Satz (Satz von Brockway McMillan, 1956)**.** *Jeder eindeutig entzifferbare binäre Kode mit n Kodewörtern mit Längen $\ell_1, \ldots, \ell_n$ erfüllt die Kraftsche Ungleichung*

$$\sum_{i=1}^{n} 2^{-\ell_i} \leq 1. \tag{1}$$

Beweis. Wir bezeichnen mit A_k die Anzahl der Nachrichten der Länge k, die sich aus den Kodewörtern zusammensetzen lassen. Durch vollständige Induktion ergibt sich die Rekursion

$$A_k = \sum_{i=1}^{n} A_{k-\ell_i} \tag{2}$$

für $k \geq 1$ mit den Anfangsbedingungen

$$A_0 = 1, \quad A_k = 0 \text{ für } k < 0.$$

Bei der Begründung von (2) wird verwendet, dass der Kode eindeutig entzifferbar ist und sich deshalb bei den Wörtern, die auf der rechten Seite von (2) zusammengezählt werden, keine Dopplungen ergeben.

Wir bezeichnen die Länge des längsten Kodeworts mit $\ell_{\max}$.

Wir führen einen Widerspruchsbeweis. Nehmen wir an, dass die Ungleichung (1) verletzt ist. Dann gilt die entgegengesetzte Ungleichung

$$\sum_{i=1}^{n} y^{-\ell_i} > 1 \tag{3}$$

für $y = 2$, und wir können auf Grund der Stetigkeit auch einen Wert $y > 2$ finden, für den (3) gilt. Wir fixieren einen solchen Wert y. (Die entsprechende *Gleichung* $\sum_{i=1}^{n} x^{-\ell_i} = 1$ beziehungsweise $1 - \sum_{i=1}^{n} x^{-\ell_i} = 0$ wird übrigens durch Multiplikation mit $x^{\ell_{\max}}$ zur *charakteristischen Gleichung* der *linearen Rekursion* (2).)

Vereinfachende Annahme. Es gibt ein k_0, sodass $A_k \geq 1$ für alle $k \geq k_0$ ist. Dies ist genau dann der Fall, wenn der größte gemeinsame Teiler der Längen $\ell_1, \ldots, \ell_n$ gleich 1 ist. Wenn zum Beispiel alle Längen ℓ_i gerade sind, dann ist klarerweise $A_k = 0$ für alle ungeraden k. Für solche Fälle müsste man den Beweis anpassen.

Wir behaupten: Es gibt ein $C > 0$, sodass für alle $k \geq k_0$ gilt:

$$A_k \geq C \cdot y^k \tag{4}$$

Wir beweisen das durch vollständige Induktion nach k. Der Induktionsschritt ist ganz einfach und funktioniert unabhängig vom Wert von C:

$$A_k \overset{(2)}{=} \sum_{i=1}^{n} A_{k-\ell_i} \overset{\text{I.V.}}{\geq} \sum_{i=1}^{n} C \cdot y^{k-\ell_i} = C \cdot y^k \sum_{i=1}^{n} y^{-\ell_i} \overset{(3)}{>} C \cdot y^k$$

Die Induktionsvorraussetzung (I.V.) können wir nur anwenden, wenn $k \geq k_0 + \ell_{\max}$ ist. Daher müssen wir die Fälle $k = k_0, k_0+1, \ldots, k_0+\ell_{\max}-1$ als Induktionsbasis behandeln: Wir wählen einfach $C > 0$ klein genug, dass (4) für diese endlich vielen Fälle erfüllt ist.

Nun ist aber offensichtlich $A_k \leq 2^k$, weil es überhaupt nur 2^k Wörter der Länge k gibt. Dies ist ein Widerspruch zu (4), wenn k groß genug ist. □