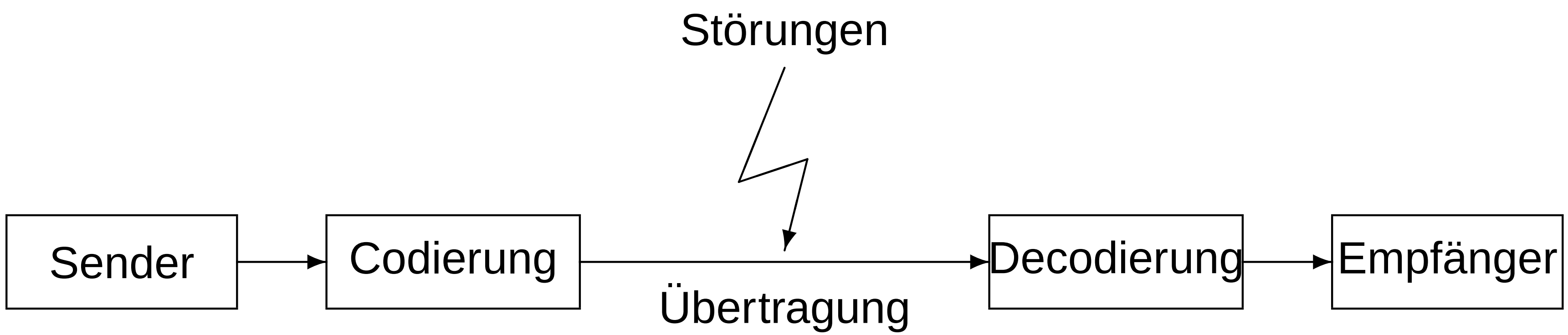

Störungen
Sender
Codierung
Decodierung
Empfänger
Übertragung

Def: Der **(Hamming-)Abstand** $d(x, y)$ von zwei Vektoren $x, y \in B^n$ ist die Anzahl der Stellen, an denen sich x und y unterscheiden.

Das **(Hamming-)Gewicht** $w(x)$ eines Vektors $x \in B^n$ ist definiert als die Anzahl der von 0 verschiedenen Stellen von x.

$w(x) = d(x, 00 \ldots 0)$ und $d(x, y) = w(x \oplus y)$

Def: Ein **Code** ist eine nicht-leere, endliche Teilmenge von $B^+ = B \cup B^2 \cup B^3 \cup \ldots$

Falls die Elemente eines Codes C (die **Codewörter** alle dieselbe Länge haben, also $C \subseteq B^n$ für ein $n \in N$, so spricht man von einem **Blockcode** (der Länge n).

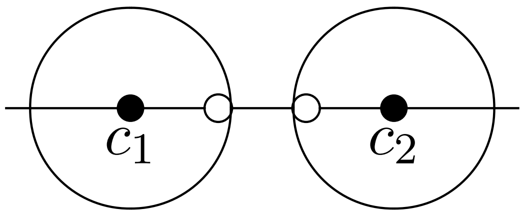
Der **Minimalabstand** eines Codes C ist definiert als

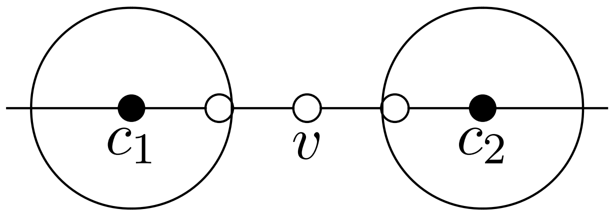
$$d = \min\{d(x, y) \mid x, y \in C, \, x \neq y\}$$

Die Menge der Wörter mit Hamming-Distanz $\leq t$ von einem Codewort c heißt **Kugel** um c vom Radius t.

Def: Ein Code heißt t**-Fehler-korrigierend**, falls für alle $c \in C$ und alle c' mit $d(c, c') \leq t$ gilt, daß es kein anderes Codewort (als c) mit Abstand $\leq t$ zu c' gibt.

Satz: Jeder Code mit Minimalabstand d ist $\lfloor (d-1)/2 \rfloor$-Fehler-korrigierend.





Def: Ein Blockcode $C \subseteq B^n$ heißt **systematisch** in den Stellen $i_1, \ldots, i_k$, wenn es zu jedem Vektor $u = (u_1, \ldots, u_k) \in B^k$ *genau ein* Codewort $c = (c_1, \ldots, c_n)$ gibt mit $u_1 = c_{i_1}, \ldots, u_k = c_{i_k}$. Man nennt u dann die **Nachricht**, die als Codewort c codiert wird.

Unter einem $[n, k]$ Code versteht man einen in k Stellen systematischen Code der Länge n. Ein $[n, k, d]$ Code ist ein $[n, k]$ Code mit Minimalabstand d.

Def: Ein Code heißt **linearer Code**, falls mit je zwei Codewörtern x, y immer auch $x \oplus y$ (bitweises Xor) Codewort ist.

Minimalabstand

$$d \;=\; \min\{w(x) \mid x \in C,\, x \neq 00\ldots0\}$$

Satz: (Hammingschranke) Für die Anzahl der Codewörter in einem t-Fehler-korrigierenden Code C der Länge n gilt:

$$|C| \;\leq\; 2^n / \left(\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{t} \right)$$

Wenn bei einem Code hier sogar die Gleichheit gilt, so sprechen wir von einem t-**perfekten** Code.