

- ▶ $\mathbb{B}^n = \{0, 1\}^n$: Bitvektoren der Länge n
- ▶ $\|\mathbf{a}\|$: HAMMING-Gewicht von \mathbf{a}
- ▶ \mathbb{B}_k^n : Vektoren $u \in \mathbb{B}^n$ mit HAMMING-Gewicht = k .
- ▶ $\mathbb{B}_{\leq k}^n$: Vektoren $u \in \mathbb{B}^n$ mit HAMMING-Gewicht $\leq k$.
- ▶ $S_k(\mathbf{a}) = \mathbf{a} \oplus \mathbb{B}_{\leq k}^n$: HAMMING-Kugel mit Radius k um \mathbf{a} .
- ▶ $\text{bin}_{n,p}$: Binomialverteilung zum Parameter p ($0 < p < 1$) auf \mathbb{B}^n , d.h.

$$\begin{aligned} \text{bin}_{n,p}(\mathbf{a}) &= \text{bin}_{n,p}(a_1, a_2, \dots, a_n) \\ &= \prod_{1 \leq i \leq n} p^{a_i} (1-p)^{1-a_i} = p^{|\mathbf{a}|} (1-p)^{n-|\mathbf{a}|} \end{aligned}$$

Fakten:

- ▶ $\#\mathbb{B}^n = 2^n$,
- ▶ $\#\mathbb{B}_k^n = \binom{n}{k}$,
- ▶ $\#\mathbb{B}_{\leq k}^n = \sum_{0 \leq j \leq k} \binom{n}{j}$.
- ▶ $\binom{n}{k} \sim_{n \rightarrow \infty} \frac{n^k}{k!}$
- ▶ $\sum_{0 \leq j \leq \lambda \cdot n} \binom{n}{j} \sim_{n \rightarrow \infty} 2^{n \cdot H(\lambda)}$

▶ Parameter der Binomialverteilung

▶ Mittelwert

$$\mu_{n,p} = \sum_{\mathbf{a} \in \mathbb{B}^n} \|\mathbf{a}\| \cdot \text{bin}_{n,p}(\mathbf{a}) = \sum_{k=0}^n k \cdot \binom{n}{k} \cdot p^k (1-p)^{n-k} = n \cdot p$$

▶ Varianz

$$\begin{aligned} \sigma_{n,p}^2 &= \sum_{\mathbf{a} \in \mathbb{B}^n} (\|\mathbf{a}\| - \mu_{n,p})^2 \cdot \text{bin}_{n,p}(\mathbf{a}) \\ &= \sum_{k=0}^n (k - \mu_{n,p})^2 \cdot \binom{n}{k} \cdot p^k (1-p)^{n-k} = n \cdot p \cdot (1-p) \end{aligned}$$

▶ CHEBYCHEV-Abschätzung für die Binomialverteilung

$$\text{bin}_{n,p} \{ \mathbf{a} \in \mathbb{B}^n; \|\mathbf{a}\| - \mu_{n,p} \geq c \cdot \sigma_{n,p} \} \leq \frac{1}{c^2}$$

Beweis: mit

$$X = \{ \mathbf{a} \in \mathbb{B}^n; \|\mathbf{a}\| - \mu_{n,p} \geq c \cdot \sigma_{n,p} \}$$

$$Y = \mathbb{B}^n \setminus X = \{ \mathbf{a} \in \mathbb{B}^n; \|\mathbf{a}\| - \mu_{n,p} < c \cdot \sigma_{n,p} \}$$

gilt

$$\begin{aligned} \sigma_{n,p}^2 &= \left(\sum_{\mathbf{a} \in X} + \sum_{\mathbf{a} \in Y} \right) (\|\mathbf{a}\| - \mu_{n,p})^2 \cdot \text{bin}_{n,p}(\mathbf{a}) \\ &\geq c^2 \cdot \sigma_{n,p}^2 \cdot \text{bin}_{n,p}(X) \end{aligned}$$

- ▶ Kanalmodell: BSC_p binärer symmetrischer Kanal (ohne Gedächtnis) mit Fehlerwahrscheinlichkeit p :

$$\mathbb{B}_n \ni \mathbf{a} \rightsquigarrow \mathbf{b} = \mathbf{a} \oplus \mathbf{f} \quad \text{mit Wahrscheinlichkeit } \text{bin}_{n,p}(\mathbf{f})$$

- ▶ (n, K) -Code : Teilmenge $\mathcal{C} \subset \mathbb{B}^n$ mit $\#\mathcal{C} = K$.
- ▶ Coderate von \mathcal{C} :

$$R(\mathcal{C}) = \frac{1}{n} \cdot \log_2 \#\mathcal{C}, \quad \text{also } K = 2^{n \cdot R(\mathcal{C})}$$

- ▶ Decodierung mit Radius r ($0 \leq r < n$): wird $\mathbf{a} \in \mathcal{C}$ gesendet und $\mathbf{b} \in \mathbb{B}^n$ empfangen,

$$\mathbf{a} \rightsquigarrow \mathbf{b} = \mathbf{a} \oplus \mathbf{f}$$

so wird decodiert zu:

- ▶ $\mathbf{a}' \in \mathcal{C}$, falls \mathbf{a}' das einzige Element von $\mathcal{C} \cap S_r(\mathbf{b})$ ist;
- ▶ Fehlanzeige (oder beliebiges Element von \mathcal{C}), falls $\#\mathcal{C} \cap S_r(\mathbf{b}) \neq 1$.
- ▶ Fehlertypen:
 - ▶ Fehler 1. Art: $\|\mathbf{f}\| > r$.
 - ▶ Fehler 2. Art: $\|\mathbf{f}\| \leq r$, aber $\#\mathcal{C} \cap S_r(\mathbf{b}) \geq 2$.

- ▶ Fehler 1. Art

Sei $\epsilon > 0$ und $r = \lfloor n \cdot p + \sqrt{\frac{2}{\epsilon}} \cdot \sigma_{n,p} \rfloor$. Dann gilt

$$\begin{aligned} P^{(1)} &= \text{bin}_{n,p} \{ \mathbf{f} \in \mathbb{B}^n; \|\mathbf{f}\| > r \} \\ &\leq \text{bin}_{n,p} \left\{ \mathbf{f} \in \mathbb{B}^n; \left| \|\mathbf{f}\| - n \cdot p \right| > \sqrt{\frac{2}{\epsilon}} \cdot \sigma_{n,p} \right\} \leq \frac{\epsilon}{2} \end{aligned}$$

wegen der CHEBYCHEV-Abschätzung.

- ▶ Fehler 2. Art

Für einen (n, K) -Code \mathcal{C} mit r -Decodierung und Vektoren $\mathbf{a}, \mathbf{b} \in \mathbb{B}^n$ wird definiert:

$$\chi_{\mathcal{C},r}(\mathbf{a}, \mathbf{b}) = \begin{cases} 1 & \text{falls es ein } \mathbf{a}' \neq \mathbf{a} \text{ gibt mit } \mathbf{a}, \mathbf{a}' \in \mathcal{C} \cap S_r(\mathbf{b}) \\ 0 & \text{sonst.} \end{cases}$$

- ▶ Dann gilt bei Summation über alle (n, K) -Codes \mathcal{C} für $\mathbf{a} \in \mathcal{C} \cap S_r(\mathbf{b})$ und mit $t = \#\mathbb{B}_{\leq r}^n$:

$$\begin{aligned} N &= \sum_{\mathcal{C}} \chi_{\mathcal{C},r}(\mathbf{a}, \mathbf{b}) = \binom{2^n - 1}{K - 1} - \binom{2^n - t}{K - 1} \\ &= \binom{2^n - 1}{K} \frac{K}{2^n - K} - \binom{2^n - t}{K} \frac{K}{2^n - K - t + 1}, \end{aligned}$$

unabhängig von \mathbf{a} und \mathbf{b} .

Dabei ist

$$\frac{\binom{2^n-1}{K}}{\binom{2^n}{K}} = \frac{(2^n-1) \cdots (2^n-K)}{(2^n) \cdots (2^n-K+1)} = 1 - \frac{K}{2^n}$$

und

$$1 > \frac{\binom{2^n-t}{K}}{\binom{2^n}{K}} > 1 - t \cdot \frac{K}{2^n}$$

Die letzte Ungleichung folgt aus der Tatsache, dass für $0 \leq k \leq n$ gilt:

$$\frac{\binom{n-x}{k}}{\binom{n}{k}} > 1 - x \cdot \frac{k}{n} \text{ für } 0 < x < 1.$$

Beide Polynome nehmen für $x = 0$ und $x = 1$ gleiche Werte an und das Polynom auf der linken Seite hat $n, n-1, \dots, n-k+1$ als einfache Nullstellen, also negative erste und positive zweite Ableitung im Intervall $0 \leq x \leq 1$.

▶ Mit der Abschätzung für N ergibt sich

$$\bar{P}^{(2)} \leq 1 - \left(1 - t \cdot \frac{K}{2^n}\right) \cdot \frac{2^n}{2^n - K - t + 1} < t \cdot \frac{K}{2^n}.$$

▶ Wählt man nun wie bei der Abschätzung des Fehlers 1. Art $r = \lfloor n \cdot \rho + \sqrt{\frac{2}{\epsilon}} \cdot \sigma_{n,\rho} \rfloor$, so hat man mit $\rho = \frac{r}{n} \sim \rho$ und

$$K = 2^{n \cdot R}, t \leq 2^{n \cdot H(\rho)}$$

also

$$\bar{P}^{(2)} \leq 2^{n \cdot (R+H(\rho)-1)} = 2^{n \cdot (R-C(\rho))}$$

wobei

$$C(\rho) = 1 - H(\rho) = 1 + \rho \cdot \log \rho + (1 - \rho) \cdot \log(1 - \rho)$$

die *Kapazität* des binären symmetrischen Kanals mit Fehlerwahrscheinlichkeit ρ ist.

▶ Annahme:

- ▶ ein Code \mathcal{C} wird aus der Menge $\mathcal{C}_{n,K}$ aller (n, K) -Codes mit Gleichverteilung genommen,
- ▶ \mathbf{a} wird aus \mathcal{C} mit Gleichverteilung gezogen und übertragen,
- ▶ $\mathbf{a} \rightsquigarrow \mathbf{b}$ mit Wahrscheinlichkeit $\text{bin}_{n,p}(\mathbf{a} \oplus \mathbf{b})$.

▶ Abschätzung für die mittlere Wahrscheinlichkeit für das Auftreten von Fehlern der zweiten Art:

$$\begin{aligned} \bar{P}^{(2)} &= \frac{1}{\binom{2^n}{K} \cdot K} \sum_{\substack{\mathcal{C} \in \mathcal{C}_{n,K} \\ \mathbf{a}, \mathbf{b} \in \mathbb{B}^n}} \chi_{\mathcal{C},r}(\mathbf{a}, \mathbf{b}) \cdot \text{bin}_{n,p}(\mathbf{a} \oplus \mathbf{b}) \\ &= \frac{N}{\binom{2^n}{K} \cdot K} \sum_{\mathbf{a} \in \mathbb{B}^n} \sum_{\mathbf{b} \in \mathbb{B}_{\leq r}^n} \text{bin}_{n,p}(\mathbf{b}) \\ &= \frac{N \cdot 2^n}{\binom{2^n}{K} \cdot K} \cdot \text{bin}_{n,p}(\mathbb{B}_{\leq r}^n) \leq \frac{N \cdot 2^n}{\binom{2^n}{K} \cdot K}. \end{aligned}$$

- ▶ Für $R < C(\rho)$ gilt $2^{n(R-C(\rho))} \rightarrow_{n \rightarrow \infty} 0$
- ▶ Bei Vorgabe eines $\epsilon > 0$ kann man also $\bar{P}^{(2)} < \epsilon/2$ erreichen, indem man n genügend gross macht.
- ▶ Das bedeutet: betrachtet man Codes \mathcal{C} mit Rate $R(\mathcal{C}) < C(\rho)$ so ist für hinreichend grosses n im Mittel – d.h. bei gleichverteilter zufälliger Auswahl der Codes und der gesendeten Codevektoren – die W.keit $\bar{P}^{(2)}$ für das Auftreten von Fehlern 2. Art $< \epsilon/2$.

- ▶ Insgesamt wird für den BSC_p für Coderaten $\lesssim C(p)$ für hinreichend grosse Länge n die Fehlerwahrscheinlichkeit im Mittel $< \varepsilon$ werden.
- ▶ Es muss also auch (lange) Codes mit Rate $\lesssim C(p)$ geben, bei denen die Fehlerwahrscheinlichkeit $< \varepsilon$ ist!
- ▶ Dies ist eine nicht-konstruktive Existenzaussage!
- ▶ SHANNONS Theorem in Prosa:
Fehlerkorrigierende Informationsübertragung über gestörte Kanäle ist für Coderaten, die (beliebig wenig) unterhalb der Kanalkapazität liegen, mit beliebig kleinen Fehlerwahrscheinlichkeiten prinzipiell möglich.

- ▶ *With many profound scientific discoveries it is possible with the aid of hindsight to see that the times were ripe for the breakthrough. Not so with information theory!*
While of course Shannon was not working in a vacuum in the 1940's, his results were so breathtakingly original that even the communication specialists of the day were at loss to understand their significance.
R. J. MCELIECE in *The Theory of Information and Coding*, Encyclopedia of Mathematics and Its Applications, vol. 3, Addison-Wesley, 1977.