Aufgabe 25: Entropie und Volumen von Hammingkugeln

Bitvektoren und Entropiebegriff stehen in einem engen Zusammenhang, der in der Informationstheorie detailliert untersucht und ausgenutzt wird. Zwei wichtige quantitative Aussagen werden hier behandelt. $\mathbb{B}^n_{\leq k}$ bezeichnet hierbei die Menge der Bitvektoren der Länge n mit einem HAMMING-Gewicht $\leq k$.

1. Für $0 \leq k \leq n/2$ und mit der Bezeichnung $x = k/n$ lässt sich das Volumen der Hamming-Kugel $\mathbb{B}^n_{\leq k}$ mittels der Entropiefunktion folgendermassen nach oben abschätzen:
$$\sharp\mathbb{B}^n_{\leq k} \leq 2^{n \cdot H(x, 1-x)},$$

2. Für $0 \leq k \leq n$ und mit der Bezeichnung $x = k/n$ lässt sich das Volumen der Hamming-Kugel $\mathbb{B}^n_{\leq k}$ mittels der Entropiefunktion folgendermassen nach unten abschätzen:
$$\sharp\mathbb{B}^n_{\leq k} \geq \frac{1}{n+1} \cdot 2^{n \cdot H(x, 1-x)}.$$

Für die erste Ungleichung sollten Sie erst einmal den Ausdruck $x^k \cdot (1-x)^{n-k}$ (mit $x = k/n$, wohlgemerkt!) mit Hilfe der Entropiefunktion ausdrücken und im übrigen auf die Identität $1 = (x + (1-x))^n$ die Binomialformel anwenden.

Für die zweite Ungleichung sollten Sie feststellen, dass die Ausdrücke

$$a_j = \binom{n}{j} x^j \cdot (1-x)^{n-j} \quad (0 \leq j \leq n)$$

für $j = k$ das Maximum annehmen. Dann folgt die Ungleichung schnell, wenn Sie noch Information aus dem erste Teil berücksichtigen.