UNIVERSITÄT LEIPZIG

Windischleuba LSGM Wochenende, 1. Nov 2024

Existenzbeweise durch Wahrscheinlichkeit

Łukasz Grabowski

Mathematisches Institut

Übersicht

1. Die meisten Existenzbeweise sind Konstruktionen

2. Manchmal ist ein Beweis keine Konstruktion, aber wir können einen anderen Beweis finden

3. Probabilistischer Beweis 1 - effiziente probabilistische Konstruktion fast unmittelbar

4. Probabilistischer Beweis 2 - der “wahre” Beweis der Existenz.

1. Die meisten Existenzbeweise sind Konstruktionen

2. Manchmal ist ein Beweis keine Konstruktion, aber wir können einen anderen Beweis finden

3. Probabilistischer Beweis 1 - effiziente probabilistische Konstruktion fast unmittelbar

4. Probabilistischer Beweis 2 - der “wahre” Beweis der Existenz.

- Es gibt unendlich viele Primzahlen

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.

- Es gibt unendlich viele Primzahlen
    - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p

- Es gibt unendlich viele Primzahlen
    - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
    - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung

- Es gibt unendlich viele Primzahlen
    - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
    - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.

- Es gibt unendlich viele Primzahlen
    - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
    - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
    - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.

- Es gibt unendlich viele Primzahlen
    - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
    - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
    - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung,

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
  - Sei $p_1, \ldots, p_n$ Primzahlen.

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
  - Sei $p_1, \ldots, p_n$ Primzahlen. Wir wollen zeigen,

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
  - Sei $p_1, \ldots, p_n$ Primzahlen. Wir wollen zeigen, wie man eine andere Primzahl als diese

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
  - Sei $p_1, \ldots, p_n$ Primzahlen. Wir wollen zeigen, wie man eine andere Primzahl als diese konstruieren kann.

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
  - Sei $p_1, \ldots, p_n$ Primzahlen. Wir wollen zeigen, wie man eine andere Primzahl als diese konstruieren kann.
  - Betrachten wir die Zahl

- Es gibt unendlich viele Primzahlen
    - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
    - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
    - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
    - Sei $p_1, \ldots, p_n$ Primzahlen. Wir wollen zeigen, wie man eine andere Primzahl als diese konstruieren kann.
    - Betrachten wir die Zahl $p_1 \cdot \ldots p_n + 1$.

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
  - Sei $p_1, \ldots, p_n$ Primzahlen. Wir wollen zeigen, wie man eine andere Primzahl als diese konstruieren kann.
  - Betrachten wir die Zahl $p_1 \cdot \ldots p_n + 1$. Nehmen wir ihre Primzahlzerlegung.

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
  - Sei $p_1, \ldots, p_n$ Primzahlen. Wir wollen zeigen, wie man eine andere Primzahl als diese konstruieren kann.
  - Betrachten wir die Zahl $p_1 \cdot \ldots p_n + 1$. Nehmen wir ihre Primzahlzerlegung. Jede Primzahl in dieser Zerlegung

- Es gibt unendlich viele Primzahlen
  - Nehmen wir an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt.
  - Betrachten wir eine beliebige Primzahl p in der Primzahlzerlegung von $p_1 \cdot \ldots \cdot p_n + 1$.
  - p kann keine der Zahlen $p_1, p_2, \ldots, p_n$ sein. Widerspruch.
- Das ist in Ordnung, aber Euklids Argument war ungefähr:
  - Sei $p_1, \ldots, p_n$ Primzahlen. Wir wollen zeigen, wie man eine andere Primzahl als diese konstruieren kann.
  - Betrachten wir die Zahl $p_1 \cdot \ldots p_n + 1$. Nehmen wir ihre Primzahlzerlegung. Jede Primzahl in dieser Zerlegung ist von den gegebenen verschieden.

- Betrachten Sie ein konvexes Fünfeck

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben.

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
  - Modelllösung.

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
  - **Modelllösung.** Angenommen, dies ist nicht der Fall.

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
    - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.

    - ▶ Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
    - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.
    - Betrachte alle Intervalle

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
    - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.
    - Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
    - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.
    - Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden. (Also Diagonalen und die Kanten von $ABCDE$)

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
    - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.
    - Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden. (Also Diagonalen und die Kanten von $ABCDE$)
    - Nach dem Schubladenprinzip,

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
  - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.
  - Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden. (Also Diagonalen und die Kanten von $ABCDE$)
  - Nach dem Schubladenprinzip, gibt es zwei Eckpunkte

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.

  - ▶ Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.

  - ▶ Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden. (Also Diagonalen und die Kanten von $ABCDE$)

  - ▶ Nach dem Schubladenprinzip, gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
  - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.
  - Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden. (Also Diagonalen und die Kanten von $ABCDE$)
  - Nach dem Schubladenprinzip, gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.
  - Der Mittelpunkt M

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.

  - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.
  - Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden. (Also Diagonalen und die Kanten von $ABCDE$)
  - Nach dem Schubladenprinzip, gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.
  - Der Mittelpunkt M des Intevalls zwischen diesen beiden Punkten

- Betrachten Sie ein konvexes Fünfeck , dessen Eckpunkte ganzzahlige Koordinaten haben. Zu zeigen ist, dass es einen Punkt mit ganzzahligen Koeffizienten existiert, der echt innerhalb dieses Fünfecks liegt.
  - Modelllösung. Angenommen, dies ist nicht der Fall. Sei $ABCDE$ ein Gegenbeispiel mit der kleinstmöglichen Fläche.
  - Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden. (Also Diagonalen und die Kanten von $ABCDE$)
  - Nach dem Schubladenprinzip, gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.
  - Der Mittelpunkt M des Intevalls zwischen diesen beiden Punkten hat ganzzahlige Koeffizienten.

- Da $ABCDE$ ein Gegenbeispiel ist,

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein.

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$ durch $AMCDE$ ersetzen,

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$ durch $AMCDE$ ersetzen, um ein Gegenbeispiel

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$ durch $AMCDE$ ersetzen, um ein Gegenbeispiel mit der kleineren Fläche

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$ durch $AMCDE$ ersetzen, um ein Gegenbeispiel mit der kleineren Fläche zu erhalten.

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$ durch $AMCDE$ ersetzen, um ein Gegenbeispiel mit der kleineren Fläche zu erhalten.
- Dieser Widerspruch

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$ durch $AMCDE$ ersetzen, um ein Gegenbeispiel mit der kleineren Fläche zu erhalten.
- Dieser Widerspruch zeigt,

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$ durch $AMCDE$ ersetzen, um ein Gegenbeispiel mit der kleineren Fläche zu erhalten.
- Dieser Widerspruch zeigt, dass es keine Gegenbeispiele gibt.

- Da $ABCDE$ ein Gegenbeispiel ist, muss dieses Intervall eine Kante von $ABCDE$ sein. Angenommen M ist der Mittelpunkt von AB.
- Wir können $ABCDE$ durch $AMCDE$ ersetzen, um ein Gegenbeispiel mit der kleineren Fläche zu erhalten.
- Dieser Widerspruch zeigt, dass es keine Gegenbeispiele gibt. $\square$

- Betrachten Sie ein konvexes Fünfeck

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben.

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
    - Das Fünfeck sei $ABCDE$.

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
    - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
    - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
    - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.
    - Nach dem Schubladenprinzip

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
    - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.
    - Nach dem Schubladenprinzip gibt es zwei Eckpunkte

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
  - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.
  - Nach dem Schubladenprinzip gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
  - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.
  - Nach dem Schubladenprinzip gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.
  - Der Mittelpunkt M

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
    - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.
    - Nach dem Schubladenprinzip gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.
    - Der Mittelpunkt M des Intevalls zwischen diesen beiden Punkten

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
  - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.
  - Nach dem Schubladenprinzip gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.
  - Der Mittelpunkt M des Intevalls zwischen diesen beiden Punkten hat ganzzahlige Koeffizienten.

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
    - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.
    - Nach dem Schubladenprinzip gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.
    - Der Mittelpunkt M des Intevalls zwischen diesen beiden Punkten hat ganzzahlige Koeffizienten.
    - Wenn M innen ist, dann beende.

- Betrachten Sie ein konvexes Fünfeck , dessen Knoten ganzzahlige Koordinaten haben. Konstruiere einen Punkt mit ganzzahligen Koeffizienten , der echt innerhalb dieses Fünfecks liegt.
    - Das Fünfeck sei $ABCDE$. Betrachte alle Intervalle , die zwei Eckpunkte dieses Fünfecks verbinden.
    - Nach dem Schubladenprinzip gibt es zwei Eckpunkte mit den Koordinaten (a, b) (c, d) so, dass $a \equiv c$ und $b \equiv d$ modulo 2.
    - Der Mittelpunkt M des Intevalls zwischen diesen beiden Punkten hat ganzzahlige Koeffizienten.
    - Wenn M innen ist, dann beende.
    - Andernfalls wiederhole diesen Vorgang mit $AMCDE$ anstelle von $ABCDE$.

1. Die meisten Existenzbeweise sind Konstruktionen

2. Manchmal ist ein Beweis keine Konstruktion, aber wir können einen anderen Beweis finden

3. Probabilistischer Beweis 1 - effiziente probabilistische Konstruktion fast unmittelbar

4. Probabilistischer Beweis 2 - der “wahre” Beweis der Existenz.

- Sei p eine Primzahl,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \dots, p-1\}$.

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
    - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
    - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
    - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)
  - Also die Funktion $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)
  - Also die Funktion $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$, definiert durch $f(x) \equiv ax \pmod p$

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)
  - Also die Funktion $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$, definiert durch $f(x) \equiv ax \pmod p$ ist injektiv.

- Sei p eine Primzahl, und sei $a \in \{1, 2, \dots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - ▶ Wenn x und y verschiedene Elemente von $\{1, 2, \dots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)
  - ▶ Also die Funktion $\{1, \dots, p-1\} \to \{1, \dots, p-1\}$, definiert durch $f(x) \equiv ax \pmod p$ ist injektiv.
  - ▶ Da $\{1, \dots, p-1\}$ eine endliche Menge ist,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)
  - Also die Funktion $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$, definiert durch $f(x) \equiv ax \pmod p$ ist injektiv.
  - Da $\{1, \ldots, p-1\}$ eine endliche Menge ist, ist f auch surjektiv,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)
  - Also die Funktion $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$, definiert durch $f(x) \equiv ax \pmod p$ ist injektiv.
  - Da $\{1, \ldots, p-1\}$ eine endliche Menge ist, ist f auch surjektiv, also haben wir für einige x

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)
  - Also die Funktion $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$, definiert durch $f(x) \equiv ax \pmod p$ ist injektiv.
  - Da $\{1, \ldots, p-1\}$ eine endliche Menge ist, ist f auch surjektiv, also haben wir für einige x dass $1 = f(x) = ax$.

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wenn x und y verschiedene Elemente von $\{1, 2, \ldots, p-1\}$ sind, dann $ax \not\equiv ay$ (sonst $a(x-y) \equiv 0$, was nicht möglich ist)
  - Also die Funktion $\{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$, definiert durch $f(x) \equiv ax \pmod p$ ist injektiv.
  - Da $\{1, \ldots, p-1\}$ eine endliche Menge ist, ist f auch surjektiv, also haben wir für einige x dass $1 = f(x) = ax$.
- Wir können das nicht als Konstruktion schreiben.

- Sei p eine Primzahl,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$.

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wir brauchen $x, y \in \mathbb{Z}$ finden,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wir brauchen $x, y \in \mathbb{Z}$ finden, mit $ax + py = 1$.

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
  - Wir brauchen $x, y \in \mathbb{Z}$ finden, mit $ax + py = 1$.
  - Dazu können wir den Euklidischen Algorthmus verwenden,

- Sei p eine Primzahl, und sei $a \in \{1, 2, \ldots, p-1\}$. Wir können b so finden, dass $ab \equiv 1$ modulo p.
    - Wir brauchen $x, y \in \mathbb{Z}$ finden, mit $ax + py = 1$.
    - Dazu können wir den Euklidischen Algorthmus verwenden, wenn wir mit p and a anfangen.

1. Die meisten Existenzbeweise sind Konstruktionen

2. Manchmal ist ein Beweis keine Konstruktion, aber wir können einen anderen Beweis finden

3. Probabilistischer Beweis 1 - effiziente probabilistische Konstruktion fast unmittelbar

4. Probabilistischer Beweis 2 - der “wahre” Beweis der Existenz.

- Wir sagen,

- Wir sagen, dass eine Menge A natürlicher Zahlen

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist,

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
    - Beispiel:

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei,

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
    - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei,

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös]

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
    - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen.

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
    - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
    - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Die Elemente von B

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Die Elemente von B seien $b_1 < b_2 < \ldots < b_n$.

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Die Elemente von B seien $b_1 < b_2 < \ldots < b_n$. Sei $p = 3k + 2$ eine Primzahl größer als b_n.

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Die Elemente von B seien $b_1 < b_2 < \ldots < b_n$. Sei $p = 3k + 2$ eine Primzahl größer als b_n.
- Die Menge $C := \{k + 1, k + 2, \ldots, 2k + 1\}$

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Die Elemente von B seien $b_1 < b_2 < \ldots < b_n$. Sei $p = 3k + 2$ eine Primzahl größer als b_n.
- Die Menge $C := \{k + 1, k + 2, \ldots, 2k + 1\}$ ist summenfrei

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
    - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Die Elemente von B seien $b_1 < b_2 < \ldots < b_n$. Sei $p = 3k + 2$ eine Primzahl größer als b_n.
- Die Menge $C := \{k + 1, k + 2, \ldots, 2k + 1\}$ ist summenfrei modulo p

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Die Elemente von B seien $b_1 < b_2 < \ldots < b_n$. Sei $p = 3k + 2$ eine Primzahl größer als b_n.
- Die Menge $C := \{k + 1, k + 2, \ldots, 2k + 1\}$ ist summenfrei modulo p (d.h. $a + b \not\equiv c \mod p$)

- Wir sagen, dass eine Menge A natürlicher Zahlen *summenfrei* ist, wenn es keine $a, b, c \in A$ gibt mit $a + b = c$.
  - Beispiel: $\{4, 5, 6, 7, 8\}$ ist summenfrei, $\{4, 6, 7, 8, 9\}$ ist summenfrei, $\{4, 6, 8, 9, 10\}$ ist nicht summenfrei.

Theorem. [Erdös] Sei B eine Menge von natürlichen Zahlen mit n Elementen. Es gibt eine summenfreie Teilmenge $A \subset B$ mit mehr als $\frac{n}{3}$ Elementen.

Beweis.

- Die Elemente von B seien $b_1 < b_2 < \ldots < b_n$. Sei $p = 3k + 2$ eine Primzahl größer als b_n.
- Die Menge $C := \{k + 1, k + 2, \ldots, 2k + 1\}$ ist summenfrei modulo p (d.h. $a + b \not\equiv c \mod p$)
- Wir haben

$$\frac{|C|}{p - 1} > \frac{1}{3}$$

- Wir verwenden nun die Methode des Doppelten Abzählens

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als “Methode des ersten Moments” bezeichnet).

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$.

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als “Methode des ersten Moments” bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als “Methode des ersten Moments” bezeichnet).
    - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$.

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
    - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als “Methode des ersten Moments” bezeichnet).
  - ▶ Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - ▶ Wenn wir b_i festlegen und alle möglichen x betrachten,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
    - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
    - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \dots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i)

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - ▶ Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - ▶ Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - ▶ Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
    - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
    - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
    - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
    - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto x b_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
    - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
    - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
    - Daraus folgt,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als “Methode des ersten Moments” bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i)

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
    - ▶ Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
    - ▶ Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
    - ▶ Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
    - ▶ Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als “Methode des ersten Moments” bezeichnet).
    - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
    - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
    - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
    - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F derjenigen $b \in B$,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F derjenigen $b \in B$, für die $x_0 b \in C$ gilt.

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F derjenigen $b \in B$, für die $x_0 b \in C$ gilt.
  - Wenn wir $a + b = c$

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als “Methode des ersten Moments” bezeichnet).
    - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
    - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
    - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
    - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F derjenigen $b \in B$, für die $x_0 b \in C$ gilt.
    - Wenn wir $a + b = c$ für einige Elemente von F haben,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F derjenigen $b \in B$, für die $x_0 b \in C$ gilt.
  - Wenn wir $a + b = c$ für einige Elemente von F haben, dann haben wir auch $x_0 a + x_0 b = x_0 c$ modulo p,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F derjenigen $b \in B$, für die $x_0 b \in C$ gilt.
  - Wenn wir $a + b = c$ für einige Elemente von F haben, dann haben wir auch $x_0 a + x_0 b = x_0 c$ modulo p, was unmöglich ist,

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als “Methode des ersten Moments” bezeichnet).
  - Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F derjenigen $b \in B$, für die $x_0 b \in C$ gilt.
  - Wenn wir $a + b = c$ für einige Elemente von F haben, dann haben wir auch $x_0 a + x_0 b = x_0 c$ modulo p, was unmöglich ist, weil C summenfrei modulo p ist.

- Wir verwenden nun die Methode des Doppelten Abzählens (in diesem Kontext als "Methode des ersten Moments" bezeichnet).
  - ▶ Fixieren wir $x \in \{1, \ldots, p-1\}$. Betrachten wir die Funktion $b_i \mapsto xb_i \mod (p)$. Wie viele Elemente von B werden auf C abgebildet?
  - ▶ Wenn wir b_i festlegen und alle möglichen x betrachten, dann ist $x \cdot b_i \in C$ in mehr als $\frac{1}{3}$ Fällen.
  - ▶ Daraus folgt, dass unter allen Paaren (x, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x \cdot b_i$ in C modulo p ist.
  - ▶ Daraus folgt, dass es x_0 gibt, dass unter allen Paaren (x_0, b_i) mehr als $\frac{1}{3}$ der Fälle so sind, dass $x_0 b_i$ in C modulo p ist.
- Betrachten wir die Menge F derjenigen $b \in B$, für die $x_0 b \in C$ gilt.
  - ▶ Wenn wir $a + b = c$ für einige Elemente von F haben, dann haben wir auch $x_0 a + x_0 b = x_0 c$ modulo p, was unmöglich ist, weil C summenfrei modulo p ist. □

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \dots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \dots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \dots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$.

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \dots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \dots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^50 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
    - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
    - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
    - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^50 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern,

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten.

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \dots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \dots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten. Übung:

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten. Übung: Für jeden $\varepsilon > 0$

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten. Übung: Für jeden $\varepsilon > 0$ gibt es $\pi < 1$,

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten. Übung: Für jeden $\varepsilon > 0$ gibt es $\pi < 1$, so dass

$$|\{x \in \{1, \ldots, p-1\}:$$

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^50 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten. Übung: Für jeden $\varepsilon > 0$ gibt es $\pi < 1$, so dass

$$|\{x \in \{1, \ldots, p-1\} \colon |\{b_i : xb_i \in C\}| < (\frac{1}{3} - \varepsilon)|B|\}|$$

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
    - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
    - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
    - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten. Übung: Für jeden $\varepsilon > 0$ gibt es $\pi < 1$, so dass

$$|\{x \in \{1, \ldots, p-1\} \colon |\{b_i \colon xb_i \in C\}| < (\frac{1}{3} - \varepsilon)|B|\}| < \pi \cdot (p-1).$$

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten. Übung: Für jeden $\varepsilon > 0$ gibt es $\pi < 1$, so dass

$$|\{x \in \{1, \ldots, p-1\} \colon |\{b_i : xb_i \in C\}| < (\frac{1}{3} - \varepsilon)|B|\}| < \pi \cdot (p-1).$$

  - Bemerkung:

- Übung: Im Beweis ist die Wahrscheinlichkeit, dass ein gegebenes $x \in \{1, \ldots, p-1\}$ weniger als $\frac{1}{4}$ von b_i nach C sendet, durch $\frac{8}{9}$ beschränkt.
- Effizienter Algorithmus zum Finden einer summenfreien Menge mit $\frac{n}{4}$ Elementen:
  - Wähle $x \in \{1, \ldots, p-1\}$ zufällig.
  - Prüfe, ob es $\frac{1}{4}$ von b_i nach C schickt.
  - Wenn ja, dann liste diese Elemente auf und beende es.
- Die Wahrscheinlichkeit, dass wir nach 50 Iterationen scheitern, ist kleiner als $(\frac{8}{9})^5 0 < 0,003$. Diese Wahrscheinlichkeit hängt nicht von n ab!
- Wir können es problemlos verallgemeinern, um summenfreie Teilmengen von beliebiger Größe nahe $\frac{1}{3}$ zu erhalten. Übung: Für jeden $\varepsilon > 0$ gibt es $\pi < 1$, so dass

$$|\{x \in \{1, \ldots, p-1\} \colon |\{b_i \colon xb_i \in C\}| < (\frac{1}{3} - \varepsilon)|B|\}| < \pi \cdot (p-1).$$

  - Bemerkung: Diese Übung ist im Wesentlichen als *Markov-Ungleichung* bekannt.

1. Die meisten Existenzbeweise sind Konstruktionen

2. Manchmal ist ein Beweis keine Konstruktion, aber wir können einen anderen Beweis finden

3. Probabilistischer Beweis 1 - effiziente probabilistische Konstruktion fast unmittelbar

4. Probabilistischer Beweis 2 - der “wahre” Beweis der Existenz.

- Bei einem Graphen $G = (V, E)$

- Bei einem Graphen $G = (V, E)$ mit n Knoten

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant,

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten:

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$,

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein?

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere:

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
  - Man kann die Frage präzisieren,

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
    - Man kann die Frage präzisieren, indem man den Erwartungswert

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
    - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses

- Bei einem Graphen $G=(V,E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
  - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
  - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
  - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.
- Es gibt sehr effiziente Algorithmen,

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
  - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.
- Es gibt sehr effiziente Algorithmen, die eine unabhängige Menge

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
    - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.
- Es gibt sehr effiziente Algorithmen, die eine unabhängige Menge mit einem Verhältnis von ca. $\log(d)/d$

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
  - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.
- Es gibt sehr effiziente Algorithmen, die eine unabhängige Menge mit einem Verhältnis von ca. $\log(d)/d$ konstruieren können.

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
  - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.
- Es gibt sehr effiziente Algorithmen, die eine unabhängige Menge mit einem Verhältnis von ca. $\log(d)/d$ konstruieren können.
- Es gibt jedoch einen probabilistischen Beweis,

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
    - ▶ Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.
- Es gibt sehr effiziente Algorithmen, die eine unabhängige Menge mit einem Verhältnis von ca. $\log(d)/d$ konstruieren können.
- Es gibt jedoch einen probabilistischen Beweis, dass es unabhängige Mengen der Größe $\frac{2\log(d)}{d}$ gibt.

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
  - ▶ Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.
- Es gibt sehr effiziente Algorithmen, die eine unabhängige Menge mit einem Verhältnis von ca. $\log(d)/d$ konstruieren können.
- Es gibt jedoch einen probabilistischen Beweis, dass es unabhängige Mengen der Größe $\frac{2\log(d)}{d}$ gibt. Es gibt keinen bekannten Algorithmus,

- Bei einem Graphen $G = (V, E)$ mit n Knoten ist es interessant, unabhängige Mengen zu betrachten: $I \subset V$, so dass keine zwei Elemente von I miteinander verbunden sind.
- Insbesondere wie groß kann I sein? Das größtmögliche $|I|/|V|$ nennt man das Unabhängigkeitsverhältnis.
- Insbesondere: Wie groß ist das Unabhängigkeitsverhältnis eines typischen Graphen mit dem maximalen Grad d?
    - Man kann die Frage präzisieren, indem man den Erwartungswert des Unabhängigkeitsverhältnisses eines Graphen vom maximalen Grad d mit n Knoten betrachtet und n gegen unendlich gehen lässt.
- Es gibt sehr effiziente Algorithmen, die eine unabhängige Menge mit einem Verhältnis von ca. $\log(d)/d$ konstruieren können.
- Es gibt jedoch einen probabilistischen Beweis, dass es unabhängige Mengen der Größe $\frac{2\log(d)}{d}$ gibt. Es gibt keinen bekannten Algorithmus, der über $\frac{\log(d)}{d}$ hinausgeht.

UNIVERSITÄT LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski
Mathematisches Institut

grabowski@math.uni-leipzig.de