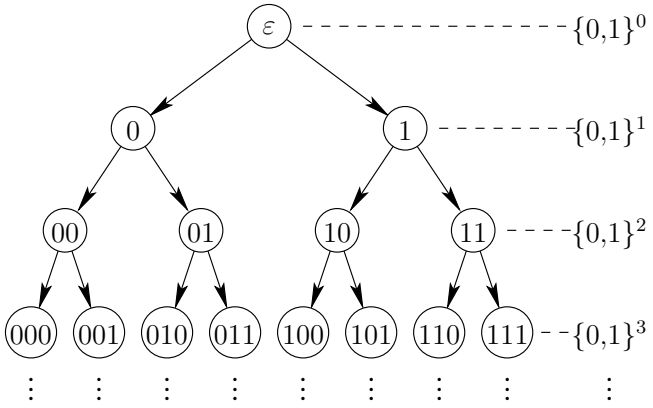
Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
ILMENAU

2. Studienbrief zur Informations- und Codierungstheorie

Aus Ihren Reihen kamen einige Fragen, die mir von so allgemeinem Interesse erschienen, daß ich an dieser Stelle darauf eingehen möchte statt einzeln zu antworten.

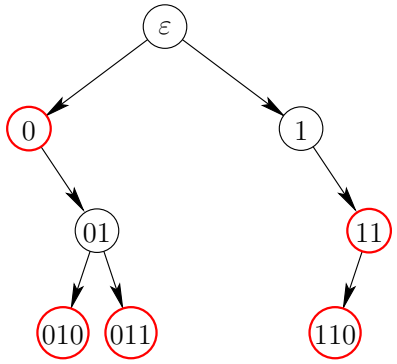
Hier noch einmal eine Anleitung, wie man zu Anschauungen und einfachen Beispielen kommen kann. Der Baum aller Wörter über A ist tatsächlich ein *unendlicher* Baum. Seine Eckenmenge ist *gleich* der Menge A^* aller Wörter, und man kann ihn zum Beispiel schichtweise wie in folgendem Bild darstellen. Exemplarisch sei $A = \{0, 1\}$, bei größeren Alphabeten ist der Baum entsprechend stärker verzweigt. Die Punkte im unteren Teil des Bildes deuten an, daß die Welt dort noch nicht zuende ist. Die Verzweigung findet systematisch statt: Das Wort $u0$ steht links, das Wort $u1$ rechts unter dem Wort u. Das muß so nicht sein, und der Baum muß auch nicht „schichtweise" gezeichnet werden, beides erhöht aber die Lesbarkeit.



Der von einem Code induzierte Baum ist der von allen Wörtern und ihrern Präfixen in diesem Graphen induzierte Teilgraph. Für den (recht übersichtlichen) Code

$$C = \{010, 011, 110, 11, 0\}$$

ist das zum Beispiel der folgende Teilbaum, wobei die Codewörter (das sind ja spezielle Ecken) rot eingekreist sind.

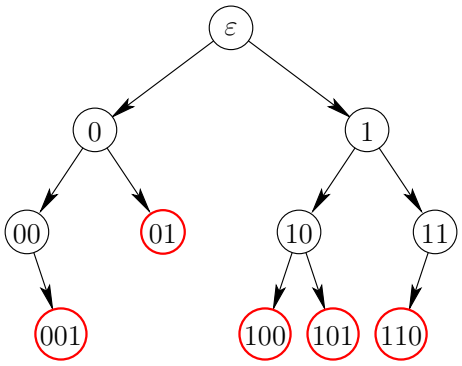


Weil der Baum mit jedem Wort u des Codes auch alle Präfixe von u enthält, gibt es darin stets einen von der Wurzel ausgehenden Weg nach u, also einen ε, u-Weg. Enthält dieser Weg ein weiteres Codewort $v \in C$, wie es in diesem Beispiel öfter geschieht, so ist v ein echtes Präfix von u und daher C nicht präfixfrei. Das sieht man dem Code selbst natürlich auch an: 0 ist Präfix von 010 und 011; 11 ist ein Präfix von 110.

Der präfixfreie Code

$$C = \{01, 001, 100, 101, 110\}$$

induziert dagegen folgenden Baum:



Die (wieder rot eingekreisten) Wörter aus C sind die Blätter des Baums.

Man kann mittels solcher Anschauungen auch alternative Beweise gewinnen, zum Beispiel für Satz 1, der besagt, daß ein präfixfreier Code (genauer: Dessen Längenprofil) die Kraftsche Ungleichung erfüllt: Dazu denke man sich jedes Wort u des präfixfreien Codes C im von C induzierten Baum mit der „Ladung" $1/|A|^{\ell(u)}$ versehen, alle anderen mit Ladung 0. In einem Entladungsschritt betrachten wir ein beliebiges Wort u mit der Eigenschaft, daß alle Nachfolger im Baum Blätter sind (ein Nicht-Blatt größter Länge ist ein solcher Kandidat). Alle Blätter unter u transportieren nun ihre Ladung Richtung u und werden danach

abgeschnitten; auf diese Weise erhält u (das zuvor die Ladung 0 hatte) eine Gesamtladung von höchstens $|A| \cdot 1/|A|^{\ell(u)+1} = 1/|A|^{\ell(u)}$ und wird zu einem Blatt des modifizierten Baumes; alle Nichtblätter des modifizierten Baumes behalten eine Ladung von 0. Induktiv schiebt man auf diese Weise die komplette Initialladung — die ja die linke Seite der zu beweisenden Ungleichung darstellt — auf das leere Wort ε, und diese Gesamtladung ist höchstens $1/|A|^{\ell(\varepsilon)} = 1/|A|^0 = 1/1 = 1$. Sie können die Wanderwege der Initialladung ja einmal im letzten Beispiel nachverfolgen! Im Prinzip beruht auch der Skript-Beweis von Satz 1 auf diesem Gedanken, das Spiel wird jedoch in jedem Schritt mit allen längsten Blätter zugleich gespielt.

*

Noch ein Wort zur Kraftschen Ungleichung: Auch das Längenprofil eines nicht präfixfreien Codes kann die Kraftsche Ungleichung erfüllen, zum Beispiel gilt das für $C = \{1, 11, 111\}$ als Code über dem Alphabet $A = \{0, 1\}$, denn: $1/2^1 + 1/2^2 + 1/2^3 = 7/8 \leq 1$. Das steht natürlich nicht im Widerspruch zu Satz 2; der besagt ja, daß es zum Längenprofil von C auch einen präfixfreien Code über A gibt; in der Tat ist $\{0, 10, 110\}$ ein solcher Code.

Abschließend noch ein Hinweis zu Aufgabe 3: Hierzu kann man ein aus den zwei Codewörtern 11 und 1110 zusammengesetztes Wort betrachten, zum Beispiel $w = u_1 u_2 \ldots u_r$ mit $u_i \in \{11, 1110\}$ und ein Verfahren angeben, daß die u_i zweifelsfrei bestimmt. Ein Ausgangspunkt kann sein: Ist der letzte Buchstabe von w eine Null, so ist zwingend $u_r = 1110$, andernfalls ist zwingend $u_r = 11$. Induktiv kann man dann alle u_i bestimmen. Dieses Vorgehen läßt sich auch leicht in einen Beweis übertragen, der näher an der Definition von eindeutiger Entzifferbarkeit liegt.

*

Ihr Lesepensum (siehe ganz unten) umfaßt unter anderem auch den Satz 4 mit Beweis. Dabei kommt in der abschließenden Abschätzung in der zweiten Gleichung das *allgemeine Ausmultiplizieren* zur Anwendung, etwas, das nach meiner Erfahrung gelegentlich Kummer bereitet. Sollten Sie bei mir die Anfängervorlesungen Grundlagen und Diskrete Strukturen oder Lineare Algebra I gehört haben, ist ihnen das Prinzip zuerst beim Beweis des allgemeinen binomischen Lehrsatzes erschienen.

Allgemein hat man es mit einem „langen" Produkt „langer Summen" zu tun, das in eine „sehr lange Summe" von Produkten umgeformt wird. Im beinahe einfachsten und bekanntesten Fall sieht das so aus:

$$(a + b) \cdot (A + B) = aA + aB + bA + bB.$$

Aus dem Produkt zweier Zweiersummen wird also eine Vierersumme von Produkten. Einem etwas größeren Fall sieht man schon das Allgemeine an:

$$\begin{aligned} & (a + b + c) \cdot (A + B + C) \cdot (\alpha + \beta) \\ = \quad & (aA + aB + aC + bA + bB + bC + cA + cB + cC) \cdot (\alpha + \beta) \end{aligned}$$

$$
\begin{aligned}
= \quad & aA\alpha + aB\alpha + aC\alpha + bA\alpha + bB\alpha + bC\alpha + cA\alpha + cB\alpha + cC\alpha \\
& + aA\beta + aB\beta + aC\beta + bA\beta + bB\beta + bC\beta + cA\beta + cB\beta + cC\beta
\end{aligned}
$$

Das Produkt von zwei Dreiersummen und einer Zweiersumme wird also eine 18er-Summe von Produkten. Wie sieht der typische Summand dieser 18er-Summe aus? Er ist ein Dreierprodukt, das sich aus den drei verschiedenen zu multiplizierenden Summen bedient: Der erste Faktor entstammt $a + b + c$, der zweite der Summe $A + B + C$ und der dritte der Summe $\alpha + \beta$. Alle 18 Auswahlmöglichkeiten werden dabei berücksichtigt, jede genau einmal.

Ganz allgemein hat man es mit k vielen zu multiplizierenden Summen zu tun, etwa

$$a_{i,1} + a_{i,2} + \ldots + a_{i,\ell(i)}$$

für $i \in \{1, \ldots, k\}$. Der erste Index i bei $a_{i,j}$ gibt also die Summe an, der zweite den Summanden innerhalb dieser i-ten Summe, und $\ell(i)$ ist die Anzahl dieser Summanden. Nun sollen alle diese Summen miteinander multipliziert werden, also

$$P := (a_{1,1} + \ldots + a_{1,\ell(1)}) \cdot \ldots \cdot (a_{k,1} + \ldots + a_{k,\ell(k)})$$

bestimmt werden. Wie wir ahnen, läßt sich P als Summe von Produkten schreiben. Der typische Summand ist ein Produkt von k vielen der $a_{i,j}$, mit genau einem Faktor aus jeder der k initialen Summen. Er sieht also so aus:

$$a_{1,j_1} \cdot a_{2,j_2} \cdot \ldots \cdot a_{k,j_k},$$

wobei die $j_1, \ldots, j_k$ natürlich angeben, welcher Summand der jeweiligen Summe hier beiträgt. Es gilt also

$$j_1 \in \{1, \ldots, \ell(1)\},\ j_2 \in \{1, \ldots, \ell(2)\}, \ldots, j_k \in \{1, \ldots, \ell(k)\},$$

oder, ein wenig gedrängter:

$$(j_1, \ldots, j_k) \in I := \{1, \ldots, \ell(1)\} \times \ldots \times \{1, \ldots, \ell(k)\}.$$

Jedes derartig formbare Produkt kommt in der P darstellenden Summe genau einmal vor:

$$P = \sum_{(j_1,\ldots,j_k)\in I} \prod_{i=1}^{k} a_{i,j_i},$$

und das ist es schon, das allgemeine Ausmultiplizieren. — In der schon angesprochenen Situation, Beweis Satz 4, ist alles sogar ein wenig einfacher: Hier wird nämlich einfach eine Summe in die k-te Potenz erhoben, also einunddieselbe Summe k-mal mit sich selber multipliziert. Ist

$$a_1 + \ldots + a_\ell$$

diese Summe, so erhält man mit den obigen Betrachtungen schlicht

$$(a_1 + \ldots + a_\ell)^k = \sum_{(j_1,\ldots,j_k)\in\{1,\ldots,\ell\}^k} \prod_{i=1}^{k} a_{j_i}.$$

Noch einfacher wird es im allgemeinen Binomialsatz, dort geht es nur um eine Zweiersumme

$$(a_1 + a_2)^k = \sum_{(j_1,\ldots,j_k)\in\{1,2\}^k} \prod_{i=1}^{k} a_{j_i}.$$

Tatsächlich ist der typische Summand $\prod_{i=1}^{k} a_{j_i}$ gleich $a_1^q \cdot a_2^{k-q}$, wobei q die Zahl der Einsen in $(j_1, \ldots, j_k)$ und $k - q$ die Zahl der Zweien angibt. Nun gibt es aber bekanntlich unter den 2^k vielen Auswahlmöglichkeiten für $(j_1, \ldots, j_k)$ genau $\binom{k}{q}$ viele, bei denen die Zahl der Einsen gleich q ist, und alle erzeugen denselben typischen Summanden $a_1^q \cdot a_2^{k-q}$. So kommt

$$(a_1 + a_2)^k = \sum_{q=0}^{k} \binom{k}{q} a_1^q \cdot a_2^{k-q},$$

oder, in etwas landläufigerer Notation:

$$(a + b)^k = \sum_{i=0}^{k} \binom{k}{i} a^i \cdot b^{k-i}.$$

*

Lesepensum bis zum 1. Mai 2020:

Skript bis Ende Abschnitt 1.2 (Skript Seite 9 ganz oben).

Das Lesepensum taugt eigentlich für anderthalb Wochen, nächste Woche wird's entsprechend entspannter.

*

Übungspensum bis zum 1. Mai 2020:

Aufgaben 1 bis 9 (siehe Skript Abschnitt 1.5).

*

Ilmenau, den 26. April 2020 · Matthias Kriesell