Die optisch codierte Karte: System- und Sicherheitsaspekte

DK: 351.755.6:535.2:535.411

H. Lienhard

In diesem Heft werden erste Produkte als Anwendungen der kohärenten Optik und der Landis & Gyr-Kartentechnologie vorgestellt: der PHONOCARD und das Zutritts-Kontrollsystem ID 2000. Hier sollen Systemkonzepte sowie auch einige informationstheoretische Überlegungen zur Sicherheit solcher Geräte und Anlagen dargelegt werden.

1. Allgemeines

Die erwähnten Produkte sind Beispiele von zwei unterschiedlichen Anwendungsbereichen mit verschiedenen Kartentypen: der *Wert-* oder *Geldersatzkarte* und der *Identifikationskarte* oder kurz *ID-Karte*.

Beide Karten enthalten eine bestimmte Anzahl von optisch codierten Einheiten, die im einen Fall *Werteinheiten*, welche konsumiert werden können, im anderen Fall *Informationseinheiten* repräsentieren. Im Grunde handelt es sich um zwei alte Bekannte: Die Entwertungskarte und den Ausweis (ID-Karte, Kreditkarte...). Da diese Dokumente nur von speziellen, autorisieten Stellen hergestellt resp. abgegeben werden dürfen, muss ihre Echtheit überprüfbar und schwer nachahmbar sein. Im Gegensatz zu den herkömmlichen Varianten interessieren hier nur solche Dokumente, die ausschliesslich von Maschinen akzeptiert und überprüft werden sollen. Wie komplex nun derartige Maschinen (sie werden hier Akzeptoren genannt) auch immer sein mögen, im Vergleich zum Menschen besitzen sie nur verschwindend kleine kognitive Fähigkeiten. Um trotzdem zu Systemen hoher Sicherheit zu gelangen, müssen spezielle Anforderungen an die Echtheitsmerkmale der Dokumente gestellt werden; *insbesondere aber müssen Dokument und Akzeptor genau aufeinander abgestimmt sein.*

Vom Akzeptor wird verlangt, dass er gute (echte) Dokumente möglichst fehlerfrei annimmt, daneben gefälschte mit hoher Wahrscheinlichkeit zurückweist; in vielen Anwendungen soll er auch noch billig sein.

2. W- und E-Systeme

Man unterscheidet zwei wesentlich verschiedene Systeme mit maschinenlesbaren Dokumenten:

W-System (rewriting system) – die Information kann vom Akzeptor geändert werden;

E-System (erasing system) – die Information kann im Akzeptor höchstens gelöscht werden.

Folglich können z.B. die Geldersatzkarten im Falle „W" mit neuen Werteinheiten aufgeladen werden; im Falle „E" dagegen werden diese physikalisch zerstört.

Ein relativ sicherer Akzeptor kann mit vernünftigem Aufwand dann realisiert werden, wenn beim Dokument Auswahl und Qualität der für den Akzeptor relevanten Parameter

- eine Nachahmung der *echten* Einheiten unwahrscheinlich machen, da technologisch schwierig resp. zu aufwendig;
- eine gute Diskrimination gegenüber den häufigsten Fälschungen ermöglichen (Ein Mass für die Diskrimination wird im Anhang zusammen mit möglichen Entscheidungsprozeduren eingeführt).

Soll nun der Akzeptor allgemein zugänglich sein, so kann dieser Forderung bei W-Systemen kaum nachgekommen werden: Erstens kommt „schwierige Technologie" zur Erzeugung dieser Einheiten in einem solchen Akzeptor schwerlich in Frage, zweitens genügt der Diebstahl eines solchen Gerätes, damit der Betrüger selbst solche Einheiten erzeugen kann. W-Systeme sind daher als *inhärent unsicher* zu betrachten (ein klassisches Beispiel: die Magnetkarte). Aus diesem Grund sind die Kartensysteme von Landis & Gyr als E-Systeme konzipiert worden.

3. System-Ebenen

Obwohl Geldersatz- und ID-Kartensysteme unterschiedlichen Zwecken dienen, können sie, rein technisch gesehen, zusammen behandelt werden. Wertkarten enthalten im allgemeinen zusätzlich zu den Werteinheiten auch gewisse ID-Information (z.B. Ausgabedatum); die ID-Karten werden durch

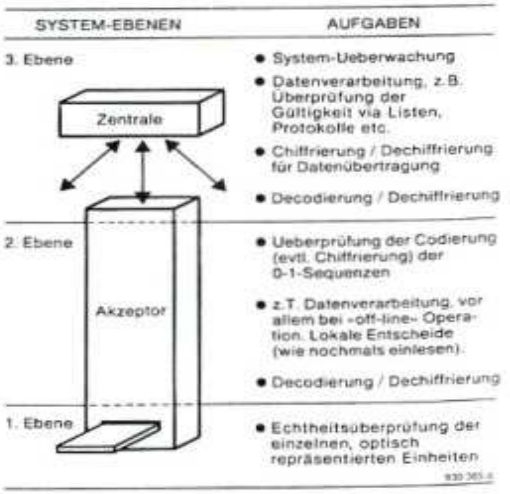
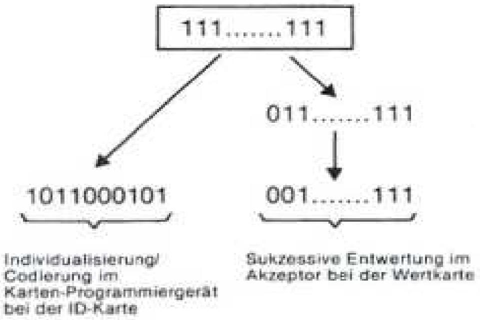


Bild 1 Logische Ebenen und ihre Aufgaben in einem Kartensystem

„Löschen" individualisert, allerdings geschieht dieses „Löschen" im Unterschied zur Entwertung bei der Wertkarte nicht im Akzeptor, sondern in einem (sicher aufbewahrten) speziellen Programmiergerät. Im folgenden werden eine noch gültige Werteinheit sowie eine binäre Eins mit „1" dargestellt; eine gelöschte Werteinheit oder binäre Null mit „0". Die noch unbenützte Wertkarte und die „blanko" ID-Karte enthalten beide eine Folge von „1", die dann durch Löschen verändert wird:



In einem Kartensystem lassen sich drei logische Ebenen, mit relativ loser Kopplung untereinander, erkennen (siehe *Bild 1*):

- Auf der *ersten Ebene* wird die Informations- (oder Wert-) Einheit verschlüsselt. Auf dieser Ebene wird die Einheit *physikalisch dargestellt*.

- Bereits auf der *zweiten Ebene* – der Code-Ebene – wird mit abstrakten Symbolen („0", „1") operiert. Sequenzen solcher Symbole werden zu Wörtern („bit-strings") zusammengefasst. Im Akzeptor wird auf dieser Ebene die Codierung, evtl. auch Chiffrierung (der Karte) überprüft.

- Die *dritte Ebene* umfasst die eigentliche Datenverarbeitung, wie Überprüfen von Sperrlisten, etc. Im Falle autonomer Leser erfolgt dies durch den im Akzeptor vorhandenen Mikrocomputer; bei ganzen Zutrittskontrollsystemen kann der Zentralrechner diese Aufgabe übernehmen.

4. Illegales Löschen

Auf der ersten Ebene wird die Echtheit der „1" und „0" überprüft. Während die Erzeugung echter „1" (des optisch codierten Musters) sehr schwierig und daher die Wahrscheinlichkeit der illegalen Erzeugung gering ist, dürfte illegales Löschen, d.h. die Erzeugung echter „0", wesentlich einfacher sein. Bei der Wertkarte wird durch ein illegales Löschen die Karte lediglich entwertet; bei der ID-Karte könnte aber versucht werden, die Information (z.B. ein Zutrittsrecht) durch Löschen zu verändern. Es existiert eine Unsymmetrie in der Sicherheit von „0" und „1". Durch entsprechende Codierung der Bit-Sequenz kann nun aber auf der 2. Ebene diese Unsymmetrie eliminiert werden. So wird z.B. eine Codierung verwendet, bei der legale Bit-Sequenzen immer eine feste Anzahl von „0" und „1" haben. Wird eine Karte eingelesen, so wird auf Ebene 2 sofort überprüft, ob die Anzahl „0" und „1" stimmt. Ein Beispiel: Die Binär-Sequenz umfasse 96 Bit; sie soll nur dann akzeptiert werden, wenn sie genau 48 „0" und 48 „1" enthält. Es gibt $\binom{96}{48}(\approx 6.4 \cdot 10^{27})$ solcher Sequenzen gegenüber 2^{96} ($\approx 8 \cdot 10^{28}$), wenn keine Einschränkungen gemacht würden. Beim „48 aus 96-Code" verliert man also nur etwa eine Dezimalstelle gegenüber der rein binären Codierung.

5. Chiffrierung

Wie oben (*Bild 1*) angedeutet, unterscheiden wir zwei Arten von Chiffrierung: die Kartenchiffrierung und die Chiffrierung für die Datenübertragung vom Akzeptor zur Zentrale. Im ersten Fall handelt es sich vor allem um den Schutz der Datenbank; im zweiten Fall um den Schutz der Datenübertragung. Kann die Übertragungsleitung unzugänglich gemacht werden, so entfällt die zweite Chiffrierung.

Mit der Kartenchiffrierung will man verhindern, dass Leute, die mit der Herstellung oder Inbetriebnahme eines solchen Systems zu tun haben, Kenntnisse über Datenbank (z.B. Liste der Zutrittsberechtigten) und Datenverarbeitung missbrauchen können. Man will also vermeiden, dass z.B. der Programmierer, der die Decodierung und Dechiffrierung kennt, zusammen mit Kenntnissen über legale Codes, in der Weise, in der sie in der Datenbank dargestellt sind, auf die eigentlichen Kartencodes schliessen kann. Dazu verwendet man z.B. sogenannte „trap-door one-way functions" [1]. *Bild 2* zeigt, wie eine gültige Karteninformation (KI) in der Datenbank gespeichert sein kann. Die Karte enthält nun nicht diese Information, sondern eine chiffrierte Form davon. Diese wird im (sicher aufbewahrten) Programmiergerät mit einer geheim gehaltenen speziellen Funktion f(·) erzeugt:

Kartencode KC' = f(KI)

Im Akzeptor, oder evtl. erst in der Zentraleinheit, wird auf KC' die inverse Funktion $f^{-1}(\cdot)$ angewandt. In einem Zutrittskontrollsystem z.B. wird nun geprüft, ob f^{-1}(KC') in der Liste der Zutrittsberechtigten enthalten ist. Die Funktion f ist so zu wählen, dass es ohne Kenntnis einer speziellen „trap-door"-Information praktisch unmöglich ist, von f^{-1} auf f zu schliessen. Damit nützt auch die Kenntnis der „Zutrittsliste" (oder "Sperrliste") nicht mehr viel.

Kann die Verbindungsleitung Akzeptor–Zentrale in einem Zutrittskontrollsystem ausserhalb des Sicherheitsbereiches angezapft werden, so kann illegaler Zutritt ohne eine Benützung des Akzeptors erhalten werden: Es genügt, eine erfolgreiche Signalsequenz (also eine, die zur Türöffnung führt) zu registrieren, um im geeigneten Zeitpunkt eine solche Sequenz direkt auf die Leitung zu geben. Ein komplizierter Dialog zwischen Akzeptor und Zentrale dürfte einen derartigen Eingriff erschweren, grundsätzlich ändert sich dabei die Situation nicht.

An eine Chiffrierung für die Datenübertragung muss daher die folgende Bedingung gestellt werden: Aus der Beobachtung von n Signal-Sequenzen S_i soll es praktisch ausgeschlossen sein, auf eine mögliche erfolgreiche Sequenz E_{n+1} zu schliessen:

$$S_1, S_2, \ldots S_n \not\mapsto E_{n+1}$$

Eine zeit- und datumabhängige Chiffrierung/Dechiffrierung kann dies im Prinzip gewährleisten [1].

Die zuerst erwähnte Kartenchiffrierung, bei der es vor allem um den Schutz des Systemträgers gegenüber dem Karten- und Akzeptorlieferanten geht, kann auf ganz verschiedene Weise realisiert werden. Eine interessante Möglichkeit bieten die bereits genannten „trap-door one-way functions". Hier kann die Dechiffrierung voll zugänglich gemacht werden, ohne dadurch das System zu gefährden. Wird dagegen eine klassische Blockchiffrierung [2] verwendet, so muss der Schlüssel K vom Systemträger geheim gehalten werden. Für die sichere Übertragung des Schlüssels zu den Akzeptoren kann eine spezielle „Schlüssel-

FIRMENCODE			123
IDENTIFIKATION			321654987
RAUMZONE			05
ZEITZONE			0
AUSGABENUMMER			0
PIN-ERZEUGUNG	ANZ. GEHEIM ZIFF.	0	
	ALGORITHMUS	6	

Bild 2 Karteninformation KI im Klartext für eine Zutrittskarte

930 366 d

Karte" dienen, mit der der Schlüssel in den Akzeptor eingelesen wird. In *Bild 3* ist ein möglicher Ablauf von Code-Umwandlungen in einem ID-System dargestellt.

6. Struktur des Akzeptors

In seiner Struktur ist der Akzeptor ein Steuer-, Regel- und Entscheidungssystem; *Bild 4* zeigt den allgemeinen Fall. Die eingeschobene Karte wird von den Quellen beleuchtet, das resultierende zurückgeworfene Licht wird von den Detektoren aufgefangen und in analoge elektrische Signale verwandelt, die dann von der Elektronik weiterverarbeitet werden. Die Sensorsignale $S_i(t)$ werden so auf einen Punkt eines mehrdimensionalen Entscheidungsraumes abgebildet, d.h. auf einen Vektor $\underline{Y}$ von digitalen Werten. Der eigentliche Entscheidungsalgorithmus ist im Mikrocomputer des Akzeptors programmiert (siehe auch Anhang). Ebenfalls im Mikrocomputer sind die Steuer- und Regelalgorithmen enthalten, mit denen Quellen, Löschvorgang und Transport gesteuert werden. Damit kann nun neben der Echtheit des optischen Musters, z.B. auch das Verhalten des Kartenmaterials beim löschen überprüft werden. Das gewählte Akzeptorkonzept bringt neben einer optimalen Sicherheit grosse Flexibilität.

7. Das Entscheidungsproblem

Die Entscheidungsverfahren müssen einerseits eine hohe Sicherheit gegenüber Betrugsversuchen bringen, andererseits sich einfach und effizent durch Mikrocomputer-Software verwirklichen lassen. Solche Entscheidungsprozeduren lassen sich mit Hilfe statistischer Methoden herleiten, wie sie ähnlich in Estimationstheorie und Hypothesentests verwendet werden. Wie oben erwähnt, werden durch eine elektronische Vorverarbeitung (durch einen Operator T_v) die Sensorsignale auf einen Vektor $\underline{Y}$ eines Entscheidungsraumes $\mathfrak{G}$ der Dimension N abgebildet. Insbesondere für $N>2$ wird es meist praktisch unmöglich, rein intuitiv zu einem guten Entscheidungsverfahren zu kommen. Im Anhang wird gezeigt, wie die Minimalisierung des durch Fehlentscheide erwarteten Risikos (das sogenannte Bayes-Risiko) zu einem optimalen Test führt (Gleichung (7)). Das Verfahren ist für eine Implementierung im Akzeptor zu unhandlich; es wird daher aus dem optimalen ein *suboptimaler,* aber strengerer Test hergeleitet, der zu einer einfachen Entscheidungsprozedur führt. Bei Annahme einer Gauss'schen Statistik wird durch dieses Verfahren der Entscheidungsraum $\mathfrak{G}$ durch Hyperebenen in drei Bereiche aufgeteilt: in Γ_0, Γ_1 und den Rest. Ist der Vektor $\underline{Y}$ in Γ_0, so wird für eine „0" entschieden, ist er in Γ_1 für eine „1". Ist er weder in Γ_0 noch Γ_1, so wird die Einheit nicht akzeptiert. Numerisch bedeutet das die Überprüfung einer Anzahl Ungleichungen der Form

$$\underline{\alpha}_{ik}^{T}\,\underline{Y} < D_{ki}$$

wobei $\underline{\alpha}_{ik}^{T}$ ein vorausberechneter Reihenvektor und D_{ki} eine vorausberechnete Konstante bedeuten (Gleichung (17) bis (19)). Zusammen mit dem Entscheidungsverfahren wird im Anhang auch ein Diskriminationsmass, die Diskriminations-Information, eingeführt. Dieses Mass erlaubt eine quantitative Beurteilung der Unterscheidbarkeit verschiedener Alternativen, z.B. der Unterscheidbarkeit der „1" gegenüber einer bestimmten Fälschung. Dieses Mass kann als Hilfsmittel für die Spezifikation der Dokumentparameter sowie den Akzeptordesign eingesetzt werden.

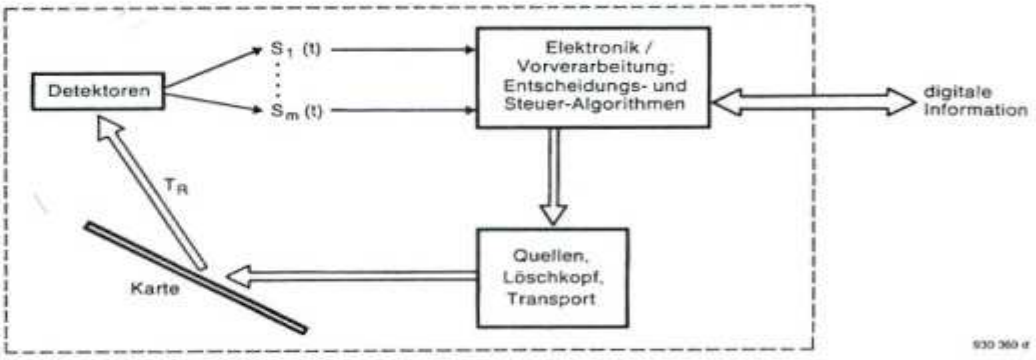


Bild 4 Struktur des Akzeptors

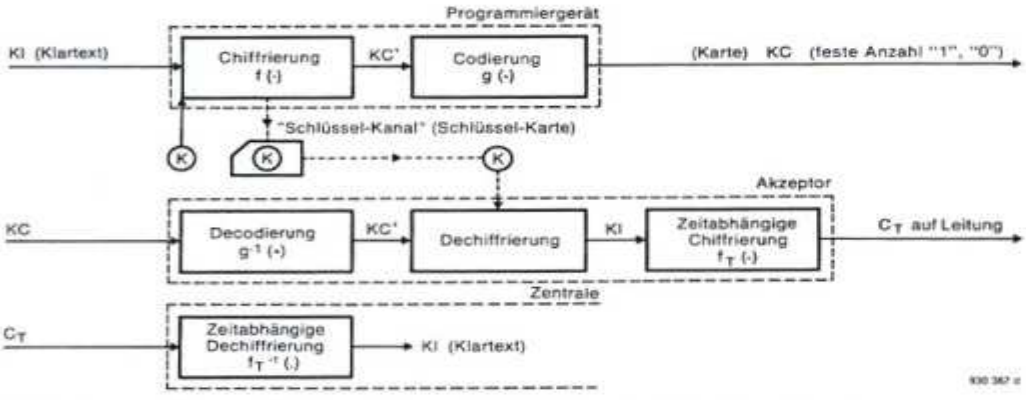


Bild 3a Kartenchiffrierung mittels Blockchiffrierung; Schlüssel K nur dem Systemträger bekannt

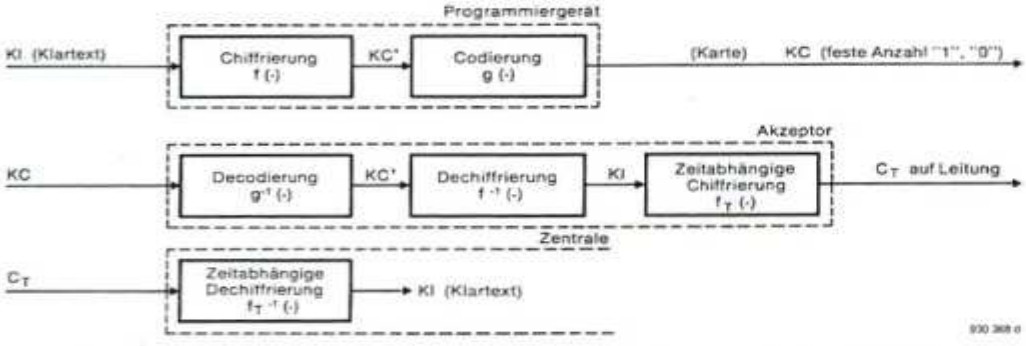


Bild 3b Kartenchiffrierung mit „trap-door one way function f"; f nur dem Systemträger bekannt; f^{-1} wird dem Akzeptorlieferant vom Systemträger bekanntgegeben.

8. Verbindung zum „Inversen Problem"

(vergl. Seite 7)

Bevor eine Entscheidungsprozedur angewandt wird, werden – wie oben er-

wähnt - die Messdaten mit einer Transformation T_v auf einen Vektor $\underline{Y}$ im Entscheidungsraum abgebildet. Ist das „Inverse Problem", abgekürzt IP, lösbar, d.h. kann z.B. aus Intensitätsmessungen des Fernfeldes auf den optischen Streuer geschlossen werden, so kann der *Darstellungsraum* des Streuers direkt als *Entscheidungsraum genommen* werden. Man beschränkt sich hier auf den parametrischen Fall: das Muster oder der Streuer lasse sich durch einen Parametervektor $\underline{Y}$ der Dimension N beschreiben. Die Abbildung

T_v^*: Messraum $\longrightarrow$ Entscheidungsraum (= Darstellungsraum)

wird nun aus der Lösung des „Inversen Problems" gewonnen. Für das im letzten Paragraphen erwähnte Entscheidungsverfahren braucht das IP nicht unbedingt lösbar zu sein. Dafür setzt man die Kenntnis der leicht herstellbaren Fälschungen a priori voraus. Es genügt in diesem Fall, sich gegen diese Fälschungen abzusichern; d.h. man braucht im Entscheidungsraum genügend „Distanz" zwischen den echten Mustern und den Fälschungen. Um diese „Distanz" quantitativ erfassen zu können, benützt man ein entsprechendes Diskriminationsmass.

Ist nun aber nichts über solche Fälschungen bekannt, so muss anders vorgegangen werden: man muss jetzt gewährleisten, dass Messdaten, die zu einem Entscheid „echt" führen, mit hoher Wahrscheinlichkeit nur von einem bestimmten (echten) Muster herrühren können. In diesem Falle soll das IP eine stabile, wenn möglich eindeutige, Lösung haben. Mehrdeutigkeit kann prinzipiell dann zugelassen werden, wenn jede der Lösungen, d.h. jedes der möglichen Muster nur schwer herstellbar ist. Werden die Messdaten auf einen Entscheidungsraum abgebildet, so sollte dabei keine Diskriminationsinformation verloren gehen. Mit Hilfe des Diskriminationsmasses können im Entscheidungsraum Umgebungen Γ_0 und Γ_1 für die Annahme der legalen Muster „0" und „1" definiert werden; dabei werden die Umgebungen so eng gewählt, dass die verlangte minimale Annahmequote echter Einheiten gerade noch erfüllt wird [3]. Die Forderung der Lösbarkeit des IP bedingt entsprechend umfangreiche Messdaten; das Verfahren ist nur praktikabel, wenn der damit verbundene Messaufwand vertretbar ist.

Im Akzeptor wird der passive Streuer beleuchtet, wodurch Signale in einem Messraum $\mathfrak{M}$ erzeugt werden; man nennt das die Lesetransformation T_R *(Bild 4)*. Bezeichnet man den Darstellungsraum der Streuer (oder Muster) mit $\mathfrak{D}$ und die Entscheidungsfunktion mit Γ, so kann der ganze Akzeptionsvorgang wie in *Bild 5* schematisch dargestellt werden.

9. Systemabgrenzung

Es sind zwei Entscheidungsverfahren erwähnt worden:
Im einen wird Kenntnis der gefährlichen Fälschungen vorausgesetzt, im andern nicht. In Wirklichkeit sind meist gewisse Fälschungen bekannt. So geht es bei einem System wie PHONOCARD (siehe Seite 40) nicht nur darum, sich gegen eigentliche Fälschungen zu schützen, sondern man muss sich auch gegen andere Systeme abgrenzen. Die Karten des einen Landes sollen natürlich nicht im PHONOCARD-Akzeptor eines anderen Landes angenommen werden. Um eine sichere Trennung der verschiedenen Systeme zu erhalten, werden die Einheiten (die „1" bei den Wertkarten) in jedem System wieder anders dargestellt. Systemfremde Karten müssen vom Akzeptor wie Fälschungen mit grosser Sicherheit zurückgewiesen werden können.

10. Anhang: Entscheidungsverfahren und Diskrimination

Es wird hier versucht, über statistische Methoden zu rationalen Entscheidungsverfahren zu gelangen. Bei höheren Dimensionen (N) des Entscheidungsraumes kommt man mit intuitiven Überlegungen nicht mehr durch. Zuerst wird ein in gewissem Sinne optimaler Test abgeleitet. Aus diesem wird ein suboptimaler, aber strengerer Test entwickelt, der sich im Akzeptor besser implementieren lässt.

Wie in *Bild 6* dargestellt, werden die rohen Sensorsignale (Vektor $\underline{S}$ (t)) erst aufgearbeitet und in einen Vektor (oder Punkt) eines Entscheidungsraumes $\mathfrak{E}$ der Dimension N transformiert:

Transformation

$$T_v: [\underline{S}(t), 0 \le t \le T] \longrightarrow \underline{Y} \qquad (1)$$
$$\underline{Y} \in \mathfrak{E}$$

wobei [0, T] das Beobachtungsintervall darstellt.

Obwohl im folgenden ausschliesslich das Entscheidungsproblem behandelt wird, sei zur Vorverarbeitung, d.h. zur Transformation $T_v(\cdot)$ bemerkt:

- wie gezeigt wird, spielt im Entscheidungsalgorithmus die *Diskriminationsinformation* I(i:j) zwischen verschiedenen Hypothesen H_i und H_j eine zentrale Rolle. Idealerweise sollte durch die Transformation $T_v(\cdot)$ diese Information I nicht verkleinert werden; nach Kullback [3] wäre dann $\underline{Y}$ eine „sufficient statistic" für die Diskriminierung.
- Im Normalfall wird die Entscheidungsprozedur D (siehe *Bild 6*) in Mikrocomputer-Software realisiert; demgegenüber verlangt die Vorverarbeitung meist noch anspruchsvolle Analogelektronik.

10.1 Der optimale Test

Im Raum $\mathfrak{E}$ sollen - in einem gewissen Sinn optimale - Untermengen Γ_i definiert werden, so dass aus

$\underline{Y} \in \Gamma_j$ mit grosser Sicherheit auf die Hypothese H_j geschlossen werden kann.

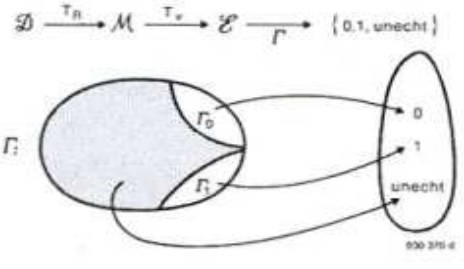


Bild 5 Lese- und Prüfvorgang im Akzeptor

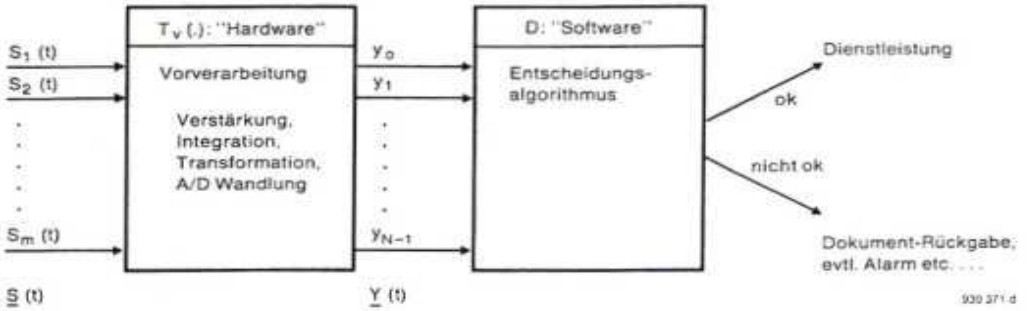


Bild 6 Struktur der Signalverarbeitung im Akzeptor

Dazu wird das „Bayes'sche Risiko" eingeführt (siehe z.B. [4]), das man zu minimalisieren versucht.

Mit E[ ] = math. Erwartung und Prob( ), oder P( ) = Wahrscheinlichkeit, kann dieses Risiko (d.h. die zu erwartenden Kosten) wie folgt geschrieben werden:

$$E\,|\text{Kosten}| = \sum_{i=0}^{M-1}\sum_{j=0}^{M-1} c_{ij}\ \text{Prob}\,(\text{Entscheid für } H_j, \text{ in Wirklichkeit } H_i)$$

$$= \sum_{i,j} c_{ij} \cdot P\,(\underline{Y} \in \Gamma_j \text{ und } H_i)\ ; \qquad (2)$$

c_{ij} = Kostenfaktoren.

Dabei werden insgesamt M verschiedene Hypothesen betrachtet.

Der Klarheit halber soll das Problem noch etwas weiter konkretisiert werden:

Die Hypothesen H_0 und H_1 sollen *legitime Alternativen* repräsentieren (z.B. „0" oder „1" bei einer Zutritts- oder Kreditkarte) während H_2 ... H_{M-1} Fälschungen darstellen sollen. Dabei kann mit zunehmender Erfahrung M später erhöht werden, was lediglich zu einer Änderung der Akzeptor-Software führt.

Theoretisch gibt es natürlich unzählige vorstellbare falsche Alternativen. Die Praxis zeigt aber, dass nur die mit relativ geringem Aufwand herstellbaren Falsifikate dem System wirklich gefährlich werden können. In diesem Sinne sollen die H_2 ... H_{M-1}, die (M-2) gefährlichsten Alternativen darstellen. Entsprechend werden nun die *Kostenfaktoren* c_{ij} in (2) gewählt:

$c_{ii} = 0$:
Kein Verlust bei korrektem Entscheid

$c_{ij} = 0$, für i, j ≥ 2:
Kein Verlust beim Verwechseln verschiedener falscher Muster

$c_{ij} \ll c_{ji}$, für i = 0,1; j ≥ 2.
Man setzt $c_{ij} = \underline{c}$; $c_{ji} = \overline{c}$
d.h. niedriger Kostenfaktor, wenn gutes Muster refusiert wird; dagegen hohe Kosten, wenn falsches Muster akzeptiert wird.

$c_{01} = c_{10} = \underline{c}$
Niedriger Kostenfaktor für Verwechslung von 0 und 1.

oder in Matrix-Form:

$$\left[\begin{array}{c|c} \begin{matrix} 0 & \underline{c} \\ \underline{c} & 0 \end{matrix} & \begin{matrix} \underline{c}\ \underline{c} \ \ldots\ldots\ldots\ldots\ \underline{c}\ \underline{c} \\ \underline{c}\ \underline{c} \ \ldots\ldots\ldots\ldots\ \underline{c}\ \underline{c} \end{matrix} \\ \hline \begin{matrix} \overline{c}\ \overline{c} \\ \overline{c}\ \overline{c} \\ \vdots\ \vdots \\ \vdots\ \vdots \\ \vdots\ \vdots \\ \vdots\ \vdots \\ \vdots\ \vdots \\ \overline{c}\ \overline{c} \end{matrix} & 0 \end{array}\right] = [c_{ij}]$$

Durch Einführen bedingter Wahrscheinlichkeitsdichten $p\,(\underline{y} \mid H_i)$ kann für (2) geschrieben werden

$$E\,|\text{Kosten}| = \sum_{i,j}\int_{\Gamma_j} c_{ij}\,P(H_i)\,p\,(\underline{y} \mid H_i)\,d\underline{y}$$

$$= \sum_{j}\int_{\Gamma_j}\sum_{i} c_{ij}\,P(H_i)\,p\,(\underline{y} \mid H_i)\,d\underline{y} \qquad (3)$$

Um das Risiko zu minimalisieren, werden die Untermengen Γ_j nun so gewählt, dass die Integranden in (3) möglichst klein werden:

$$\underline{Y} \in \Gamma_j \longleftrightarrow \text{alle } k \neq j\text{:}$$

$$\sum_i c_{ij} P(H_i)\,p(\underline{y}|H_i) < \sum_i c_{ik} P(H_i)\,p(\underline{y}|H_i) \qquad (4)$$

Für die a priori-Wahrscheinlichkeiten $P(H_i)$ setzt man:

$$P(H_0) = P(H_1) = p \qquad (5)$$

Wie erwähnt, sollen die Hypothesen mit i ≥ M nur noch verschwindende Wahrscheinlichkeit haben. Dann gilt:

$$\sum_{i=2}^{M-1} P(H_i) = 1 - 2p \qquad (6)$$

Aus Gleichungen (4), (5) und den Annahmen über die Koeffizienten c_{ij} folgt:

$$\underline{Y} \in \Gamma_0 \longleftrightarrow \left\{ \begin{array}{l} p(\underline{y} \mid H_1) < p\,(\underline{y} \mid H_0) \\ \displaystyle\sum_{i=2}^{M-1} P(H_i)\,\frac{p(\underline{y} \mid H_i)}{p(\underline{y} \mid H_0)} < (\underline{c}/\overline{c})p \end{array} \right\}$$

$$\underline{Y} \in \Gamma_1 \longleftrightarrow \left\{ \begin{array}{l} p(\underline{y} \mid H_0) < p\,(\underline{y} \mid H_1) \\ \displaystyle\sum_{i=2}^{M-1} P(H_i)\,\frac{p(\underline{y}|H_i)}{p(\underline{y} \mid H_1)} < (\underline{c}/\overline{c})p \end{array} \right\}$$

sonst ⟶ nicht akzeptiert. (7)

10.2 Der suboptimale Test

Einen einfacheren, strengeren Test erhält man mit (8):

$$\underline{y} \in \Gamma_0 \longleftrightarrow \left\{ \begin{array}{l} p(\underline{y} \mid H_1) < p(\underline{y} \mid H_0) \\ i \geq 2 : \dfrac{p(\underline{y} \mid H_i)}{p(\underline{y} \mid H_0)} < \gamma_i \end{array} \right\}$$

$$\underline{y} \in \Gamma_1 \longleftrightarrow \left\{ \begin{array}{l} p(\underline{y} \mid H_0) < p(\underline{y} \mid H_1) \\ i \geq 2 : \dfrac{p(\underline{y} \mid H_i)}{p(\underline{y} \mid H_1)} < \gamma_i \end{array} \right\}$$

— sonst nicht akzeptiert. (8)

$$\text{mit } \gamma_i = (\underline{c}\,/\,\overline{c}) \cdot \frac{p}{(M\text{-}2)\,P(H_i)}\ ;\ (i \geq 2)$$

$$\text{oder } \gamma i = (\underline{c}\,/\,\overline{c})\ \frac{p}{1-2p}\ ;$$

$$\text{wenn } P(H_i) = \frac{1-2p}{M\text{-}2}\ ;\ (i \geq 2) \qquad (9)$$

(d.h. Falsifikate haben gleiche Wahrscheinlichkeit).
Setzt man $\gamma_0 = \gamma_1 = 1$ und definiert:

$$L_{Ki} = \log \frac{p(\underline{y} \mid H_k)}{p(\underline{y} \mid H_i)} = \log \frac{p_k\,(\underline{y})}{p_i(\underline{y})}\ ;$$

$$p_i(\underline{y}) = p(\underline{y} \mid H_i) \qquad (10)$$

dann kann man statt (8) schreiben:

$$\underline{y} \in \Gamma_0 \longleftrightarrow L_{oi} > \log \gamma_i^{-1} \text{ für } i \neq 0.$$
$$y \in \Gamma_1 \longleftrightarrow L_{1i} > \log \gamma_i^{-1} \text{ für } i \neq 1. \qquad (11)$$

Es wird nun die folgende Grösse definiert:

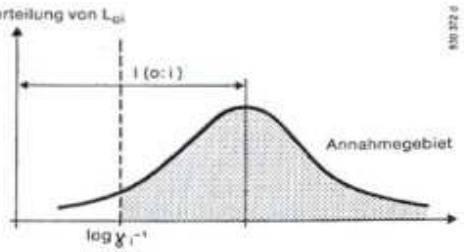
$$I(0:i) = E\,|L_{oi} \mid H_o| =$$

$$\int p_o\,(\underline{y})\,\log \frac{p_o(\underline{y})}{p_i(\underline{y})}\,d\underline{y}$$

$$(= I(p_o : p_i)) \qquad (12)$$

I(0:i) wird als die *Diskriminations-Information* der Hypothese H_o gegen die Hypothese H_i bezeichnet.

In *Bild 7* ist angedeutet, wie die Akzeptionsrate (d.h. Entscheid für H_o, wenn H_o gegeben) durch die Diskriminations-Information beeinflusst wird. Vor



Annahme:

$p(\underline{y} \mid H_0) = n(r_0, \sigma^2)$; d.h. normalverteilt mit Mittelwert r_0 und Varianz σ^2
$p(\underline{y} \mid H_i) = n(r_i, \sigma^2)$

und setzt man

$$\Phi(a) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{a} e^{-\frac{1}{2}t^2}\,dt, \text{ dann wird}$$

$$P\{L_{oi} > \log \gamma_i^{-1} \mid H_o\} = \Phi\sqrt{\tfrac{1}{2}} - \frac{\log \gamma_i^{-1}}{\sqrt{2I}}$$

$$I = I(o:i) = E\{L_{oi} \mid H_o\}$$

Bild 7: Einfluss von I(o:i)

allem bei grossen log γ_i^{-1} (z.B. bei relativ grosser Betrugswahrscheinlichkeit) braucht man ein entsprechend grösseres I(o:i) für eine vernünftige Annahmerate.

10.3 Die Dikriminations-Information

Sie ist eine Verallgemeinerung der „mutual information" von Shannon.

Aus der Ungleichheit von Jensen (z.B. [5]) folgt sofort:

$$I(p:q) \geq o \qquad (13)$$

mit $I = o \longleftrightarrow p = q$ (mit Wahrscheinlichkeit 1 bei verallgemeinerten Dichten p, q).

Ebenfalls gilt für statistisch unabhängige Merkmale $(y_1, y_2, \ldots y_N)$:

$$I(k:i;y_1, y_2, \ldots y_N) = \sum_{l=1}^{N} I(k:i;y_l) \qquad (14)$$

(Faktorisierung der Dichten $p_k(y_1, \ldots y_N)$; $p_i()$).

Die Diskriminations-Information ist *invariant* unter nicht singulären Transformationen [3]:

$$\underline{X} = T(\underline{Y}) \longrightarrow I(k:i;\underline{X}) = I(k:i;\underline{Y}) \qquad (15)$$

Aus (13) bis (15) folgt, dass nach einer entsprechenden Transformation (Rotation) der Vektoren $\underline{Y}$, $(I(k:i))^{1/2}$ als eine *geometrische Distanz* zwischen den Hypothesen H_i und H_k gedeutet werden kann.

Das wird besonders transparent im Fall von Normal-Verteilungen mit identischer Kovarianz:

Es seien $p_i(\underline{y}) = n(\underline{r}_i, \underline{\underline{\Pi}})$ (16)

d.h. Normal-Verteilungen mit Mittelwert $\underline{r}_i$ und der Einheitsmatrix als Kovarianzmatrix.

Aus (8) resp. (11) folgt sofort:

$$\underline{\alpha}_{ik}^T (\underline{y} - \underline{r}_k) < d_{ki}$$

$$\text{mit } \underline{\alpha}_{ik}^T = (\underline{r}_i - \underline{r}_k)^T / (2\, I(k:i))^{1/2} \qquad (17)$$

$$\sqrt{2}\, d_{ki} = (I(k:i))^{1/2} - \log \gamma_i^{-1} / (I(k:i))^{1/2}$$

wobei jetzt $2\, I(k:i) = (\underline{r}_k - \underline{r}_i)^T (\underline{r}_k - \underline{r}_i) = \| \underline{r}_k - \underline{r}_i \|^2$

mit $\| \underline{r}_k - \underline{r}_i \|$: Euklid'sche Vektordistanz.

Die Ungleichung in (17) sagt nichts anderes aus, als dass die *Projektion* des Vektors $(\underline{y} - \underline{r}_k)$ auf Vektor $(\underline{r}_i - \underline{r}_k)$ kleiner als d_{ki} sein muss;
in einem zweidimensionalen Beispiel:

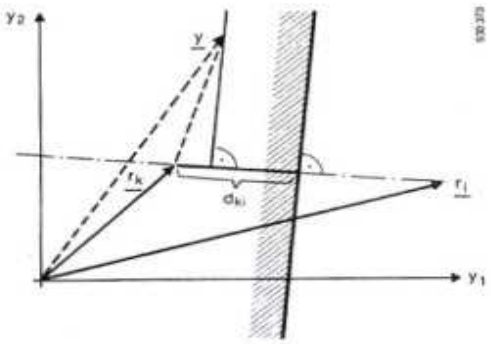


Bild 8 Zweidimensionales Beispiel für die Entscheidungsprozedur (17)

d.h. $\underline{y}$ muss sicher im durch Schraffur markierten Halbraum liegen. Im N-dimensionalen Raum wird die Annahmemenge durch Hyperebenen eingegrenzt. Dies gilt allgemein für Wahrscheinlichkeitsverteilungen, die zur „exponentiellen" Familie gehören, also für viele der praktisch wichtigen Verteilungen wie Normalverteilung, Poisson etc. Setzt man statt (16) Normalverteilungen mit einer Kovarianzmatrix Σ voraus, so erhält man an Stelle von (17):

$$\underline{\beta}_{ik}^T (\underline{y} - \underline{r}_k) < d_{ki} \qquad (18)$$

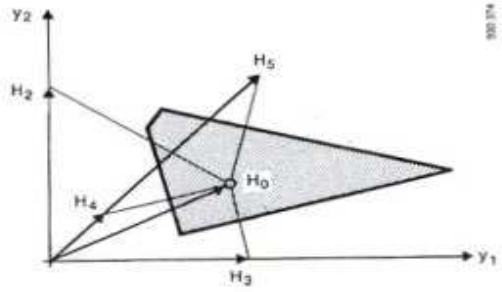


Bild 9 Beispiel mit nur einer zulässigen Hypothese H_0
Entscheidungsraum für H_0
Abgrenzung gegen H_2, H_3, H_4, H_5

$$\text{mit } \underline{\beta}_{ik}^T = (\underline{r}_i - \underline{r}_k)^T \Sigma^{-1} / (2\, I(k:i))^{1/2}$$

$$\text{und } 2\, I(k:i) = (\underline{r}_i - \underline{r}_k)^T \Sigma^{-1} (\underline{r}_i - \underline{r}_k) \qquad (19)$$

Die Diskriminations-Information ist also in diesem Fall gegeben durch die relative Lage der Vektoren $\underline{r}_i$, $\underline{r}_k$ und die Streumatrix Σ.

In *Bild 9* ist der vereinfachte (auf 2 Dimensionen reduzierte) Fall eines Entscheidungsraumes dargestellt. Die gefährlichsten Fälle sind hier:

- Nur ein Merkmal berücksichtigt (Hypothesen H_2, H_3)
- gleiche, kleine Werte in Y_1 und Y_2 (H_4)
- gleiche, maximale Werte in Y_1 und Y_2 (H_5)

Alle γ_i sind in diesem Fall gleich 1 gesetzt worden; d.h. das Kostenverhältnis in (9) wird dem Verhältnis Betrugswahrscheinlichkeit / $P(H_o)$ gleichgesetzt. Das ist nur dann sinnvoll, wenn schon diese Betrugsfälle kleine Wahrscheinlichkeit haben.

Bild 10 illustriert noch den Fall einer 0/1-Detektion.

10.4 Design-Kriterien

Sind alle anderen Parameter fixiert, so wird durch Variation von $(\underline{c}/\overline{c})$ die Annahme-Wahrscheinlichkeit gegenüber der „power of rejection" verändert:

durch eine Verkleinerung von $(\underline{c}/\overline{c})$ wird die Annahmerate verkleinert, dafür wird der Test schärfer gegenüber Fälschungen. In der Praxis muss man eine Anzahl Fälle durchrechnen, um zu einem vernünftigen Kompromiss zu gelangen.

Die Wahrscheinlichkeitsverhältnisse $\frac{p}{(M\text{-}2)P(H_i)}$ (siehe (9)) sind in Wirklichkeit völlig unbekannt. Man wird hier, abhängig von der verwendeten Technologie, einen „intelligent guess" vornehmen müssen.

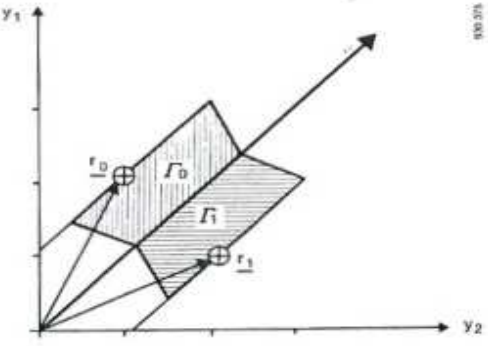


Bild 10 Beispiel einer 0/1-Detektion
$y \in \Gamma_0 \rightarrow$ "0" $\quad y \in \Gamma_1 \rightarrow$ "1"
sonst: Falsifikat

Die *Diskriminations-Information* hängt nicht nur vom Design des Akzeptors, sondern auch von der *Beschaffenheit des Dokumentes ab:* weist das Dokument eine grosse Streuung in den zu prüfenden Parametern auf, so wird diese Information entsprechend klein (siehe (19)). Wie gut ein Akzeptor (bei endlichen Kosten!) überhaupt ausgelegt werden kann, hängt stark von der Produktionsqualität der zu prüfenden Dokumente ab.

Zusammenfassend kann festgehalten werden:

Auswahl und *Qualität* der Dokumentparameter sollten

1. zu *kleinen Nachahm-Wahrscheinlichkeiten* führen (schwierige Technologie);

2. eine *grosse Diskriminations-Information* gegenüber den häufigsten Falsifikaten bringen.

11. Bibliographie

[1] Diffie, W., Hellman, M.E.: New directions in cryptography; IEEE Transactions on Information Theory, Vol IT-22, No. 6, Nov. 1976.

[2] Feistel, H.; Notz, W.A., Smith, D.L.: Some cryptographic techniques for machine-to-machine data communications. Proceedings of the IEEE, Vol. 63, No. 11, Nov. 1975.

[3] Kullback, S. Information Theory and Statistic (1959), Dover, 1968.

[4] Fukunaga, K. Introduction to Statistical Pattern Recognition, Academic Press NY, 1972.

[5] Feller, W. An Introduction to Probability Theory and its Applications; Vol. II. John Wiley, 1966.

[6] Rivert, R.L.: Shavric, A.: Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems.

Autor: Heinz Lienhard
LGZ Landis & Gyr Zug AG
CH-6301 Zug (Schweiz)