Die Lineare Algebra-Methode

Mahir Kilic

24. Juni 2004

Überblick

- Wo wird diese Methode benutzt?

Überblick

- Wo wird diese Methode benutzt?
- Für die Bestimmung einer Obergrenze für die Mächtigkeit einer Menge

Überblick

- Wo wird diese Methode benutzt?
- Für die Bestimmung einer Obergrenze für die Mächtigkeit einer Menge
- Anwendung mit dem Fisher's Satz

Überblick

- Wo wird diese Methode benutzt?
- Für die Bestimmung einer Obergrenze für die Mächtigkeit einer Menge
- Anwendung mit dem Fisher's Satz
- Für die Feststellung der Gleicheit zweier Vektoren

Überblick

- Wo wird diese Methode benutzt?
- Für die Bestimmung einer Obergrenze für die Mächtigkeit einer Menge
- Anwendung mit dem Fisher's Satz
- Für die Feststellung der Gleicheit zweier Vektoren
- Anwendung mit dem Flipping Card Games

Lineare Algebra

- Einige Kentnisse der Lineare Algebra notwendig. Deswegen ein paar Definitionen:

Lineare Algebra

- Einige Kentnisse der Lineare Algebra notwendig. Deswegen ein paar Definitionen:
- **Ein Vektorraum** V über den Körper **F** ist $\mathbf{F}^n$, wobei $v \in \mathbf{F}^n$ die Form $v = (v_1, \ldots, v_n)$ mit $v_i \in \mathbf{F}$ hat.

Lineare Algebra

- Einige Kentnisse der Lineare Algebra notwendig. Deswegen ein paar Definitionen:
- **Ein Vektorraum** V über den Körper **F** ist $\mathbf{F}^n$, wobei $v \in \mathbf{F}^n$ die Form $v = (v_1, \ldots, v_n)$ mit $v_i \in \mathbf{F}$ hat.
- mit zwei grundlegenden Operationen:
  Komponentenweise Addition: $u + v = (u_1 + v_1, \ldots, u_n + v_n)$
  Multiplikation mit einem Skalar: $\lambda v = (\lambda v_1, \ldots, \lambda v_n), \lambda \in \mathbf{F}$.

Lineare Algebra

- Einige Kentnisse der Lineare Algebra notwendig. Deswegen ein paar Definitionen:
- **Ein Vektorraum** V über den Körper **F** ist $\mathbf{F}^n$, wobei $v \in \mathbf{F}^n$ die Form $v = (v_1, \ldots, v_n)$ mit $v_i \in \mathbf{F}$ hat.
- mit zwei grundlegenden Operationen:
  Komponentenweise Addition: $u + v = (u_1 + v_1, \ldots, u_n + v_n)$
  Multiplikation mit einem Skalar: $\lambda v = (\lambda v_1, \ldots, \lambda v_n), \lambda \in \mathbf{F}$.
- **Eine Linearkombination** von Vektoren $v_1, \ldots, v_m$ ist ein Vektor der Form $\lambda_1 v_1 + \ldots + \lambda_m v_m$ mit $\lambda_i \in \mathbf{F}$.

Lineare Algebra

- **Ein Untervektorraum** von V ist eine unter Linearekombination abgeschlossene nicht leere Untermenge von V.

Lineare Algebra

- **Ein Untervektorraum** von V ist eine unter Linearekombination abgeschlossene nicht leere Untermenge von V.
- **Lineare Hülle** von $v_1, \ldots, v_m$ ist die Menge aller Linearkombinationen von $v_1, \ldots, v_m$. $(span\{v_1, \ldots, v_m\})$

Lineare Algebra

- **Ein Untervektorraum** von V ist eine unter Linearekombination abgeschlossene nicht leere Untermenge von V.
- **Lineare Hülle** von $v_1, \ldots, v_m$ ist die Menge aller Linearkombinationen von $v_1, \ldots, v_m$. $(span\{v_1, \ldots, v_m\})$
- Ein Vektor u ist **linear abhängig** von den Vektoren $v_1, \ldots, v_m$, wenn $u \in span\{v_1, \ldots, v_m\}$.

Lineare Algebra

- **Ein Untervektorraum** von V ist eine unter Linearekombination abgeschlossene nicht leere Untermenge von V.
- **Lineare Hülle** von $v_1, \ldots, v_m$ ist die Menge aller Linearkombinationen von $v_1, \ldots, v_m$. $(span\{v_1, \ldots, v_m\})$
- Ein Vektor u ist **linear abhängig** von den Vektoren $v_1, \ldots, v_m$, wenn $u \in span\{v_1, \ldots, v_m\}$.
- Andernfalls ist u von $v_1, \ldots, v_m$ unabhängig.

Lineare Algebra

- Eine **Basis** $B = \{v_1, \ldots, v_m\}$ von V ist eine Menge von unabhängigen Vektoren, welche V erzeugen.

Lineare Algebra

- Eine **Basis** $B = \{v_1, \ldots, v_m\}$ von V ist eine Menge von unabhängigen Vektoren, welche V erzeugen.
- Jede Basis von V hat die gleiche Kardinalität. Das ist die **Dimension** von V.

Lineare Algebra

- Eine **Basis** $B = \{v_1, \ldots, v_m\}$ von V ist eine Menge von unabhängigen Vektoren, welche V erzeugen.
- Jede Basis von V hat die gleiche Kardinalität. Das ist die **Dimension** von V.
- **Behauptung 1:** Wenn $(v_1, \ldots, v_k)$ linear unabhängige Vektoren in einem Vektorraum mit Dimension m sind, dann gilt $k \leq m$.

Lineare Algebra

- **Das Skalarprodukt** von zwei Vektoren $\langle u, v \rangle$ ist so definiert: $\langle u, v \rangle = u \cdot v := u_1 v_1 + \ldots + u_n v_n$.

Lineare Algebra

- **Das Skalarprodukt** von zwei Vektoren $\langle u, v \rangle$ ist so definiert: $\langle u, v \rangle = u \cdot v := u_1 v_1 + \ldots + u_n v_n$.
- Die Norm eines Vektors v=$(v_1, \ldots, v_n)$ ist

$$\| v \| := \langle v, v \rangle^{1/2} = \left(\sum_{i=1}^{n} v_i^2 \right)^{1/2}.$$

Lineare Algebra

- **Das Skalarprodukt** von zwei Vektoren $\langle u, v \rangle$ ist so definiert: $\langle u, v \rangle = u \cdot v := u_1 v_1 + \ldots + u_n v_n$.
- Die Norm eines Vektors v=$(v_1, \ldots, v_n)$ ist

$$\| v \| := \langle v, v \rangle^{1/2} = \left(\sum_{i=1}^{n} v_i^2 \right)^{1/2}.$$

- **Cauchy-Schwarz-Ungleichung:**
  Für Vektoren $u, v \in \mathrm{R}^n$ gilt $\langle u, v \rangle \leq \| u \| . \| v \|$.
  Das heisst:

$$\left(\sum_{i=1}^{n} v_i u_i \right)^2 \leq \left(\sum_{i=1}^{n} v_i^2 \right) \left(\sum_{i=1}^{n} u_i^2 \right).$$

Übersicht

- Ziel: Bestimmung einer Obergrenze für die Mächtigkeit einer Menge

Übersicht

- Ziel: Bestimmung einer Obergrenze für die Mächtigkeit einer Menge
- Die Elemente der Mengen werden als Vektoren dargestellt.

Übersicht

- Ziel: Bestimmung einer Obergrenze für die Mächtigkeit einer Menge
- Die Elemente der Mengen werden als Vektoren dargestellt.
- Nun werden Methoden der Lineare Algebra benutzt.

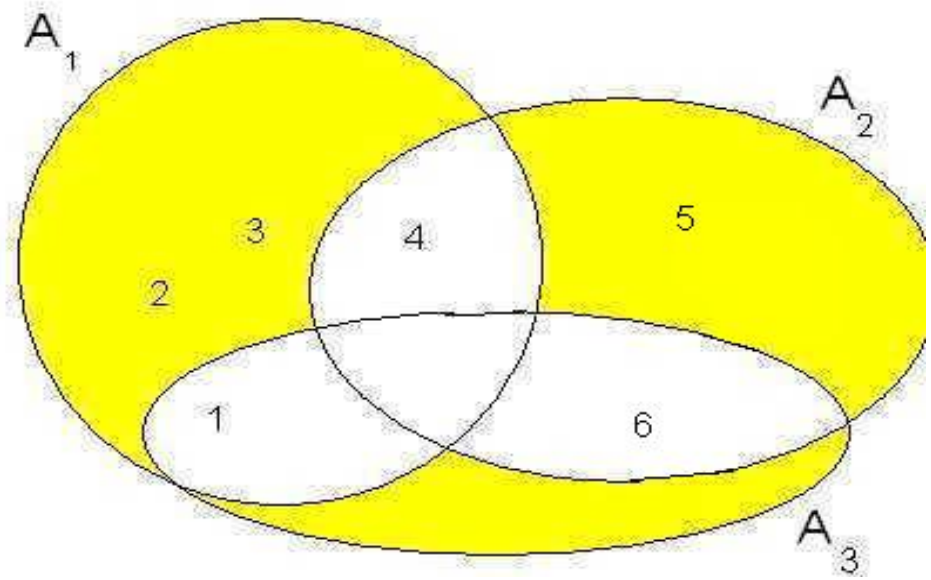
Fisher's Ungleichung

- Gegeben ist eine Familie von Mengen (F), die bestimmte Bedingungen erfüllen. Wir möchten wissen, wie viele Mengen so eine Familie haben kann.

Fisher's Ungleichung

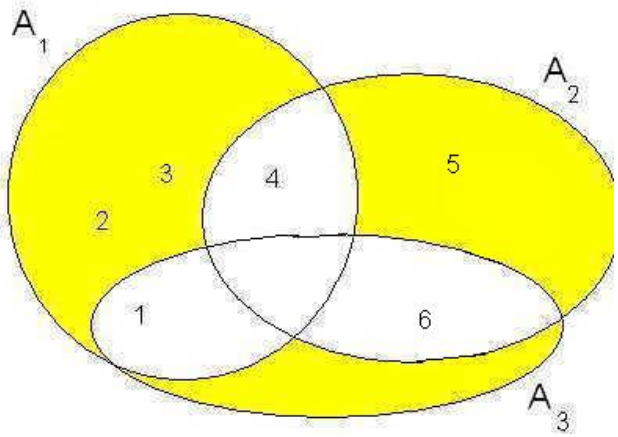
- Gegeben ist eine Familie von Mengen (F), die bestimmte Bedingungen erfüllen. Wir möchten wissen, wie viele Mengen so eine Familie haben kann.
- **Satz.** Seien $A_1, \ldots, A_m$ Untermengen von $\{1, \ldots, n\}$ und es gelte $|A_i \cap A_j| = k$ für eine k mit $1 \leq k \leq n$ für alle $i \neq j$. Dann ist $m \leq n$.

Fisher's Ungleichung



Satz. Seien $A_1, \ldots, A_m$ Untermengen von $\{1, \ldots, n\}$ und es gilt $|A_i \cap A_j| = k$ für eine $1 \leq k \leq n$ für alle $i \neq j$.
Dann ist $m \leq n$.

Fisher's Ungleichung



$$V_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad V_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad V_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Beweis von Fisher's Satz

- Seien $V_1, \ldots, V_m \in \{0,1\}^n$ Inzidenzvektoren von $A_1, \ldots, A_m$.

Beweis von Fisher's Satz

- Seien $V_1, \ldots, V_m \in \{0,1\}^n$ Inzidenzvektoren von $A_1, \ldots, A_m$.
- Wegen Behauptung 1 reicht es aus zu zeigen, dass diese Vektoren über R linear unabhängig sind.

Beweis von Fisher's Satz

- Seien $V_1, \ldots, V_m \in \{0,1\}^n$ Inzidenzvektoren von $A_1, \ldots, A_m$.
- Wegen Behauptung 1 reicht es aus zu zeigen, dass diese Vektoren über R linear unabhängig sind.
- **Erinnerung :** Behauptung 1: Wenn $(v_1, \ldots, v_k)$ linear unabhängige Vektoren in einem Vektorraum mit Dimension m sind, dann gilt $k \leq m$.

Beweis von Fisher's Satz

- Seien $V_1, \ldots, V_m \in \{0,1\}^n$ Inzidenzvektoren von $A_1, \ldots, A_m$.
- Wegen Behauptung 1 reicht es aus zu zeigen, dass diese Vektoren über R linear unabhängig sind.
- **Erinnerung :** Behauptung 1: Wenn $(v_1, \ldots, v_k)$ linear unabhängige Vektoren in einem Vektorraum mit Dimension m sind, dann gilt $k \leq m$.
- Beweis von linearer Unabhängigkeit durch Widerspruch

Beweis von Fisher's Satz

- Seien $V_1, \ldots, V_m \in \{0,1\}^n$ Inzidenzvektoren von $A_1, \ldots, A_m$.
- Wegen Behauptung 1 reicht es aus zu zeigen, dass diese Vektoren über R linear unabhängig sind.
- **Erinnerung :** Behauptung 1: Wenn $(v_1, \ldots, v_k)$ linear unabhängige Vektoren in einem Vektorraum mit Dimension m sind, dann gilt $k \leq m$.
- Beweis von linearer Unabhängigkeit durch Widerspruch
- Angenommen die Gleichung $\sum_{i=1}^{m} \lambda_i v_i = 0$ hat eine nicht triviale Lösung.

Beweis von Fisher's Satz

- Seien $V_1, \ldots, V_m \in \{0,1\}^n$ Inzidenzvektoren von $A_1, \ldots, A_m$.
- Wegen Behauptung 1 reicht es aus zu zeigen, dass diese Vektoren über R linear unabhängig sind.
- **Erinnerung :** Behauptung 1: Wenn $(v_1, \ldots, v_k)$ linear unabhängige Vektoren in einem Vektorraum mit Dimension m sind, dann gilt $k \leq m$.
- Beweis von linearer Unabhängigkeit durch Widerspruch
- Angenommen die Gleichung $\sum_{i=1}^{m} \lambda_i v_i = 0$ hat eine nicht triviale Lösung.
- Offensichtlich ist $\langle v_i, v_i \rangle = |A_i|$ und $\langle v_i, v_j \rangle = k$, wenn $i \neq j$ ist.

Beweis von Fisher's Satz

- $0 = (\sum_{i=1}^{m} \lambda_i v_i)(\sum_{j=1}^{m} \lambda_j v_j)$

Beweis von Fisher's Satz

- $0 = (\sum_{i=1}^{m} \lambda_i v_i)(\sum_{j=1}^{m} \lambda_j v_j)$
- $= \sum_{i=1}^{m} \lambda_i^2 \langle v_i, v_i \rangle + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j \langle v_i, v_j \rangle$

Beweis von Fisher's Satz

- $0 = (\sum_{i=1}^{m} \lambda_i v_i)(\sum_{j=1}^{m} \lambda_j v_j)$
- $= \sum_{i=1}^{m} \lambda_i^2 \langle v_i, v_i \rangle + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j \langle v_i, v_j \rangle$
- $= \sum_{i=1}^{m} \lambda_i^2 |A_i| + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j k$

Beweis von Fisher's Satz

- $0 = (\sum_{i=1}^{m} \lambda_i v_i)(\sum_{j=1}^{m} \lambda_j v_j)$
- $= \sum_{i=1}^{m} \lambda_i^2 \langle v_i, v_i \rangle + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j \langle v_i, v_j \rangle$
- $= \sum_{i=1}^{m} \lambda_i^2 |A_i| + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j k$
- $= \sum_{i=1}^{m} \lambda_i^2 (|A_i| - k) + k \cdot (\sum_{i=1}^{m} \lambda_i)^2$

Beweis von Fisher's Satz

- $0 = (\sum_{i=1}^{m} \lambda_i v_i)(\sum_{j=1}^{m} \lambda_j v_j)$
- $= \sum_{i=1}^{m} \lambda_i^2 \langle v_i, v_i \rangle + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j \langle v_i, v_j \rangle$
- $= \sum_{i=1}^{m} \lambda_i^2 |A_i| + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j k$
- $= \sum_{i=1}^{m} \lambda_i^2 (|A_i| - k) + k \cdot (\sum_{i=1}^{m} \lambda_i)^2$
- Klar ist $|A_i| \geq k$ für alle i. Hierbei gilt $|A_i| = k$ für maximal ein i.

Beweis von Fisher's Satz

- $0 = (\sum_{i=1}^{m} \lambda_i v_i)(\sum_{j=1}^{m} \lambda_j v_j)$
- $= \sum_{i=1}^{m} \lambda_i^2 \langle v_i, v_i \rangle + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j \langle v_i, v_j \rangle$
- $= \sum_{i=1}^{m} \lambda_i^2 |A_i| + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j k$
- $= \sum_{i=1}^{m} \lambda_i^2 (|A_i| - k) + k \cdot (\sum_{i=1}^{m} \lambda_i)^2$
- Klar ist $|A_i| \geq k$ für alle i. Hierbei gilt $|A_i| = k$ für maximal ein i.
- Hieraus folgt,dass rechte Seite grösser als 0 ist. Widerspruch

Übersicht

- **Ziel:** Gleichheit zweier Vektoren entscheiden.

Übersicht

- **Ziel:** Gleichheit zweier Vektoren entscheiden.
- Das Spiel wird erklärt.

Übersicht

- **Ziel:** Gleichheit zweier Vektoren entscheiden.
- Das Spiel wird erklärt.
- Unterschiedliche Lösungswege werden dargestellt.

Flipping Card Game

- Wir haben zwei Vektoren aus $\mathbf{F}_2^n$ $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ mit Länge n.

Flipping Card Game

- Wir haben zwei Vektoren aus $\mathbf{F}_2^n$ $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ mit Länge n.
- Wir möchten entscheiden, ob $u = v$ ist.

Flipping Card Game

- Wir haben zwei Vektoren aus $\mathbf{F}_2^n$ $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ mit Länge n.
- Wir möchten entscheiden, ob $u = v$ ist.
- Aber unser Zugriff zu den Bits ist eingeschränkt.

Flipping Card Game

- Wir haben zwei Vektoren aus $\mathbf{F}_2^n$ $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ mit Länge n.
- Wir möchten entscheiden, ob $u = v$ ist.
- Aber unser Zugriff zu den Bits ist eingeschränkt.
- Zu jedem Zeitpunkt können wir zu jedem Index i entweder u_i oder v_i sehen.

Flipping Card Game

- Wir können uns das so vorstellen, dass die Bits auf beiden Seiten von n Karten aufgetragen sind.

Flipping Card Game

- Wir können uns das so vorstellen, dass die Bits auf beiden Seiten von n Karten aufgetragen sind.
- Die Karten liegen auf dem Tisch.

Flipping Card Game

- Wir können uns das so vorstellen, dass die Bits auf beiden Seiten von n Karten aufgetragen sind.
- Die Karten liegen auf dem Tisch.
- Wir können nur eine Seite jede Karte sehen.

Flipping Card Game

- Wir können uns das so vorstellen, dass die Bits auf beiden Seiten von n Karten aufgetragen sind.
- Die Karten liegen auf dem Tisch.
- Wir können nur eine Seite jede Karte sehen.
- Ein Schritt besteht aus einer Drehung von einer oder mehreren Karten.

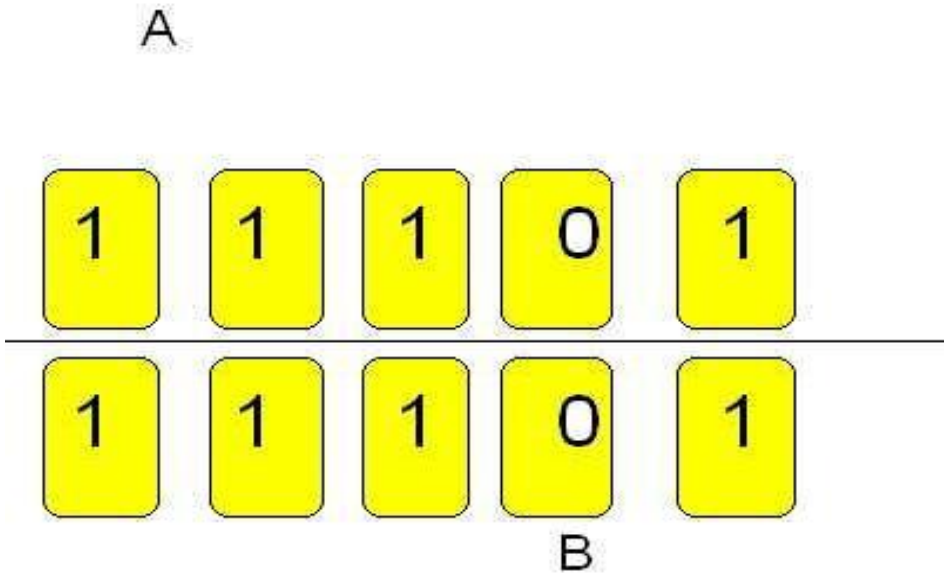
Flipping Card Game

- Wir können uns das so vorstellen, dass die Bits auf beiden Seiten von n Karten aufgetragen sind.
- Die Karten liegen auf dem Tisch.
- Wir können nur eine Seite jede Karte sehen.
- Ein Schritt besteht aus einer Drehung von einer oder mehreren Karten.
- Nach jedem Schritt können wir Informationen speichern, aber Speicher ist nicht wiederverwendbar. Die alte Informationen kann man immer benutzen.

Flipping Card Game

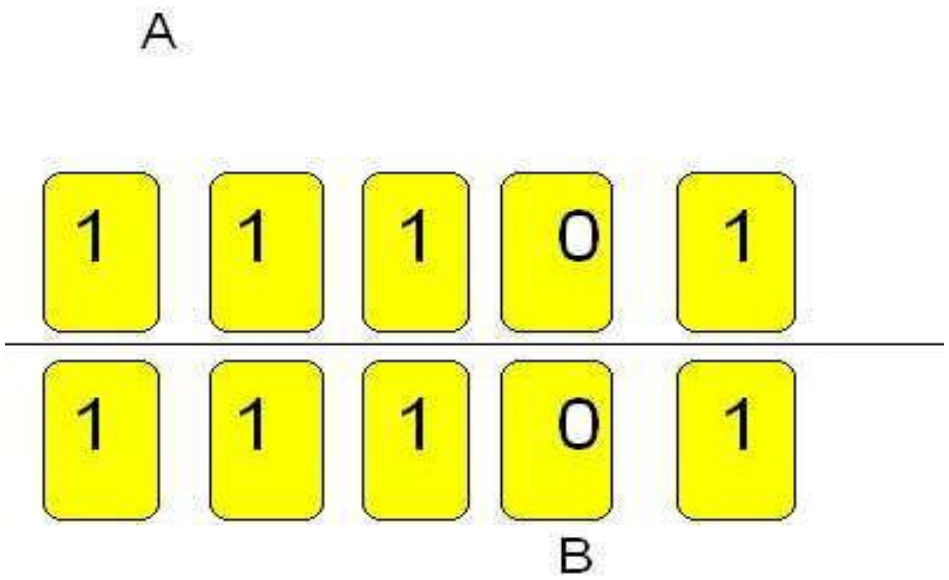
- Wir können uns das so vorstellen, dass die Bits auf beiden Seiten von n Karten aufgetragen sind.
- Die Karten liegen auf dem Tisch.
- Wir können nur eine Seite jede Karte sehen.
- Ein Schritt besteht aus einer Drehung von einer oder mehreren Karten.
- Nach jedem Schritt können wir Informationen speichern, aber Speicher ist nicht wiederverwendbar. Die alte Informationen kann man immer benutzen.
- Das Ziel ist es, mit möglichst wenig Speicherverbrauch zu entscheiden, ob die beiden Seiten der Karten gleich sind.

erster Ansatz



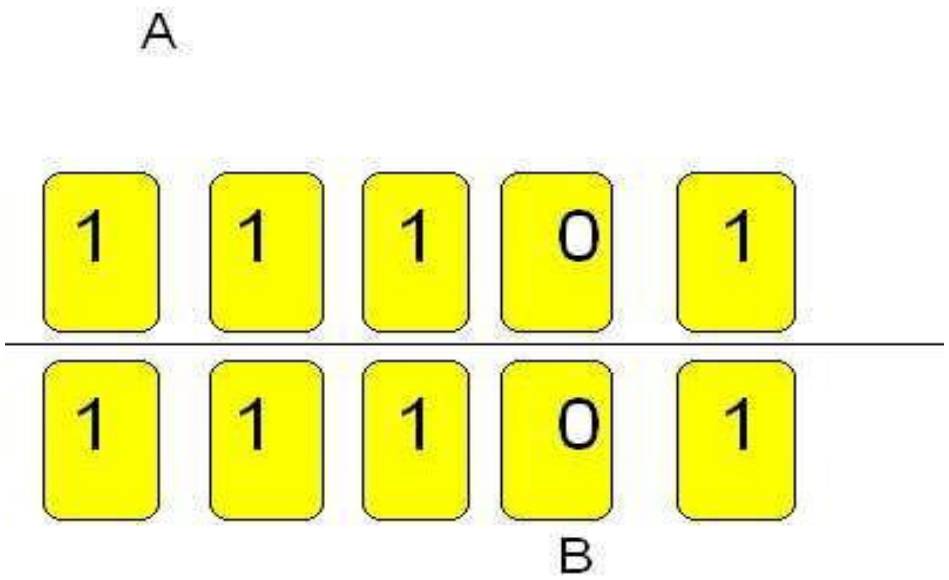
- Mit Speicherkapazität von n bits: Lösung trivial

erster Ansatz



- Mit Speicherkapazität von n bits: Lösung trivial
- Schreibe v einfach in den Speicher und drehe alle Karten um.

erster Ansatz



- Mit Speicherkapazität von n bits: Lösung trivial
- Schreibe v einfach in den Speicher und drehe alle Karten um.
- Kann man das besser machen?

zweiter Ansatz

Satz. Sei $n = r^2$ für eine $r \geq 1$. Man kann die Gleichheit von zwei Vektoren aus $\{0,1\}^n$ mit r+1 Scritten bestimmen,ohne mehr als r Bits zu schreiben

Beweis

- Teile die gegebene Vektoren u und v in r Teile der Länge r. $u = (u^1, \ldots, u^r)$ und $v = (v^1, \ldots, v^r)$.

Beweis

- Teile die gegebene Vektoren u und v in r Teile der Länge r. $u = (u^1, \ldots, u^r)$ und $v = (v^1, \ldots, v^r)$.
- erster Schritt: öffne den Vektor u an und rechne den Vektor $w_0 := u^1 + u^2 + \ldots + u^r$ über $\mathbf{F_2}$ aus.

Beweis

- Teile die gegebene Vektoren u und v in r Teile der Länge r. $u = (u^1, \ldots, u^r)$ und $v = (v^1, \ldots, v^r)$.
- erster Schritt: öffne den Vektor u an und rechne den Vektor $w_0 := u^1 + u^2 + \ldots + u^r$ über $\mathbf{F_2}$ aus.
- Diesen Vektor w_0 schreiben wir in den Speicher(Benutzung von r bits), und dann machen wir r Schritt wie folgt:

Beweis

- Teile die gegebene Vektoren u und v in r Teile der Länge r. $u = (u^1, \ldots, u^r)$ und $v = (v^1, \ldots, v^r)$.
- erster Schritt: öffne den Vektor u an und rechne den Vektor $w_0 := u^1 + u^2 + \ldots + u^r$ über $\mathbf{F_2}$ aus.
- Diesen Vektor w_0 schreiben wir in den Speicher(Benutzung von r bits), und dann machen wir r Schritt wie folgt:
- i'ter Versuch: drehe nur die Karte, die im v^i sind und rechne den Vektor
  $w_i := u^1 + \ldots + u^{i-1} + v^i + u^{i+1} + \ldots + u^r$ aus.

Beweis

- Jetzt kontrollieren wir, ob $w_i = w_0 \quad \forall i$ ist. Wenn $w_i = w_0 \quad \forall i$ ist, sind u und v gleich.

Beweis

- Jetzt kontrollieren wir, ob $w_i = w_0 \quad \forall i$ ist. Wenn $w_i = w_0 \quad \forall i$ ist, sind u und v gleich.
- Wenn die Antwort $u = v$ ist, heisst das, dass nach der ersten Schritt gilt: $u^1 + u^2 + \ldots + u^r = v^1 + u^2 + \ldots + u^r$. Daraus folgt $u^1 = v^1$.

Beweis

- Jetzt kontrollieren wir, ob $w_i = w_0 \quad \forall i$ ist. Wenn $w_i = w_0 \quad \forall i$ ist, sind u und v gleich.
- Wenn die Antwort $u = v$ ist, heisst das, dass nach der ersten Schritt gilt: $u^1 + u^2 + \ldots + u^r = v^1 + u^2 + \ldots + u^r$. Daraus folgt $u^1 = v^1$.
- Gleiches Argument gilt für jeden anderen Schritt. Daher ist $u = v$ korrekt.

dritter Ansatz

- Pudlak und Sgall(1997) haben gezeigt, dass eigentlich $O((\log n)^2)$ Bits genug sind.

dritter Ansatz

- Pudlak und Sgall(1997) haben gezeigt, dass eigentlich $O((\log n)^2)$ Bits genug sind.
- **Satz .** Es ist möglich, die Gleichheit von zwei Vektoren aus $\{0,1\}^n$ unter Benutzung von nur $O(\log n)$ Schritten und $O(\log n)$ Speicherplatz pro Schritt zu testen.

Beweis

- Wir denken u und v als Vektoren in R^n, die nur 0 oder 1 als Einträge haben.

Beweis

- Wir denken u und v als Vektoren in R^n, die nur 0 oder 1 als Einträge haben.
- Man berechnet den euklidischen Abstand von u und v, und schaut, ob es gleich 0 ist.

Beweis

- Wir denken u und v als Vektoren in R^n, die nur 0 oder 1 als Einträge haben.
- Man berechnet den euklidischen Abstand von u und v, und schaut, ob es gleich 0 ist.
- $||u - v||^2 = \langle u, u \rangle + \langle v, v \rangle - 2\langle u, v \rangle$

Beweis

- Wir denken u und v als Vektoren in R^n, die nur 0 oder 1 als Einträge haben.
- Man berechnet den euklidischen Abstand von u und v, und schaut, ob es gleich 0 ist.
- $||u - v||^2 = \langle u, u \rangle + \langle v, v \rangle - 2\langle u, v \rangle$
- $= \sum_{i=1}^{n} u_i^2 + \sum_{i=1}^{n} v_i^2 - 2 \left[(\sum_{i=1}^{n} u_i) \cdot (\sum_{i=1}^{n} v_i) - \sum_{i \neq j} u_i v_j \right]$

Beweis

- Wir denken u und v als Vektoren in R^n, die nur 0 oder 1 als Einträge haben.
- Man berechnet den euklidischen Abstand von u und v, und schaut, ob es gleich 0 ist.
- $||u - v||^2 = \langle u, u \rangle + \langle v, v \rangle - 2\langle u, v \rangle$
- $= \sum_{i=1}^{n} u_i^2 + \sum_{i=1}^{n} v_i^2 - 2\left[(\sum_{i=1}^{n} u_i) \cdot (\sum_{i=1}^{n} v_i) - \sum_{i \neq j} u_i v_j\right]$
- Wir rechnen $\langle u, u \rangle$ und $\langle v, v \rangle$ jeweils in einem Schritt.

Beweis

- Wir denken u und v als Vektoren in R^n, die nur 0 oder 1 als Einträge haben.
- Man berechnet den euklidischen Abstand von u und v, und schaut, ob es gleich 0 ist.
- $||u - v||^2 = \langle u, u\rangle + \langle v, v\rangle - 2\langle u, v\rangle$
- $= \sum_{i=1}^{n} u_i^2 + \sum_{i=1}^{n} v_i^2 - 2\left[(\sum_{i=1}^{n} u_i) \cdot (\sum_{i=1}^{n} v_i) - \sum_{i\neq j} u_i v_j\right]$
- Wir rechnen $\langle u, u\rangle$ und $\langle v, v\rangle$ jeweils in einem Schritt.
- Wir brauchen $\lceil \log(n+1)\rceil$ Bits Speicherplatz um diese zwei Zahlen, die zwischen 0 und n liegen, zu speichern.

Beweis

- Wir denken u und v als Vektoren in R^n, die nur 0 oder 1 als Einträge haben.
- Man berechnet den euklidischen Abstand von u und v, und schaut, ob es gleich 0 ist.
- $||u - v||^2 = \langle u, u\rangle + \langle v, v\rangle - 2\langle u, v\rangle$
- $= \sum_{i=1}^{n} u_i^2 + \sum_{i=1}^{n} v_i^2 - 2\left[(\sum_{i=1}^{n} u_i) \cdot (\sum_{i=1}^{n} v_i) - \sum_{i\neq j} u_i v_j\right]$
- Wir rechnen $\langle u, u\rangle$ und $\langle v, v\rangle$ jeweils in einem Schritt.
- Wir brauchen $\lceil \log(n+1)\rceil$ Bits Speicherplatz um diese zwei Zahlen, die zwischen 0 und n liegen, zu speichern.
- Es bleibt nur $\langle u, v\rangle = \sum_{i=1}^{n} u_i v_i$ zu rechnen.

Beweis

- Dafür berechnen wir erst den Produkt $N := (\sum_{i=1}^{n} u_i)(\sum_{i=1}^{n} v_i)$ mit Hilfe von vorherigen Ergebnissen. Die Berechnung wird mit Belegung von $2\lceil \log(n+1) \rceil$ Bits Speicherplatz abgespeichert..

Beweis

- Dafür berechnen wir erst den Produkt $N := (\sum_{i=1}^{n} u_i)(\sum_{i=1}^{n} v_i)$ mit Hilfe von vorherigen Ergebnissen. Die Berechnung wird mit Belegung von $2\lceil \log(n+1) \rceil$ Bits Speicherplatz abgespeichert..
- Um den gewünschten Produkt $\langle u, v \rangle$ zu berechnen, brauchen wir die Summe $\sum_{i \neq j} u_i v_j$.

Beweis

- Dafür berechnen wir erst den Produkt $N := (\sum_{i=1}^{n} u_i)(\sum_{i=1}^{n} v_i)$ mit Hilfe von vorherigen Ergebnissen. Die Berechnung wird mit Belegung von $2\lceil \log(n+1) \rceil$ Bits Speicherplatz abgespeichert..
- Um den gewünschten Produkt $\langle u, v \rangle$ zu berechnen, brauchen wir die Summe $\sum_{i \neq j} u_i v_j$.
- Das ist mit $2\lceil \log(n) \rceil$ Schritten zu machen:

Beweis

- Dafür berechnen wir erst den Produkt $N := (\sum_{i=1}^{n} u_i)(\sum_{i=1}^{n} v_i)$ mit Hilfe von vorherigen Ergebnissen. Die Berechnung wird mit Belegung von $2\lceil \log(n+1) \rceil$ Bits Speicherplatz abgespeichert..
- Um den gewünschten Produkt $\langle u, v \rangle$ zu berechnen, brauchen wir die Summe $\sum_{i \neq j} u_i v_j$.
- Das ist mit $2\lceil \log(n) \rceil$ Schritten zu machen:
- Wähle die Proben, so dass für jeden Kreuzterm eine andere Kombination berechnet wird. Dann summieren wir alle Kreuzterme.

Beweis

- Dafür berechnen wir erst den Produkt $N := (\sum_{i=1}^{n} u_i)(\sum_{i=1}^{n} v_i)$ mit Hilfe von vorherigen Ergebnissen. Die Berechnung wird mit Belegung von $2\lceil \log(n+1) \rceil$ Bits Speicherplatz abgespeichert..
- Um den gewünschten Produkt $\langle u, v \rangle$ zu berechnen, brauchen wir die Summe $\sum_{i \neq j} u_i v_j$.
- Das ist mit $2\lceil \log(n) \rceil$ Schritten zu machen:
- Wähle die Proben, so dass für jeden Kreuzterm eine andere Kombination berechnet wird. Dann summieren wir alle Kreuzterme.
- Nach jedem Schritt werden die Resultate in $O(\log n)$ Speicherbits abgespeichert.