Thomas BORYS, Karlsruhe

Codierungen im Spiegel der fundamentalen Ideen der Mathematik

Täglich sind wir in unserem modernen Leben von Codierungen jeglicher Art umgeben. Beispielsweise begegnet man ihnen im Supermarkt in Form von Strichcodes, in Aufzügen, bei denen die Stockwerksangaben auch in Blindenschrift angegeben sind, auf Online-Tickets z.B. der Bahn als Aztec-Code oder der Lufthansa in Form der PDF 417, als Geheimcodes, wenn ein Schüler Sie z.B. mit den Worten „Gulewu Telewen Talewag“ begrüßt und eigentlich nur „Guten Tag“ sagen möchte, im Umfeld des Computers z.B. ASCII, JEPG, MPEG, MP3 etc. .

Nun stellt sich die Frage, inwiefern man Codierungen für den Mathematikunterricht nutzen kann.

Diese Frage soll exemplarisch an der Huffman-Codierung und den Verschlüsselungsschablonen nach Fleissner unter Zuhilfenahme der fundamentalen Ideen der Mathematik beantwortet werden.

1. Begriffsbestimmung: Codierung

Eine sehr gute Definition des Begriffs Codierung findet man bei Schulz:

„Seien A und B nichtleere Mengen und $N \in \mathbb{N}$; dann lässt sich eine injektive Abbildung $\underline{c}: A \to \bigcup_{i=1}^{N} B^i$ (*Codierung des Alphabets* A durch Wörter über B)

zu einer Abbildung $\underline{c}^*$ von der Menge A^* der Wörter über A in die Menge B^* fortsetzen indem sukzessive jeder Komponente das Bild unter $\underline{c}$ zugeordnet wird, genauer: $\underline{c}^*: \underline{c}^*(a_1 a_2 .. a_n) := \underline{c}^*(a_1)\,\underline{c}^*(a_2) .. \underline{c}^*(a_n)$ $(und\ \underline{c}^*(\emptyset) = \emptyset)$.

$\underline{c}^*$ heißt wie $\underline{c}$ Codierung, das Bild von $\underline{c}$ Code, seine Elemente Codewörter.“

Codes haben verschiedene Aufgaben, eine davon ist die Geheimhaltung von Nachrichten. Dies ist eigentlich der zentrale Gegenstandsbereich der Kryptologie, daher sollen in der folgenden Diskussion kryptologische Verfahren als Sonderformen von Codierungen berücksichtigt werden.

Durch die Identifikation von Codierungen mit injektiven Abbildungen wird schon an dieser Stelle sehr deutlich, dass Codierungen Funktionen sind und sie somit als Illustratoren der fundamentalen Idee des funktionalen Zusammenhangs im Mathematikunterricht eingesetzt werden können.

2. Fundamentale Ideen der Mathematik

Das Konzept der fundamentalen Ideen ist eine schon lange bzw. immer noch viel diskutierte Thematik in der Mathematikdidaktik. Schon Anfang des 20. Jahrhunderts forderte der englische Mathematiker A.N. Whitehead, dass sich der Unterricht an wenigen allgemeinen Ideen von weitreichender Bedeutung orientieren soll.

Ein weiterer wichtiger Vertreter des Konzepts der fundamentalen Ideen ist J. S. Bruner, der in seinem Buch „The Process of Education“ aus dem Jahre 1960 fordert: “It is simple enough to proclaim, of course, that school curricula and methods of teaching should be geared to the teaching of fundamental ideas in whatever subject is being taught.”

Im Verlauf der didaktischen Diskussion ergaben sich verschiedene Sammlungen fundamentaler Ideen für die Mathematik und ihre Teilgebiete. Eine gute Übersicht hierzu findet man z.B. bei Heymann, Schweiger oder Vohns.

Um die Frage, in wie weit Codierungen zur Illustration fundamentaler Ideen der Mathematik beitragen können, wird folgender eigener Katalog fundamentaler Ideen verwendet: *Algorithmus, funktionaler Zusammenhang, mathematisches Modellieren, Zahl, Messen* und *Ordnen* (das beinhaltet das geometrische Strukturieren und das logische Ordnen). Bei diesem Katalog handelt es sich um eine erste Arbeitsversion. Ihm liegen die Sammlungen fundamentaler Ideen von Schreiber, Tietze/Kilka/Wolpers, Humenberger/Reichel und Heymann zu Grunde.

3. Die Huffman-Codierung im Spiegel der fundamentalen Ideen der Mathematik

Der Huffman-Code wurde im September 1952 von D. Huffman in seinem Artikel mit dem Titel „A Method for the Construction of Minimum-Redundancy Codes” veröffentlicht. Für eine genaue Darstellung sei auf diesen Artikel verwiesen.

Mit der Huffman-Codierung kann die fundamentale Idee des *Algorithmus* konkretisiert werden, denn sie kann durch eine endliche Folge von eindeutig bestimmten Elementaranweisungen, die den Lösungsweg vollständig beschreiben, dargestellt werden. Sie arbeitet mit Baumstrukturen, die eines der wesentlichen Hilfsmittel der diskreten Mathematik sind. Die Huffman-Codierung liefert als Endergebnis einen Codebaum, wobei das Endergebnis nicht eindeutig ist, denn es existieren mehrere Codebäume mit den gleichen Eigenschaften. Im Gegensatz dazu stehen die meisten Algorithmen des Mathematikunterrichts in der Schule, welche üblicherweise mit Zahlen arbei-

ten und grundsätzlich ein eindeutig bestimmtes Endergebnis besitzen z.B. der euklidische Algorithmus.

Die fundamentale Idee des *funktionalen Zusammenhangs* findet sich bei der Huffman-Codierung gleich in mehrfacher Hinsicht: Zur Gewinnung der Huffman-Liste werden den Buchstaben Häufigkeiten, jedem Knoten werden summierte Häufigkeiten und jeder Kante im Codebaum wird ein binäres Zeichen „0“ oder „1“ zugeordnet. Das Endergebnis, die gewonnene Codetabelle, stellt eine Funktion der Zeichen einer Nachricht zu einem binären Code dar.

Die fundamentale Idee der *Zahl* spielt beim Huffman-Verfahren eine entscheidende Rolle. So werden Zahlen in mehrfacher Hinsicht verwendet, jeweils in Verbindung mit einem anderen Zahlaspekt. Zur Erstellung der Häufigkeitsliste muss bestimmt werden, mit welcher Anzahl die jeweiligen Buchstaben in der Nachricht vorkommen. Diesem Vorgang liegt der Kardinalzahlaspekt zu Grunde. Statt mit absoluten Häufigkeiten, kann man bei der Huffman-Codierung auch mit relativen Häufigkeiten arbeiten, was dem Bruchzahlaspekt - relativer Anteil nach Günther Malle - entspricht. Anschließend werden die Buchstaben nach ihren Häufigkeiten geordnet, dies entspricht dem Ordinalzahlaspekt. Schließlich findet sich der Rechenzahlaspekt bei der Addition der verschiedenen Häufigkeiten.

Durch die Überlegungen zum Informationsgehalt einer Nachricht und zur Optimalität der Codewortlänge kann durch die Huffman-Codierung ein Beitrag zur fundamentalen Idee des *Messens* geleistet werden.

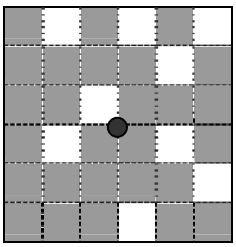
Zur fundamentalen Idee des *Ordnens* kann das Thema der Huffman-Codierung in zweierlei Hinsicht beitragen. Einerseits wird durch das Sortieren der Zeichen nach ihren Häufigkeiten eine Ordnung hergestellt (siehe Idee der Zahl), andererseits erfolgt eine Ordnung durch das Anordnen der Zeichen in Form von Knoten innerhalb eines Graphen.

4. Verschlüsselungsschablonen nach Fleissner im Spiegel der fundamentalen Ideen der Mathematik

E. Fleissner von Wostrowitz beschreibt in seinem Handbuch zur Kryptographie von 1881, wie man Verschlüsselungsschablonen zur Permutation von Buchstaben eines Textes verwenden kann. Ein geeignetes Beispiel für den Unterricht stammt von Jules Verne aus seinem Roman „Matthias Sandorf“ (siehe folgende Abbildung).

Zur Verschlüsselung werden die freien Felder nacheinander mit den Buchstaben des Klartextes beschriftet. Sind die Felder ausgefüllt wird die Schablone um ihren Mittelpunkt um 90° gedreht und die neuen freien Felder wer-

den ausgefüllt. Das wird noch zweimal wiederholt, dann hat man meistens das gesamte Quadrat ausgefüllt. Der Geheimtext wird spaltenweise ausgelesen. Ist der Klartext zu kurz, ergänzt man ihn mit einer sinnlosen Folge von Buchstaben, ist er zu lang, so verwendet man ein zweites Quadrat. Für weitere genauere Beschreibungen sei auf Fleissner verwiesen.



Bei Ver- und Entschlüsselung handelt es sich um einen *algorithmischen* Vorgang, der händisch ausgeführt werden kann. Die fundamentale Idee des *funktionalen Zusammenhangs* findet sich beim Ergebnis des Verschlüsselungsvorgangs wieder, denn mit ihm wird der Klartext durch den Geheimtext ersetzt. Erreicht wird dies durch eine Permutation der Buchstaben. Da die Verschlüsselung durch Drehung der Schablone erfolgt, kann der geometrische Begriff der Drehung auf besondere handelnde Art und Weise dargestellt werden. Durch die Beantwortung der Frage nach der Konstruktion einer funktionierenden Verschlüsselungsschablone wird die fundamentale Idee des *Ordnens* vertieft. Berechnet man die Anzahl der verschiedenen funktionsfähigen Verschlüsselungsschablonen, ist man im Bereich der fundamentalen Idee der *Zahl*.

Insgesamt wird deutlich, dass es sich lohnt, Codierungen unter dem Blickwinkel der fundamentalen Ideen der Mathematik in Augenschein zu nehmen. Codierungen stellen somit eine Bereicherung für den Mathematikunterricht dar.

Fleissner von Wostrowitz, E. (1881). *Handbuch der Kyptographie.* Wien: K. k. Hofbuchdruckerei Carl Fromme.

Heymann, H. W. (1996). *Allgemeinbildung und Mathematik*. Weinheim: Beltz Verlag

Huffman D. (1952). *A Method for the Construction of Minimum-Redundancy Codes*, Prococeedings of the I.R.E., pp. 1098-1101

Schreiber, A. (1979). *Universelle Ideen im mathematischen Denken – ein Forschungsgegenstand der Didaktik.* In: mathematica didactica 2, 165-171

Schweiger, F. (1992). *Fundamentale Ideen. Eine geistesgeschichtliche Studie zur Mathematikdidaktik.* Journal für Mathematikdidaktik (13), 2/3 S. 207-214

Schulz, R.-H. (2003). *Codierungstheorie*. 2. Auflage, Wiesbaden: Vieweg

Tietze, U.-P., Klika, M., Wolpers, H. (Hrsg.) (2000). *Mathematikunterricht in der Sekundarstufe II* Band 1. 2. Auflage, Wiesbaden: Vieweg

Vohns, A. (2007). *Grundlegende Ideen und Mathematikunterricht*. Norderstedt: BoD