

H. JÜRGENSEN

M. KUNZE

**Charakterisierung redundanzfreier codes
zur datenverschlüsselung**

RAIRO. Informatique théorique, tome 18, n° 2 (1984), p. 131-146

http://www.numdam.org/item?id=ITA_1984__18_2_131_0

© AFCET, 1984, tous droits réservés.

L'accès aux archives de la revue « RAIRO. Informatique théorique » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

CHARAKTERISIERUNG REDUNDANZFREIER CODES ZUR DATENVERSCHLÜSSELUNG (*)

par H. JÜRGENSEN ⁽¹⁾ et M. KUNZE ⁽²⁾

Communiqué par J. BERSTEL

Résumé. — On étudie une famille des applications qui sont définies comme objets arithmétiques et qui peuvent être utilisées comme codes sans redondance et aussi comme codes cryptographiques. Dans cet article on présente une caractérisation axiomatique de ces codes. Un article subséquent considère leur complexité algorithmique, une question fondamentale pour leur application pratique.

Abstract. — A class of arithmetically defined mappings which are suitable for redundancy-free encoding of messages of a discrete information source is studied. Here, we give an axiomatic characterization of these redundancy-free codes. A forthcoming paper deals with the complexity of the corresponding encoding algorithms which is crucial for the proposed cryptographic application in data protection.

EINLEITUNG

Kryptocodes haben in letzter Zeit erhebliche Bedeutung im Bereich des Datenschutzes gewonnen ([13] mit umfangreicher Bibliographie); sie werden eingesetzt, um z.B. die Zugriffsrechte auf Daten jeweils autorisierten Rechnerbenutzern vorbehalten oder die Herkunft von Daten nachweisen zu können.

Von einer guten Kryptocodierung wird man verlangen, dass sie selbst wie auch die Decodierung effiziente Realisierungen besitzen, dass aber die Kryptanalyse unter verschiedenen, je nach Aufgabenbereich unterschiedlich vereinfachenden Bedingungen unverhältnismässig schwierig ist. Eine der wichtigsten Methoden der Kryptanalyse findet man — allerdings in ihrer einfachsten Form — spannend in Poes Goldkäfer beschrieben: Es werden die statistischen Eigenschaften von Kryptogramm und Quellsprache verglichen. Die Analyse gelingt durch Anpassung der entsprechenden Häufigkeitsvertei-

(*) Reçu en avril 1981, révisé en juillet 1983.

⁽¹⁾ Department of Computer Science, The University of Western Ontario, London, Ontario, Canada, N6A 5B7.

⁽²⁾ Department of Mathematics, University of Arkansas, Fayetteville, AR 72701, U.S.A.

lungen und aufgrund der Kenntnis des Verschlüsselungsverfahrens. Eine moderne Version dieses Verfahrens wird in [1] beschrieben.

Es ist klar, dass sich der statistische Analyseversuch nur dadurch verhindern lässt, dass die statistischen Eigenschaften des Kryptogramms mit denen des Quelltextes oder der Quellsprache in höchstens sehr komplizierter Weise zusammenhängen; genauer wird man insbesondere versuchen, die im Quelltext vorhandene Redundanz im Kryptogramm zu beseitigen. Selbstverständlich braucht dabei das Kryptogramm selbst gar nicht redundanzfrei zu sein; dies ist wichtig im Hinblick auf die sichere Übertragung des Kryptogramms durch ein gestörtes Übertragungsmedium. Man kann sich die Verschlüsselung gewissermassen zerlegt vorstellen in eine Codierung, welche die Redundanz des Quelltextes beseitigt, und eine weitere Codierung, welche wiederum Redundanz zur Erhöhung der Übertragungssicherheit einführt.

Redundanzfreie Codes könnten einen ersten Schritt in Richtung auf eine statistisch nicht analysierbare Kryptocodierung darstellen; diese Grundidee liegt vielen der klassischen Verfahren zugrunde; man findet sie von Shannon ausgesprochen [14]. Neuerdings wurde diese Idee wieder von Rubin [11] diskutiert.

Ein Satz der Informationstheorie [z.B. 2] garantiert, dass bei geeigneter Codierung genügend langer Ausgabeblöcke einer stationären diskreten Quelle Q der mittlere Informationsgehalt je Symbol der codierten Nachricht fast gleich der Entropie $H(Q)$ von Q wird; die Redundanz der codierten Nachricht wird dann fast 0. Als Codierungsverfahren für diese Aufgabe kommen einerseits solche Verfahren in Frage, die zu wachsender Länge der Ausgabeblöcke von Q jeweils einen optimalen Code benutzen (z.B. Huffmancode) und andererseits solche, die den Grenzübergang aus dem Vorgehenden vorwegnehmend, unter Benutzung unbeschränkt grosser Rechner in einem Schritt einen redundanzfreien Code herstellen (etwa die arithmetischen Codierungen). Rubin [11] weist darauf hin, dass einfache Huffmancodes noch genügend viel Redundanz haben, um eine statistische Analyse nicht auszuschliessen — dies ist vermutlich der Kernpunkt seines Arguments. Dies ist sicherlich richtig solange die Blocklänge des Huffmancodes klein ist. Man könnte das Problem für gedächtnislose Quellen durch Huffmancodes grösserer Länge zu lösen versuchen, wobei aber die Praktikabilität zu diskutieren wäre, weil für den Rechenaufwand aufgrund vergrösserter Blocklänge schnell anwachsende Codierungstabellen zu berücksichtigen sind. Da wir jedoch im Hinblick auf die Praxis vielmehr an komplexeren Informationsquellen interessiert sind, beschäftigen wir uns hier nicht näher mit der soeben angesprochenen Möglichkeit. Nichtsdestoweniger stellen auch für uns gerade die gedächtnislosen Quellen wegen ihrer Einfachheit ein willkommenes Schulbeispiel dar, beson-

ders, weil sich viele interessante Eigenschaften der in dieser Arbeit studierten Codes schon an diesen demonstrieren lassen. Rubin [11] schlägt dann die Benutzung arithmetischer Codes [4], [6], [7], [10], [12] vor. Das Hauptproblem bei der Verwendung arithmetischer Codes ist zweifellos die Realisierbarkeit von Codierung und Decodierung. Dieses Problem bildete den Ausgangspunkt der vorliegenden Arbeit, wird aber erst in deren zweiten Teil »Über die Implementierung...« in den Mittelpunkt des Interesses rücken [8].

Im vorliegenden, ersten Teil der Arbeit geht es vor allem um die axiomatische Beschreibung redundanzfreier Codes. Durch diese abstrakte Beschreibung ist es nämlich relativ einfach, eine konkrete Vorstellung von diesen Abbildungen zu gewinnen, welche eine redundanzfreie Codierung einer diskreten Informationsquelle leisten. Die eigentlichen Schwierigkeiten ergeben sich erst aus der für die Praxis natürlich unverzichtbaren Forderung, dass die codierten Nachrichten selbst wieder über einem endlichen Alphabet dargestellt sein sollen. Doch auf diese, wenn man so will, syntaktischen Probleme, werden wir wie gesagt erst im zweiten Teil zu sprechen kommen.

AXIOMATISCHE BESCHREIBUNG REDUNDANZFREIER CODES

Sei $Q=(\Sigma, p)$ eine diskrete Informationsquelle mit Alphabet $\Sigma = \{a_1, \dots, a_n\}$, $n \geq 2$, und Wahrscheinlichkeitsmass p auf der von den Zylindermengen erzeugten σ -Algebra \mathcal{L} über :

$$\Sigma^\omega := \{b_1 b_2 \dots \mid \forall i \in \mathbb{N} : b_i \in \Sigma\}.$$

Mit Σ^* sei die Menge der Wörter (endlicher Länge) über Σ bezeichnet; \square ist das leere Wort. Abkürzend schreiben wir oft w für die Zylindermenge $w\Sigma^\omega$. Für hier nicht erklärte Begriffe der Informationstheorie wird auf [3] oder [5] verwiesen.

Wir betrachten Abbildungen $f : \Sigma^* \rightarrow [0, 1] \subseteq \mathbb{R}$, die als redundanzfreie Codierungen in Frage kommen, und dabei insbesondere solche, die den Forderungen E1, E2, E3 genügen :

(E1) *Relative Konvexität* : Für alle $w \in \Sigma^*$ ist $f(w\Sigma^*)$ konvex in $f(\Sigma^*)$.

(E2) *Schwache Injektivität* : Für alle $w \in \Sigma^*$ gilt :

$$f^{-1}(f(w\Sigma^*) \setminus \{\inf f(w\Sigma^*), \sup f(w\Sigma^*)\}) \subseteq w\Sigma^*.$$

(E3) *Schwache Gleichverteilung* : Für alle $w \in \Sigma^*$ ist :

$$\sup f(w\Sigma^*) - \inf f(w\Sigma^*) = p(w\Sigma^\omega).$$

Die Forderungen E1-E3 besagen, dass disjunkte Mengen $v\Sigma^*$, $w\Sigma^*$ in fast-disjunkte Teilintervalle von $[0, 1]$ abgebildet werden, deren Länge sich aus den entsprechenden Wahrscheinlichkeiten ergibt. E1 ist dadurch motiviert, dass $f(w)$ möglichst leicht durch einen rekursiven Algorithmus entsprechend der Gestalt von w berechnet werden können sollte.

Mit \mathbf{O}_w^f sei das offene Intervall

$$] \inf f(w\Sigma^*), \sup f(w\Sigma^*) [$$

bezeichnet. Aus E1 und E2 zusammen folgt, dass jedes abgeschlossene Intervall $\overline{\mathbf{O}_w^f}$ in $f(\Sigma^*)$ konvex ist und dass als Bildpunkt $f(w)$ nur ein Punkt in der Menge

$$\overline{\mathbf{O}_w^f} \setminus \bigcup_{a \in \Sigma} \mathbf{O}_{wa}^f$$

in Frage kommt. Es ist nämlich :

$$f^{-1}(\overline{\mathbf{O}_w^f} \cap f(\Sigma^*)) \subseteq w\Sigma^*.$$

Es soll nun erreicht werden, dass die »Codewörter« für die von Q gesendeten Nachrichten, d.h., die Elemente von $f(\Sigma^*)$ gleichmässig auf das Intervall $[0, 1]$ verteilt werden; dies würde bewirken, dass die Bildmenge unter f als Ausgabe einer redundanzfreien gedächtnislosen Quelle aufgefasst werden kann, so dass die codierten Nachrichten keine statistische Information über die uncodierten Nachrichten mehr tragen. Dazu liegt im Hinblick auf die angestrebte »gleichmässige Verteilung« von $f(\Sigma^*)$ auf $[0, 1]$ eine Forderung der Art $p(f(w) \in [x, y]) = y - x$ nahe; diese erweist sich jedoch als präzisionsbedürftig. Die gewählte Formulierung E4 kann als eine solche Präzisierung verstanden werden :

(E4) *Redundanzfreiheit* : Für alle $x, y \in [0, 1]$, $x \leq y$ hat die Menge :

$$W_{x,y} = \{ w \mid f(w\Sigma^*) \subseteq [x, y] \} \Sigma^{\omega}$$

das p -Mass $p(W_{x,y}) = y - x$.

Wir werden unten die Abhängigkeiten im Axiomensystem E1-E4 genauer untersuchen, indem wir einige mit E4 äquivalente Bedingungen herleiten. Im Hinblick auf dieses Ziel ist es nützlich, die Elemente $\alpha \in \Sigma^{\omega}$ als Zahlen $\iota(\alpha) \in [0, 1]$ in der üblichen Weise zu interpretieren : Man fasst die Symbole $a_1, \dots, a_n \in \Sigma$ als Ziffern $0, 1, \dots, n-1$ auf und versteht $\iota(\alpha)$ als die n -adisch dargestellte Zahl $0, \alpha$. Man beachte, dass jede Zahl $x \in [0, 1]$ höchstens zwei n -adische Darstellungen hat, d.h. $|\iota^{-1}(x)| \leq 2$. Mit \mathcal{B} sei die σ -Algebra der Borelmengen in $[0, 1]$ bezeichnet. Man beweist leicht :

LEMMA 1. — Die Abbildung $\iota: \Sigma^\omega \rightarrow [0, 1]$ ist \mathcal{L} - \mathcal{B} -messbar.

Das durch ι auf $([0, 1], \mathcal{B})$ von p induzierte Mass werde mit \bar{p} bezeichnet; φ_p sei die zugehörige Verteilungsfunktion. Der folgende Satz nennt einige Äquivalente zur Forderung E4 :

SATZ 2. — $Q=(\Sigma, p)$ sei eine diskrete Quelle, und $f: \Sigma^* \rightarrow [0, 1]$ sei eine Abbildung, die den Axiomen E1-E3 genügt. Dann sind die folgenden Aussagen äquivalent :

(E4) Für alle $x, y \in [0, 1], x \leq y$, ist $p(W_{x,y}) = y - x$.

(E4₁) $f(\Sigma^*)$ ist dicht in $[0, 1]$.

(E4₂) Für jede Folge $(b_i | b_i \in \Sigma)_{i \in \mathbb{N}}$ ist $\lim_{i \rightarrow \infty} p(b_1 \dots b_i \Sigma^\omega) = 0$.

(E4₃) φ_p ist stetig.

Beweis. — Die Äquivalenz von E4₂ und E4₃ ist klar. Den Rest der Behauptung beweisen wir in der Reihenfolge $E4 = \supset E4_1 = \supset E4_2 = \supset E4$.

Es sei E4 erfüllt, und E4₁ gelte nicht : Dann gibt es $x, y \in [0, 1], x < y$, mit

$$f(\Sigma^*) \cap [x, y] = \emptyset.$$

Folglich ist

$$p(W_{x,y}) = p(\emptyset) = 0 \neq y - x$$

im Widerspruch zu E4.

Falls E4₁ gilt, jedoch nicht E4₂, so existiert eine Folge $(b_i | b_i \in \Sigma)_{i \in \mathbb{N}}$ mit

$$\lim_{i \rightarrow \infty} p(b_1 \dots b_i \Sigma^\omega) = \alpha > 0.$$

Die offenen Intervalle $I_i = \mathbf{O}_{b_1 \dots b_i}^f$ bilden eine monoton fallende Kette, und mit E1 folgt :

$$f(\Sigma^*) \cap I_i \subseteq f(b_1 \dots b_i \Sigma^*)$$

Wegen E3 hat I_i die Länge $p(b_1 \dots b_i \Sigma^\omega)$, und daher hat das Intervall :

$$I := \bigcap_i I_i$$

die Länge $\lim_{i \rightarrow \infty} p(b_1 \dots b_i \Sigma^\omega) = \alpha > 0$. Sei nun $w \in \Sigma^*$ ein beliebiges Wort.

Falls

$$w \neq b_1 \dots b_{|w|}$$

ist, so ist wegen E1, E2 $f(w) \in I$ für ein $j \leq |w|$; ist andererseits $w = b_1 \dots b_{|w|}$, so ist wegen E1, $f(w) \notin I_{|w|+1} \supseteq I$. Es folgt also $I \cap f(\Sigma^*) = \emptyset$ im Widerspruch zur Voraussetzung.

Es sei jetzt E4₂ vorausgesetzt, und es seien $x, y \in [0, 1], x \leq y$. Es gilt

$$W_{x,y} = \bigcup_{i=0}^{\infty} (W_{x,y,i} \Sigma^{\omega})$$

mit

$$W_{x,y,i} := \{u \in \Sigma^i, f(u \Sigma^*) \subseteq [x, y]\}$$

$W_{x,y}$ ist also p -messbar. Nun gilt

$$W_{x,y,0} \Sigma^{\omega} \subseteq W_{x,y,1} \Sigma^{\omega} \subseteq \dots \subseteq W_{x,y,i} \Sigma^{\omega} \subseteq \dots \subseteq W_{x,y}$$

und daher folgt mit E1-E3 :

$$\begin{aligned} p(W_{x,y}) &= \lim_{i \rightarrow \infty} p(W_{x,y,i} \Sigma^{\omega}) = \lim_{i \rightarrow \infty} \sum_{\substack{u \in \Sigma^i \\ f(u \Sigma^*) \subseteq [x, y]}} p(u \Sigma^{\omega}) \\ &= \lim_{i \rightarrow \infty} \sum_{\substack{u \in \Sigma^i \\ f(u \Sigma^*) \subseteq [x, y]}} (\sup f(u \Sigma^*) - \inf f(u \Sigma^*)) \leq y - x. \end{aligned}$$

Bei dieser Abschätzung wurde E4₂ noch nicht verwendet. Sei ferner

$$\overline{W}_{x,y,i} := \{u \in \Sigma^i, f(u \Sigma^*) \cap [x, y] \neq \emptyset \neq f(u \Sigma^*) \cap ([0, x] \cup [y, 1])\}.$$

Es gilt :

$$\begin{aligned} (W_{x,y,0} \cup \overline{W}_{x,y,0}) \Sigma^{\omega} &\supseteq (W_{x,y,1} \cup \overline{W}_{x,y,1}) \Sigma^{\omega} \supseteq \dots \\ &\supseteq (W_{x,y,i} \cup \overline{W}_{x,y,i}) \Sigma^{\omega} \supseteq \dots \supseteq W_{x,y} \end{aligned}$$

Dabei ist :

$$\begin{aligned} p\left(\bigcap_{i=0}^{\infty} (W_{x,y,i} \cup \overline{W}_{x,y,i}) \Sigma^{\omega}\right) &= \lim_{i \rightarrow \infty} p(W_{x,y,i} \cup \overline{W}_{x,y,i} \Sigma^{\omega}) \\ &= \lim_{i \rightarrow \infty} p(W_{x,y,i} \Sigma^{\omega}) + \lim_{i \rightarrow \infty} p(\overline{W}_{x,y,i} \Sigma^{\omega}) \\ &= \lim_{i \rightarrow \infty} p(W_{x,y,i} \Sigma^{\omega}) = p(W_{x,y}); \end{aligned}$$

Wegen E1-E3 ist $\overline{W}_{x,y,i}$ nämlich höchstens zweielementig, und es gibt (höchstens) zwei Folgen $\alpha, \beta \in \Sigma^\omega$, so dass für alle i die Elemente von $\overline{W}_{x,y,i}$ Präfixe von α oder β sind; mit E4₂ gilt dann :

$$\lim_{i \rightarrow \infty} p(\overline{W}_{x,y,i} \Sigma^\omega) = 0.$$

Nun gilt wegen E3

$$1 = \sum_{u \in \Sigma^i} p(u \Sigma^\omega) = \sum_{u \in \Sigma^i} (\sup f(u \Sigma^*) - \inf f(u \Sigma^*)),$$

und wegen E1 und E2 sind die offenen Intervalle O_u^f für die $u \in \Sigma^i$ paarweise disjunkt.

Folglich gilt für die Mengen

$$T_{x,y,i} := \bigcup_{\substack{u \in \Sigma^i \\ f(u \Sigma^*) \cap [x,y] \neq \emptyset}} \overline{O}_u^f,$$

dass

$$T_{x,y,i} = [\inf f((W_{x,y,i} \cup \overline{W}_{x,y,i}) \Sigma^*), \sup f((W_{x,y,i} \cup \overline{W}_{x,y,i}) \Sigma^*)]$$

und

$$\inf T_{x,y,i} \leq x \leq y \leq \sup T_{x,y,i}$$

ist. Daher folgt :

$$\begin{aligned} p(W_{x,y}) &= \lim_{i \rightarrow \infty} p((W_{x,y,i} \cup \overline{W}_{x,y,i}) \Sigma^\omega) = \lim_{i \rightarrow \infty} \sum_{u \in W_{x,y,i} \cup \overline{W}_{x,y,i}} p(u \Sigma^\omega) \\ &= \lim_{i \rightarrow \infty} \sum_{u \in W_{x,y,i} \cup \overline{W}_{x,y,i}} (\sup f(u \Sigma^*) - \inf f(u \Sigma^*)) \\ &= \lim_{i \rightarrow \infty} \sup (T_{x,y,i} - \inf T_{x,y,i}) \geq y - x \end{aligned}$$

Damit ist

$$y - x \leq p(W_{x,y}) \leq y - x$$

bewiesen. \square

DEFINITION 3. — Eine diskrete Informationsquelle (Σ, p) heisst *schwach determiniert* bei $\beta = b_1 b_2 b_3 \dots \in \Sigma^\omega$, falls $p(\beta) := \lim_{i \rightarrow \infty} p(b_1 b_2 \dots b_i \Sigma^\omega) > 0$

ist.

Satz 2 lehrt also, dass wir mit Abbildungen, die den Axiomen E1-E3 genügen, redundanzfreie Codierungen für solche Informationsquellen (Σ, p) erhalten, die bei keinem $\beta \in \Sigma^\omega$ schwach determiniert sind.

Beispiel 4. — Sei $\Sigma = \{a, b\}$. Die Wahrscheinlichkeit dafür, dass das i -te gesendete Symbol der Quelle $Q = (\Sigma, p)$ ein b ist, sei $2^{-(i+1)}$. Man erhält also für $x_1, x_2, \dots \in \Sigma$:

$$p(x_1 \dots x_j \Sigma^\omega) = \prod_{\substack{x_i = a \\ i \leq j}} (1 - 2^{-(i+1)}) \prod_{\substack{x_i = b \\ i \leq j}} 2^{-(i+1)} \leq \prod_{\substack{x_i = b \\ i \leq j}} 2^{-(i+1)}.$$

Ist dabei $\{i \mid x_i = b\}$ unendlich, so ist daher

$$\lim_{j \rightarrow \infty} p(x_1 \dots x_j \Sigma^\omega) = 0.$$

Ist andererseits diese Menge endlich, d.h. $x_1 x_2 \dots \in \Sigma^* a^\omega$, etwa $x_1 x_2 \dots \in \Sigma^k a^\omega$, so gilt:

$$\begin{aligned} \lim_{i \rightarrow \infty} p(x_1 \dots x_j \Sigma^\omega) &= p(x_1 \dots x_k \Sigma^\omega) \lim_{j \rightarrow \infty} \prod_{x=k+1}^j (1 - 2^{-(i+1)}) \\ &\cong \left(\prod_{\substack{x_i = a \\ i \leq k}} (1 - 2^{-(i+1)}) \right) \left(\prod_{\substack{x_i = b \\ i \leq k}} 2^{-(i+1)} \right) (1 - 2^{-(k+1)}) > 0. \end{aligned}$$

Q ist also genau bei den Folgen $x_1 x_2, \dots \in \Sigma^* a^\omega$ schwach determiniert.

Wir geben jetzt eine Klasse \mathcal{F}_Q von Abbildungen

$$f_{\tau, \pi}: \Sigma^* \rightarrow [0, 1]$$

explizit an und zeigen dann, dass \mathcal{F}_Q durch E1-E3 charakterisiert wird; als Parameter dienen dabei Funktionen

$$\tau: \Sigma^* \rightarrow \{0, 1, \dots, n\}$$

und

$$\pi: \Sigma^* \times \{1, \dots, n\} \rightarrow \{1, \dots, n\},$$

wobei $\pi(w, \cdot)$ für jedes feste $w \in \Sigma^*$ eine Permutation von $n := \{1, \dots, n\}$ ist.

Als Spezialfälle werden insbesondere betrachtet: Für τ die Konstanten

$$\bar{i}: \Sigma^* \rightarrow \{i\}$$

und für π die Abbildung

$$e: \Sigma^* \times \underline{n} \rightarrow \underline{n}: (w, i) \mapsto i.$$

Zur Definition der Abbildung $f_{\tau, \pi}$ benötigen wir zwei Hilfsfunktionen

$$q_{\pi}: \Sigma^* \times \{0, 1, \dots, n\} \rightarrow [0, 1]$$

und

$$m: \Sigma \rightarrow [0, 1].$$

q_{π} beschreibt die *Codierung der einzelnen Buchstaben*, etwa des Buchstabens $a_{\pi(w, i)} \in \Sigma$, der auf das Wort $w \in \Sigma^*$ folgt; wir setzen

$$q_{\pi}(w, i) := \begin{cases} 0 & \text{falls } i=0 \text{ oder } p(w)=0, \\ \frac{1}{p(w)} \cdot \sum_{j=1}^i p(wa_{\pi(w, j)}) & \text{sonst.} \end{cases}$$

Im zweiten Fall ist also $q_{\pi}(w, i)$ die bedingte Wahrscheinlichkeit

$$p\left(a_{\pi(w, j)} \text{ für } j=1, \dots, i \mid \text{vorher war } w\right) = \sum_{j=1}^i p(a_{\pi(w, j)} \mid w).$$

m definiert die *Streckungsfaktoren*: Der Buchstabe $a_{\pi(w, i)} \in \Sigma$, der auf $w \in \Sigma^*$ folgt, erhält

$$m(w) := p(w)$$

als *Positionscode*.

Damit können wir jetzt $f_{\tau, \pi}$ definieren:

$$f_{\tau, \pi}(w) = \begin{cases} 0, & \text{falls } w = \square, \text{ das leere Wort, und } \tau = \bar{0}, \\ \tilde{f}_{\bar{0}, \pi}(\hat{w}) + m(\hat{w}) \cdot q_{\pi}(\hat{w}, i-1), \\ \quad \text{wobei } w = \hat{w}a_{\pi(\hat{w}, i)} \text{ und } a_{\pi(\hat{w}, i)} \in \Sigma, \text{ falls } w \neq \square \text{ und } \tau = \bar{0}, \\ \tilde{f}_{\bar{0}, \pi}(w) + m(w) q_{\pi}(w, \tau(w)), & \text{sonst.} \end{cases}$$

Der letzte Fall bewirkt eine Art »Schlussmarkierung«, deren Auswahl durch τ gesteuert wird. In der kryptographischen Anwendung wird man π und τ als die sogenannten Schlüssel ansehen.

Wir stellen zunächst einige Eigenschaften von $f_{\tau, \pi} \in \mathcal{F}_Q$ zusammen, die eine gute Vorstellung von der Wirkungsweise dieser Funktionen vermitteln.

LEMMA 5. — Für alle $w \in \Sigma^*$ gilt :

$$f_{\tau, \pi}(w \Sigma^*) \subseteq [f_{\bar{0}, \pi}(w), f_{\bar{0}, \pi}(w) + m(w)]. \quad (1)$$

$$f_{\tau, \pi}(w a_{\pi(w, i)} \Sigma^*) \subseteq [f_{\bar{0}, \pi}(w a_{\pi(w, i)}), f_{\bar{0}, \pi}(w a_{\pi(w, i+1)})] \quad (2)$$

für $i = 1, \dots, n-1$.

$$\text{Falls } Q \text{ nirgends schwach determiniert ist, gilt :} \quad (3)$$

und

$$f_{\bar{0}, \pi}(w) = \inf (f_{\tau, \pi}(w \Sigma^*))$$

$$f_{\bar{n}, \pi}(w) = \sup (f_{\tau, \pi}(w \Sigma^*)).$$

$$f_{\tau, \pi}(w) \in \{ f_{\bar{0}, \pi}(w a_{\pi(w, i)}) \mid i = 1, \dots, n \} \cup \{ f_{\bar{n}, \pi}(w) \}. \quad (4)$$

Der relativ einfache Induktionsbeweis sei dem Leser überlassen.

Die graphische Darstellung des folgenden Beispiels in Abbildung 1 veranschaulicht die Situation :

Beispiel 6. — $Q = (\Sigma, p)$ sei gedächtnislos mit

$$\Sigma = \{ a_1 = a, a_2 = b, a_3 = c \}, p(a) = \frac{1}{2}, p(b) = \frac{1}{3}, p(c) = \frac{1}{6}.$$

Es sei $\tau(w) = 1$ für alle $w \in \Sigma^*$ und

$$\pi(w, i) = \begin{cases} i, & \text{falls } |w| \text{ gerade ist,} \\ i+1 \bmod 3, & \text{falls } |w| \text{ ungerade ist.} \end{cases}$$

Im folgenden Beispiel ist $f_{\tau, \pi}$ zu einer einwertigen Funktion degeneriert. Derartige Fälle werden wir in Zukunft durch E4 auszuschliessen haben.

Beispiel 7. — $\Sigma = \{ a_1, a_2 \}$, $p(a_1^k \Sigma^\omega) = 1$ für alle k , $\tau = \bar{1}$, $\pi = \bar{e}$. Dann gilt :

$$f_{\bar{0}, \pi}(w) = \begin{cases} 1 & \text{für } w \in \Sigma^* a_2 \Sigma^* \\ 0 & \text{für } w \in a_1^* \end{cases}$$

und

$$f_{\tau, \pi}(w) = 1 \text{ für alle } w.$$

Die folgende Aussage rechtfertigt das bisherige Vorgehen.

SATZ 8. — $Q = (\Sigma, r)$ sei eine diskrete Quelle, $|\Sigma| \geq 2$. Falls Q nirgends schwach determiniert ist, stimmt \mathcal{F}_Q mit der durch E1-E3 definierten Funktionenklasse überein.

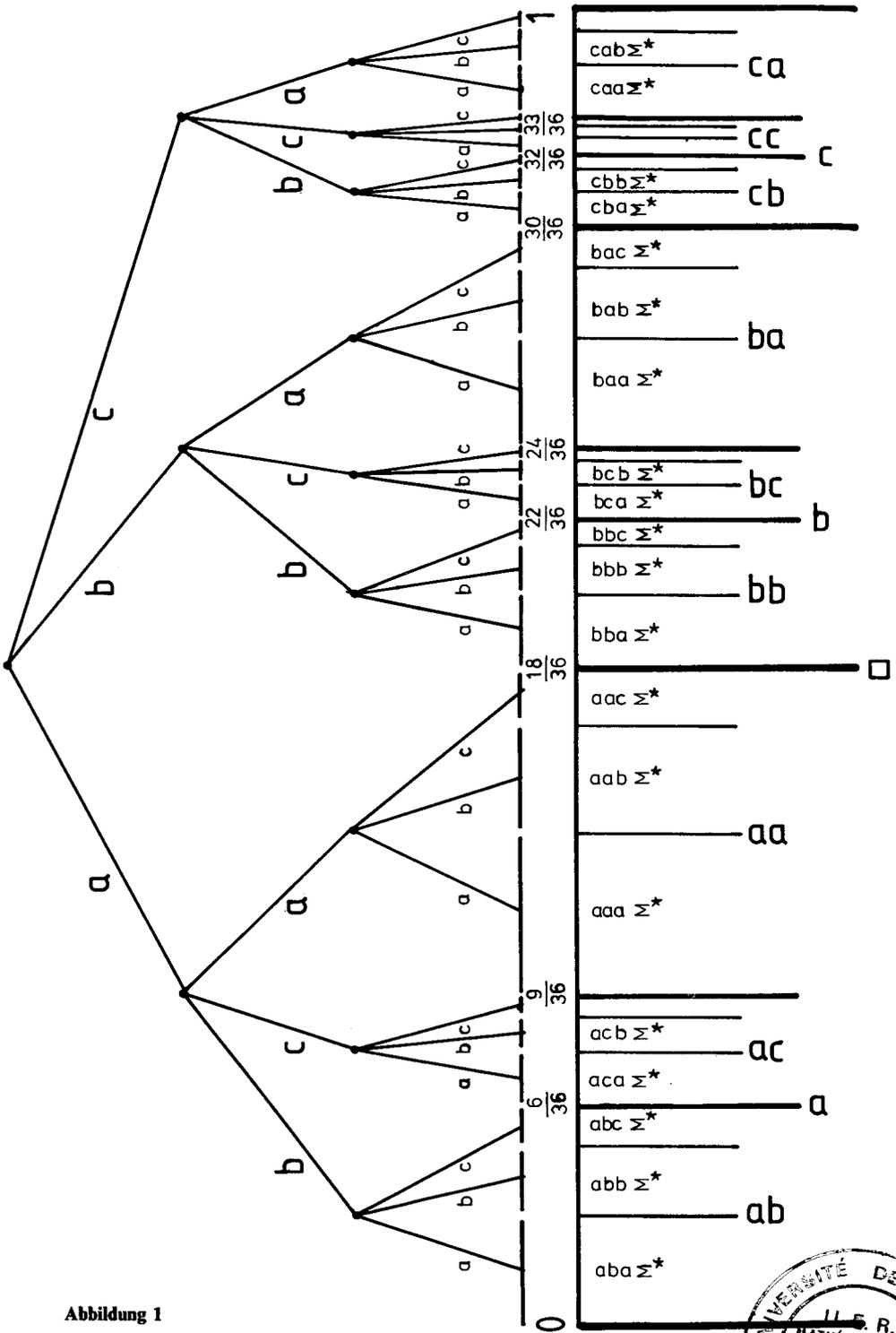
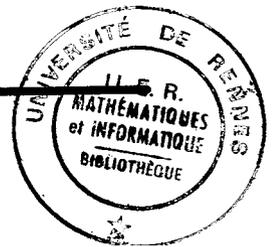


Abbildung 1



Beweis. — Mit \mathcal{G}_Q sei die durch E1-E3 definierte Funktionenklasse bezeichnet. Q sei nirgends schwach determiniert.

(a) Wir zeigen zunächst $\mathcal{F}_Q \subseteq \mathcal{G}_Q$: Nach 5(3) ist

$$\begin{aligned} \sup f_{\tau, \pi}(w \Sigma^*) - \inf f_{\tau, \pi}(w \Sigma^*) &= f_{\bar{n}, \pi}(w) - f_{\bar{0}, \pi}(w) \\ &= f_{\bar{0}, \pi}(w) + p(w) q_{\pi}(w, n) - f_{\bar{0}, \pi}(w) = \sum_{i=1}^n p(w a_{\pi}(w, i)) = p(w), \end{aligned}$$

und $f_{\tau, \pi}$ erfüllt E3. Hier wurde die Voraussetzung über Q benutzt. Nach Definition sind für disjunkte $v \Sigma^*$, $w \Sigma^*$ auch die Bildmengen $f_{\tau, \pi}(v \Sigma^*)$ und $f_{\tau, \pi}(w \Sigma^*)$ disjunkt bis auf eventuell die Randpunkte; daher gelten E1 und E2 (E1, E2 gelten für $f_{\tau, \pi}$ also auch ohne die Voraussetzung über Q).

(b) Es sei umgekehrt $f \in \mathcal{G}_Q$. Wir haben π, τ so zu bestimmen, dass:

$$f(w) = f_{\tau, \pi}(w)$$

für alle $w \in \Sigma^*$ gilt.

Sei $w \in \Sigma^*$. Wegen E1-E3 zerfällt die Menge $f(w \Sigma^*)$ in n bis auf die Randpunkte disjunkte, im Bild konvexe Stücke $f(w a_{\pi}(w, 1) \Sigma^*), \dots, f(w a_{\pi}(w, n) \Sigma^*)$. Es gibt also eine Permutation $\pi(w, \cdot)$ von \underline{n} , so dass

$$f(w a_{\pi}(w, 1) \Sigma^*) \leq f(w a_{\pi}(w, 2) \Sigma^*) \leq \dots \leq f(w a_{\pi}(w, n) \Sigma^*)$$

gilt. Dabei haben die Intervalle $\overline{\mathbf{O}}_{w a_{\pi}(w, j)}^f$ die Grösse:

$$l_{w, \pi}(w, j) = p(w a_{\pi}(w, j) \Sigma^{\omega}),$$

und wegen $\sum_{j=1}^n l_{w, \pi}(w, j) = p(w \Sigma^{\omega})$ gilt:

$$\begin{aligned} \inf f(w \Sigma^*) + m(w) q_{\pi}(w, i-1) &= \inf f(w \Sigma^*) + \sum_{j=1}^{i-1} l_{w, \pi}(w, j) = \inf f(w a_{\pi}(w, i) \Sigma^*) \\ &\leq \sup f(w a_{\pi}(w, i) \Sigma^*) = \inf f(w \Sigma^*) + \sum_{j=1}^i l_{w, \pi}(w, j) \\ &= \inf f(w \Sigma^*) + m(w) q_{\pi}(w, i). \end{aligned}$$

Mit Induktion nach der Länge von w beweist man

$$\inf f(w \Sigma^*) = f_{\bar{0}, \pi}(w).$$

Es ist also nur zu zeigen, dass

$$f(w) - \inf f(w \Sigma^*) = p(w \Sigma^*) q_{\pi}(w, \tau(w))$$

für eine geeignete Abbildung τ ist, d.h., dass $f(w)$ auf eine der Intervallgrenzen eines der Intervalle \mathbf{O}^f_{wa} , $a \in \Sigma$, fällt. Dies folgt aber aus E1 und E2. \square

Die Abbildungen $f_{\tau, \pi}$ sind im allgemeinen nicht injektiv. Wegen E4 treten Kollisionen jedoch mit Wahrscheinlichkeit O auf. Hinreichend für die Injektivität von $f_{\tau, \pi}$ sind die Bedingungen :

$$\tau(\Sigma^*) \subseteq \{1, \dots, n-1\}$$

und

$$p(u) > 0$$

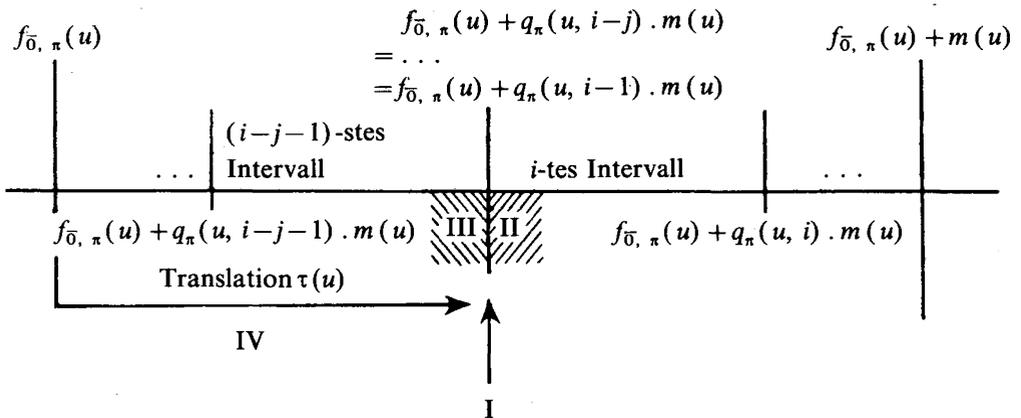
für alle $u \in \Sigma^*$.

Mit der rekursiven Definition der $f_{\tau, \pi} \in \mathcal{F}_Q$ wurde auch ein Codierungsalgorithmus für die $f_{\tau, \pi}$ angegeben. Wir beschreiben nun den naheliegenden Decodierungsalgorithmus. Die später durchzuführenden Aufwandsbetrachtungen [8] werden sich auf Realisierungen dieser Algorithmen beziehen (streng genommen, haben wir es mit Algorithmen zu tun, welche Orakel für das Rechnen mit reellen Zahlen und für die Funktionen τ , π und p benutzen) : Sei $f_{\tau, \pi}(uw)$ ein »Codewort« und $u \in \Sigma^*$ bereits entschlüsselt. Dann sind $m(u)$ und $f_{\bar{0}, \pi}(u)$ bekannt.

Ist $f_{\tau, \pi}(uw) - f_{\bar{0}, \pi}(u) \notin \{q_{\pi}(u, i) m(u) \mid 0 \leq i \leq n\}$, so wird der nächste Buchstabe entschlüsselt, wie folgt : Finde denjenigen Index i , so dass

$$q_{\pi}(u, i-1) < \frac{f_{\tau, \pi}(uw) - f_{\bar{0}, \pi}(u)}{m(u)} < q_{\pi}(u, i).$$

Es ist dann $w \in a_{\pi(u, i)} \Sigma^*$, also ein weiterer Buchstabe der Nachricht entziffert. Ist schliesslich $f_{\tau, \pi}(uw) - f_{\bar{0}, \pi}(u) = q_{\pi}(u, i-1) m(u)$ mit bei zusammenfallendem Intervallgrenzen maximal gewähltem i , so ist die Decodierung mit folgenden Ergebnis beendet :



Es seien $q_\pi(u, i-j) = q_\pi(u, i-j+1) = \dots = q_\pi(u, i-1)$ die Intervallgrenzen, die mit $q_\pi(u, i-1)$ zusammenfallen, also

$$p(ua_{\pi(u, i-j+1)}) = \dots = p(ua_{\pi(u, i-1)}) = 0.$$

Fall I. — Sofern $j \geq 2$, ist $w \in \{a_{\pi(u, i-j+1)}, \dots, a_{\pi(u, i-1)}\} \Sigma^*$ möglich.

Fall II. — Die gesendete Nachricht uw hat die Form

$$ua_{\pi(u, i)} a_{\pi(ua_{\pi(u, i)}, l_1)} \dots a_{(\dots, l_k)}$$

mit $q_\pi(\dots, l_1 - 1) = \dots = q_\pi(\dots, l_k - 1) = 0$,

so dass gilt $\tau(uw) = 0$ oder $p(uw) = 0$.

Fall III. — Die gesendete Nachricht uw hat die Form

$$ua_{\pi(u, i-j)} a_{\pi(ua_{\pi(u, i-j)}, l_1)} \dots a_{(\dots, l_k)}$$

mit $q_\pi(\dots, l_1) = \dots = q_\pi(\dots, l_k) = 1$,

so dass gilt $\tau(uw) = n$ oder $p(uw) = 0$.

Fall IV. — Sofern $i-j < \tau(u) \leq i$, bleibt noch die Möglichkeit $w = \square$.

Wie man sieht, ist für das Decodieren einer Nachricht vor allem die Kenntnis der Quellenstatistik p und des »Schlüssels« π wesentlich. Der Parameter τ spielt erst für den letzten Buchstaben der Nachricht bisweilen eine gewisse Rolle, so dass er für die Schlüsselmenge eines Kryptocodes kaum in Betracht kommt.

Da alle Codierungen $f_{\tau, \pi}$ gewissermassen aus der Codierung $f_{\bar{0}, e}$ durch Permutation der Intervalle (Parameter π) und Translation der Codeworte (Parameter τ) entstehen, lassen sich viele Eigenschaften von $f_{\tau, \pi}$ schon an $f_{\bar{0}, e}$ erkennen. $f_{\bar{0}, e}$ ist ausgezeichnet als diejenige Abbildung $f: \Sigma^* \rightarrow [0, 1]$ mit E1-E3, die anordnungstreu ist bezüglich der von $a_1 \leq a_2 \leq \dots \leq a_n$ induzierten alphabetischen Anordnung \leq auf Σ^* . Scherzhaft gesagt: Wir interessieren uns für die zunächst paradox scheinende Möglichkeit, Nachrichten zu verschlüsseln, indem man diese alphabetisch sortiert. Die ernsthaften Probleme ergeben sich, wie zu erwarten, durch die Syntax dieser Codierungen, sobald für die als Codewort auftretenden Zahlen eine Zahlendarstellung vereinbart werden soll, die effizientes Codieren und Decodieren gestattet.

ZUSAMMENFASSUNG

Mit den bisherigen Überlegungen wurde eine axiomatische Charakterisierung der arithmetischen Codes als redundanzfreier Codes geleistet. Der Vorschlag, sie zur Datenverschlüsselung einzusetzen wird dadurch motiviert, dass redundanzfreie Nachrichten in beliebig einfacher Weise verschlüsselt werden können [14], [9], ohne dass die Sicherheit gefährdet würde. Für die arithmetischen Codes bietet sich an, die Abbildungen π als Schlüssel zu verwenden. Theoretisch erreicht man damit absolute Sicherheit gegenüber jeder Form der Kryptanalyse; um genau zu sein, gilt dies nur asymptotisch, weil nur dann, wenn der so codierte Text sehr lang ist, die immer noch vorhandene Information über seine Länge keinen wesentlichen Aufschluss über den Text gibt. Die praktische Anwendung arithmetischer Codes steht und fällt mit dem Realisierungsaufwand. Diesen schätzen wir in [8] ab. Es zeigt sich, dass in Abhängigkeit von der jeweils gewählten Zahlendarstellung mit Wahrscheinlichkeit beliebig nahe an 1 der Aufwand an Zeit und Platz signifikant kleiner als derjenige für den ungünstigsten Fall ist.

LITERATUR

1. P. ANDELMAN, und J. REEDS, *On the Cryptanalysis of Rotor Machines and Substitution-Permutation Networks*, I.E.E.E. Trans. Information Theory IT-28, 1982, p. 578-584.
2. R. ASH, *Information Theory*, John Wiley & Sons, New York, 1965.
3. J. DUSKE und H. JÜRGENSEN, *Codierungstheorie*, Bi-Wissenschaftsverlag, Mannheim, 1977.
4. P. ELIAS, (*Unveröffentlicht*, vgl. [6]).
5. S. GUIAŞU, *Information Theory with Applications*, McGraw-Hill Book Co., New York, 1977.
6. F. JELINEK, *Probabilistic Information Theory*, McGraw-Hill Book Co., New York, 1968.
7. F. JELINEK und G. LONGO, *Algorithms for Source Coding*; in : G. LONGO (Hrsg.), *Coding and Complexity*, C.I.S.M. Courses and Lectures 216, Springer-Verlag, Wien, New York, 1975, p. 293-330.
8. H. JÜRGENSEN und M. KUNZE, *Über die Implementierung redundanzfreier Codes zur Datenverschlüsselung*, Erscheint in R.A.I.R.O.
9. H. JÜRGENSEN und D. MATTHEWS, *The Information Theoretic Analysis of Cryptosystems*, *Erscheint im Tagungsband von Crypto '83*, Santa Barbara, 1983.
10. R. C. PASCO, *Source Coding Algorithms for Fast Data Compression*, Ph. D. Thesis, Stanford University, CA, 1976.
11. F. RUBIN, *Cryptographic Aspects of Data Compression Codes*, *Cryptologia* 3, 1979, p. 202-205.

12. F. RUBIN, *Arithmetic Stream Coding Using Fixed Precision Registers*, I.E.E.E. Trans. Information Theory **IT-25**, 1979, p. 672-675.
13. N. RYSKA und S. HERDA, *Kryptographische Verfahren in der Datenverarbeitung*, Informatik Fachbereiche **24**, Springer-Verlag, Berlin, Heidelberg, New York, 1980.
14. C. E. SHANNON, *Communication Theory of Secrecy Systems*, Bell Syst. Techn. J. **28**, 1949, p. 656-715.