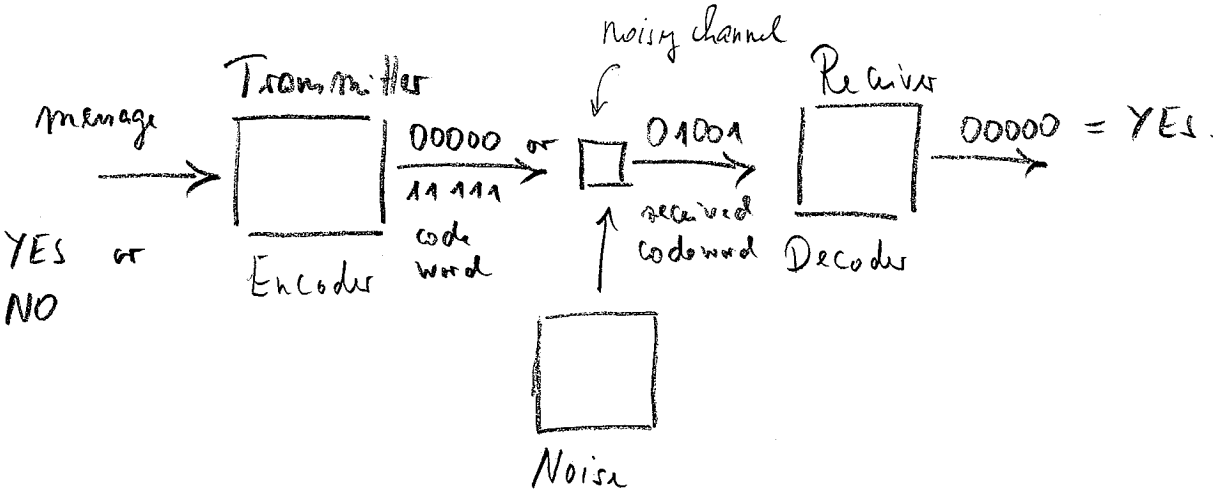


Beispiele:

a) Systeme, die Information übertragen (räumliche Kommunikation)
Radio, Fernsehen, Telefon, Glasfasernetze, ...

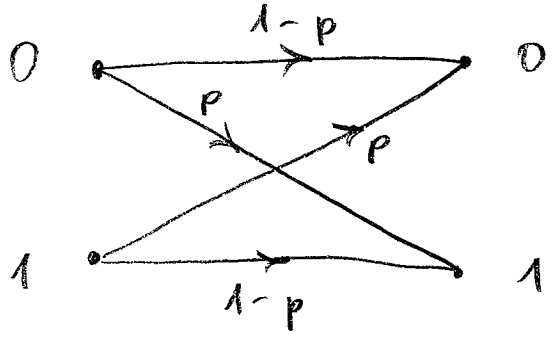
b) Systeme, die Information speichern (zeitliche Kommunikation)
magnetische (Cassette, Diskette), optische (CD, DVD, BD),
digitale (Flash) Speichermedien.

Verwendung von (fehlerkorrigierenden) Code.



Einfaches Modell für den Kommunikationskanal:

"binary symmetric channel"



Jeder Buchstabe des Alphabets (0/1) wird mit Wahrscheinlichkeit p ($p < 1/2$) falsch übertragen. Der Kanal hat kein Gedächtnis.

Sei $C \subseteq \{0,1\}^n$ ein (n, M, d)-Code mit Codewörtern $x_1, \dots, x_M$. Angenommen alle Codewörter werden mit gleich großer Wahrscheinlichkeit verwendet.

Optimale Decodierungsstrategie ("maximum likelihood decoding"): Falls y empfangen wurde, finde $x_j \in C$ so dass

$$\text{Prob}\left[y \text{ wurde empfangen} \mid x_j \text{ wurde gesendet} \right] \to \max.$$

$$\| \quad p^r (1-p)^{n-r}, \quad \text{falls } d(y, x_j) = r$$

Da $p < 1/2$, wird die W.keit maximiert, falls r minimiert wird. D.h. finde $x_j \in C$ mit $d(y, x_j) = \min \{ d(y, x) : x \in C \}$.

Theorem Sei $C \subseteq Q^n$ ein (n, M, d) - Code. Dann kann C $\lfloor \frac{d-1}{2} \rfloor$ - viele Fehler korrigieren.

Zentrales Problem in der Codierungstheorie: Gegeben n und d, finde einen (n, M, d) - Code mit möglichst großem M.

Gute Codes: n klein (Geschwindigkeit von Codierung / Decodierung)

M groß (Effizienz, wenig Redundanz)

d groß (gute Fehlerkorrektur).

§ 2 Lineare Codes

Idee: Algebra hilft gute Codes zu konstruieren und zu analysieren.

Sei Q ein endlicher Körper, d.h. $Q = \mathbb{F}_q$ für eine Primzahlpotenz $q = p^r$.

Wichtige Beispiele: $\cdot \mathbb{F}_2 = \{0, 1\}$, mit $1 + 1 = 0$

$\rightsquigarrow$ binäre Codes.

- $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1+\alpha\}$

allgemeine Konstruktion von $\mathbb{F}_q$, $q = p^r$:

Betrachte $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Sei $P \in \mathbb{F}_p[x]$ ein irreduzibles Polynom über $\mathbb{F}_p$ vom Grad r (gibt es immer). Dann ist

$$\mathbb{F}_q = \mathbb{F}_p[x]/(P).$$

z.B. $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$

<u>Def.</u>: Ein k-dimensionaler Untervektorraum $C \subseteq \mathbb{F}_q^n$ heißt linearer Code, oder auch $[n,k]$-Code.

Ein $[n,k,d]$-Code ist ein linearer $[n,k]$-Code mit Minimaldistanz $\geq d$. Es ist ein (n, q^k, d)-Code.

<u>Lemma</u> Sei C ein linearer Code. Dann ist $w(C) = d(C)$.

<u>Bew.</u>: <u>$w \geq d$</u>: klar, weil $0 \in C$, da C linear.

<u>$w \leq d$</u>: Seien $x, y \in C$ mit $d(C) = d(x,y) = \|x-y\|$.

Dann ist $w(x-y) = d(C)$ und $x-y \in C$, weil C linear. ☒