# IT-Sicherheit mit Assoziativmatrizen

H.-J. Bentz (*), J. Braun (&), A. Dierks (*), U. Dobbratz (*), O. Festerling (*), M. Glockemann (*), G. Palm (§), M. Miyamoto (#), D. Romberger (#), F. Rosenschein (*), J. Weber (#)
[* imbit.net, # Hochschule Hannover, & Ludwig–Maximilians–Universität München, § Universität Ulm]

**Der Einsatz einer besonderen Art von Assoziativmatrizen erlaubt ein informationstechnisch sicheres Ablegen und Übertragen von Daten.[1] Die durchzuführenden Matrixoperationen werden durch elektronische Schaltungen unterstützt, die in einem eigens dafür entwickelten Baustein untergebracht sind. Für unterschiedliche Anwendungsfelder entstanden Gerätemodelle, die hinsichtlich der Matrixgröße skalierbar und bezüglich der Sicherheitserfordernisse erweiterbar sind.**

## Inhalt



## Einordnung

Gegenstand unserer Untersuchungen sind die Eigenschaften und Anwendungsgebiete von Matrizen, deren Einträge nur aus Nullen und Einsen bestehen. Die Verteilung dieser Nullen und Einsen kann durch Lernregeln bestimmt werden, wie sie bei Palm [1982], Steinbuch [1965] oder Bentz and Dierks [2013] beschrieben sind.[2] Diese Matrizen dienen der Mustererkennung, -vervollständigung oder -extraktion, dem Assoziativen Rechnen oder der Assoziativen Programmierung durch ihre Fähigkeit, mit Fragen mittels der von ihnen gelernten Frage–Antwort–Paare tolerant Antworten zu assoziieren.[3] Daher nennt man diese Matrizen *Assoziativmatrizen*. Ihr Zusammenwirken in komplexeren Strukturen führt zu robusten, frei programmierbaren *Assoziativmaschinen*.[4]

Im Folgenden geht es jedoch um Eigenschaften von Assoziativmatrizen, bei denen das Eintragen der Nullen und Einsen **nicht** per Lernregel und durch vorgegebene Frage–Antwort–Paare, sondern **zufällig** erfolgt, und deren Zeilen- und Spaltenanzahl $n$ gleich groß ist, also um $n \times n$–Matrizen. Das liefert einen informationstechnischen Nutzen, der hier unser zentrales Anliegen ist.

Der ursprüngliche Ansatz, Assoziativmatrizen zur Modellierung synaptischer Verbindungen von waagerecht und senkrecht angeordneten Neuronen zu nutzen, wird durch die herkömmlichen Lernregeln deutlich.[5] Mit dem im Folgenden vorgestellten *Lernen durch den Zufall*, verlassen wir das Anwendungsgebiet der künstlichen neuronalen Netze, in welchem es um das Trainieren und Erkennen von Mustern geht.[6]

Die nachstehende Abb. 1 veranschaulicht, wie eine Matrix zur Beschreibung der Lage von Verbindungsstellen eingesetzt werden kann. Beide Darstellungen geben das gleiche Verbindungsmuster wieder. Die linke Darstellung ist in einem schaltungstechnischen, die rechte in einem mathematischen Umfeld nützlich.

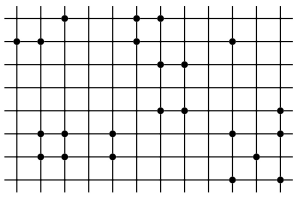

Abb. 1: Die Verbindungen zwischen waage- und senkrecht verlaufenden Neuronen sind als Punkte markiert.

$$\begin{pmatrix} 0&0&1&0&0&1&1&0&0&0&0&0 \\ 1&1&0&0&0&1&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0&1 \\ 0&1&1&0&1&0&0&0&0&1&0&1 \\ 0&1&1&0&1&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&1&0&1 \end{pmatrix}$$

Abb. 2: Die Orte, an denen Zeilen und Spalten verbunden sind, werden in der Matrix als 1 notiert, die anderen als 0.

Nunmehr lassen wir den Zufall oder einen Zufallsgenerator die Verbindungsstellen zwischen Zeilen und Spalten bestimmen. Füllt man alle Spalten einer $n \times n$–Matrix, in der vorher nur Nullen stehen (*Nullmatrix*), zufällig mit Einsen, bis eine vorgegebene Anzahl $p$ an Einsen erreicht ist, mit $p \leq n$, nennt man diese Matrix *spaltenstarr* (siehe Abb. 3). Füllt man alle Zeilen einer $n \times n$–Matrix zufällig mit p Einsen, nennt man sie *zeilenstarr*. Werden in die Spalten **und** Zeilen einer Matrix zufällig jeweils eine feste Anzahl Einsen eingetragen, heißt sie *doppeltstarr* (siehe Abb. 4). Verteilt man eine feste Anzahl p von Einsen zufällig in einer $n \times n$–Matrix, wird sie *$p$–dicht* genannt, mit $p \leq n^2$. Man beachte, dass es einen Unterschied gibt zu Matrizen, in denen auf $p$ zufälligen Positionen Einsen verteilt werden, denn das kann zu weniger als $p$ Einsen in der Matrix führen.

$$\begin{pmatrix} 0&0&1&0&1&1&0&0 \\ 1&1&1&0&0&1&1&0 \\ 1&0&1&1&0&0&1&1 \\ 0&1&1&0&0&1&0&0 \\ 0&0&0&1&0&0&1&1 \\ 1&1&0&1&1&1&0&1 \\ 0&1&0&1&1&0&1&1 \\ 1&0&0&0&1&0&0&0 \end{pmatrix}$$

Abb. 3: Eine spaltenstarre $8 \times 8$–Matrix mit $p = \frac{1}{2}n$

$$\begin{pmatrix} 1&1&0&1&0&0&1&0 \\ 0&0&0&0&1&1&1&1 \\ 0&1&1&1&0&1&0&0 \\ 1&1&1&0&0&0&1&0 \\ 0&0&1&1&0&0&1&1 \\ 1&0&0&0&1&1&0&1 \\ 1&1&0&0&1&1&0&0 \\ 0&0&1&1&1&0&0&1 \end{pmatrix}$$

Abb. 4: Eine doppeltstarre $8 \times 8$–Matrix mit $p = \frac{1}{2}n$