Diskrete Mathematik

Kryptographie und Graphentheorie

Jochen Hormes
&
Jonas Bühler

14.06.2006

Inhaltsverzeichnis

Kryptographie

1. Einführung

Es werden Funktionen benötigt, die folgende Kriterien erfüllen:

- leicht zu berechnen
- mit den richtigen Infos leicht umkehrbar
- ohne Infos extrem schwer umkehrbar

Eine verbreitete Möglichkeit ist das Produkt zweier großer Primzahlen.

2. Faktorisierung

Um auch ohne die nötigen Informationen die Umkehrung von

$$n = p * q$$

zu berechnen, gibt es verschiedene Ansätze:

1. Eine einfach Primfaktorzerlegung
   Untersuche alle Zahlen bis $m \leq \sqrt{n}$, ob diese Zahl n teilt

2. Eine erste Verbesserung:
   Untersuche dies nur für Primzahlen bis $\sqrt{n}$

3. Fermat:
   Existiert eine Zerlegung $n = a^2 – b^2$ dann ist eine Zerlegung gefunden durch $n = (a + b) * (a – b)$
   Es gilt dann auch $b^2 = a^2 – n$. Berechne dies nun für die Zahlen $a \geq \sqrt{n}$.
   Ist das Ergebnis eine Quadratzahl b^2, so ist die Zerlegung gefunden.

Beispiel:

n = 851

=> $\sqrt{n}$ = 29,171...

=> Start bei a = 30

$30^2 - 851 = 49 = 7^2$

=> a = 30, b = 7
n = (30 + 7) * (30 – 7) = 37 * 23

Übung:

Zerlege die Zahl n = 85 mit der Faktorisierungsmethode von Fermat.

Zerlege nach der selben Methode die Zahl n = 3431.

3. Zusammenfassung

Die Kryptographie ist immer ein Wettlauf zwischen besseren Verschlüsselungsalgorithmen und weiterentwickelten Algorithmen, die diese Verschlüsselung knacken sollen.

Das Produkt aus großen Primzahlen wird z.b. in der Public-Key Verschlüsselung benutzt. Wie man sich vorstellen kann, ist es selbst mit sehr eleganten Algorithmen und modernen Rechnern sehr aufwändig eine Zerlegung in große Primzahlen durchzuführen.

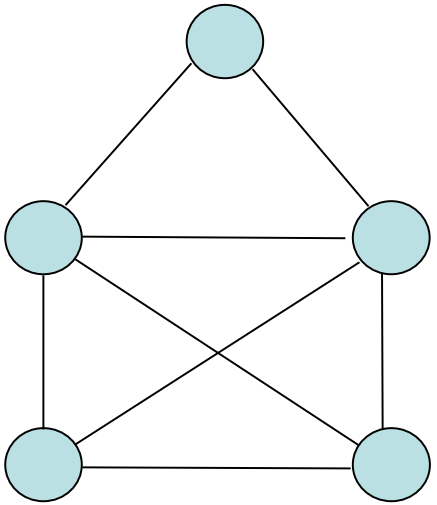
Solange dies nicht möglich ist, sind Algorithmen, die diese Art der Verschlüsselung verwenden sicher. Mit herkömmlichen Methoden wird dies in absehbarer Zeit nicht möglich sein, ein Unsicherheitsfaktor sind momentan die Quantencomputer.

Graphentheorie

1. Ungerichtete Graphen

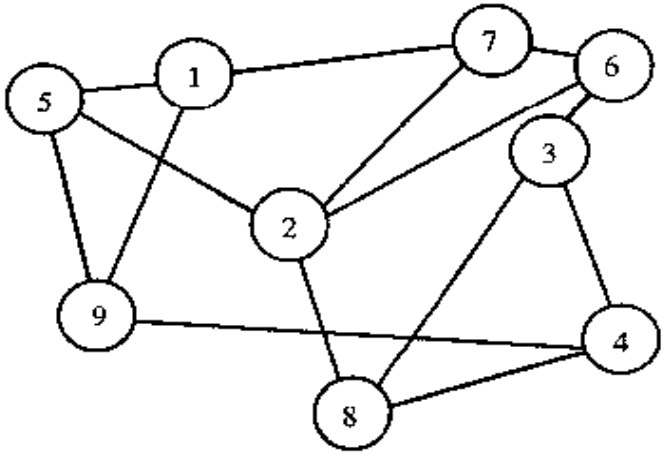
Die einfachste Form sind ungerichtete Graphen. Sie bestehen aus:

- Knoten (auch Ecken genannt)
- Kanten, die bestimmte Knoten miteinander verbinden.



Verwendung finden Graphen bei der Wegfindung (Speditionen, Flug-optimierung), in der Elektrotechnik (Leiterbahn-Layout), vielen Gebieten der Informatik und noch einigen weiteren Bereichen.

Beschrieben werden Graphen normal durch eine Durchnummerierung der Knoten und eine Auflistung der durch Kanten verbundenen Knoten:



E = {1,2,3,4,5,6,7,8,9}
K = {(1,5),(1,7),(1,9),(2,5),...,(6,7)}

2. Weitere Merkmale

- **vollständig**
  Ein Graph heißt vollständig, wenn man von jeder Ecke direkt zu jeder anderen Ecke gelangen kann. Ein vollständiger Graph mit n Ecke wird mit K_n bezeichnet.

- **zusammenhängend**
  Kann man von jeder Ecke über eine Folge von Kanten zu jeder anderen Ecke gelangen kann. Das heißt, es existieren keine isolierten Punkte.
  Ein **Kantenzug** wird durch die Folge der zu benutzenden Kanten angegeben. Im oberen Beispiel würde man mit k2,k14 (letzte Kante) von e1 zu e6 gelangen.

- **geschlossen**
  Ein Kantenzug heißt geschlossen, wenn Anfangs- und Endpunkt gleich sind.

- **Weg**
  Wird in einem Kantenzug jede Kante (maximal) einmal verwendet, so heißt er Weg.

- **Kreis**
  Ein geschlossener Weg heißt Kreis.

- **Länge**
  Die Länge eines Weges ist durch die Anzahl seiner Kanten definiert.

- **Grad**
  Der Grad einer Ecke ist gleich der Anzahl der von ihm abgehenden Kanten.

- **isoliert**
  Ist grad(e) = 0, so heißt die Ecke e isoliert.

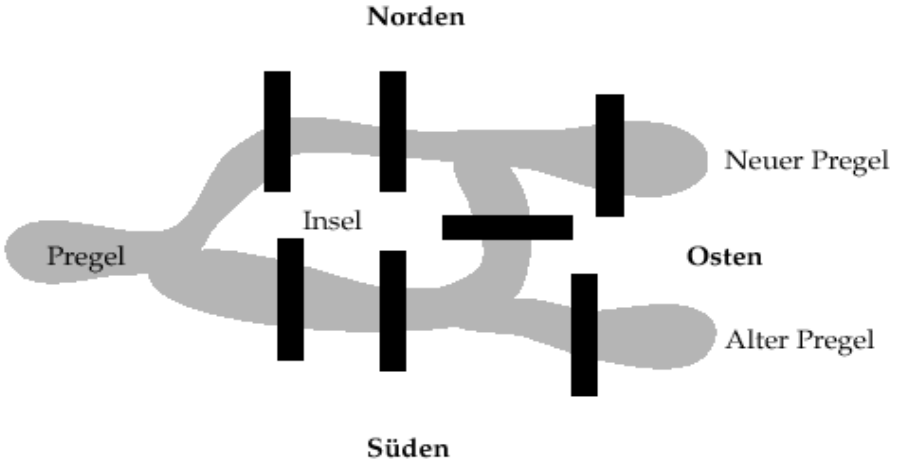
Übung:

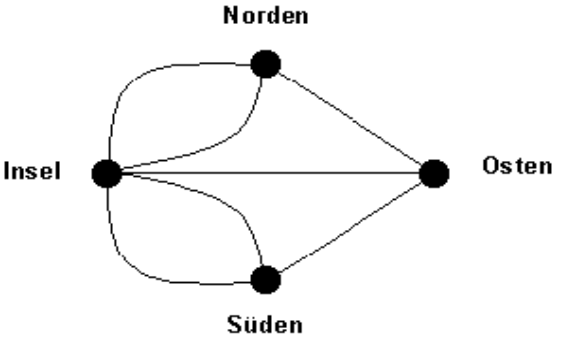
Zeichne K_1 bis K_5.

Kann man K_1 bis K_5 jeweils in einem einzigen geschlossenen Kantenzug zeichnen?

3. Königsberg

Die Stadt Königsberg wird durch die Pregel in vier Teile, darunter eine Insel, geteilt. Nachdem insgesamt sieben Brücken über die Pregel gebaut wurden, entbrannte ein Streit, ob es einen Rundweg durch die Stadt gäbe, der alle Brücken einmal überquert.





Euler übersetzte dieses Problem in die Sprache der Graphentheorie, indem er die Landgebiete als Ecken und die Brücken als Kanten definierte.
Gibt es nun einen Kreis, der jede Kante verwendet, so heißt er eulerscher Kreis und ein Graph mit eulerschem Kreis heißt ebenfalls eulersch.

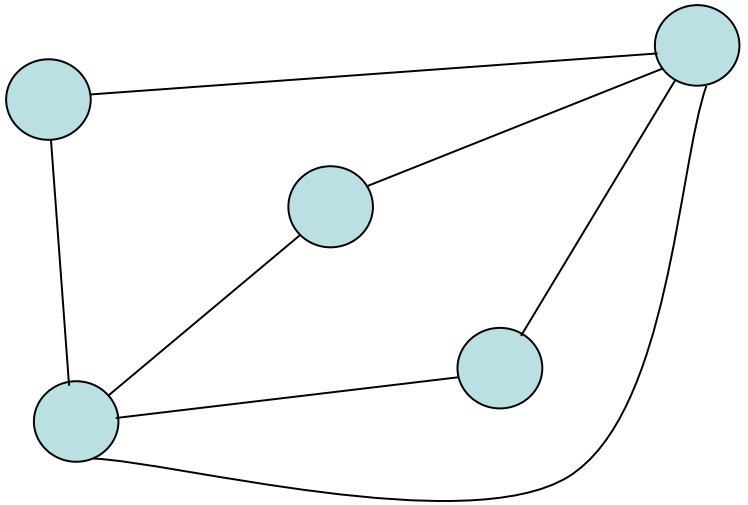
Übung:

Welcher der vollständigen Graphen K_2 bis K_5 ist eulersch?

Ist das Haus vom Nikolaus eulersch?

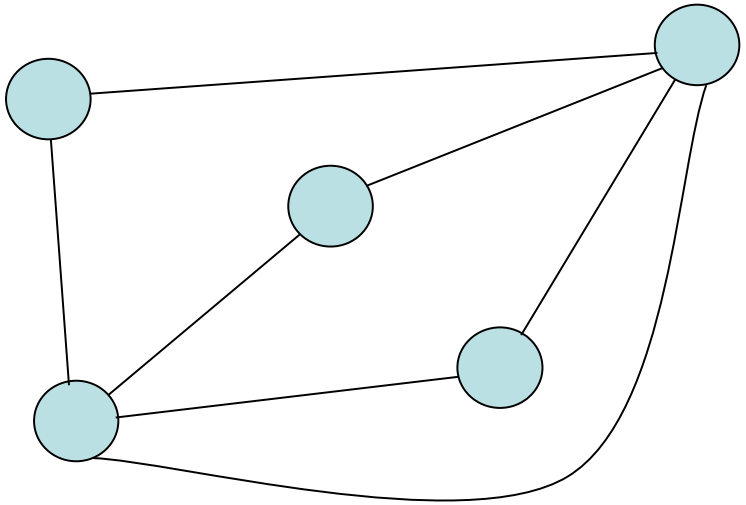
4. Satz von Euler

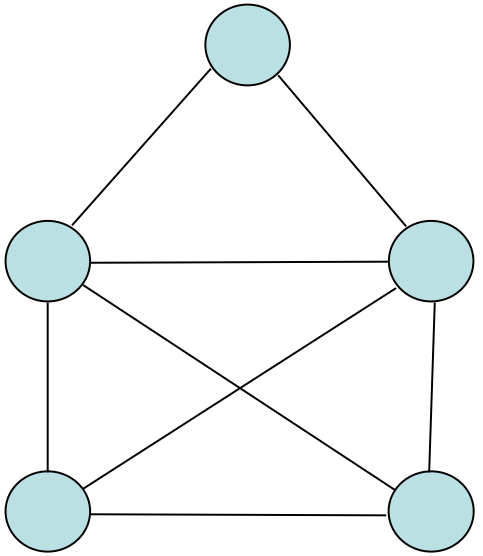
- Wenn der Graph **G eulersch** ist, dann hat jede Ecke einen **geraden Grad**



$$G\ eulersch \Rightarrow\ \ grad(e_i) = 2n_i$$

- Wenn **alle Ecken geraden Grades** sind, dann existiert ein **eulerscher Kreis**





$$G \; eulersch \Leftarrow \; grad(e_i) = 2n_i$$

- $G \text{ eulersch} \Leftrightarrow \text{grad}(e_i) = 2n_i$

- Finden wir eine Ecke ungeraden Grades, so kann dieser Graph nicht eulersch sein

- Haben nur zwei Ecken ungeraden Grad, so kann man diese durch eine zusätzliche Kante verbinden und man erhält einen eulerschen K*reis*

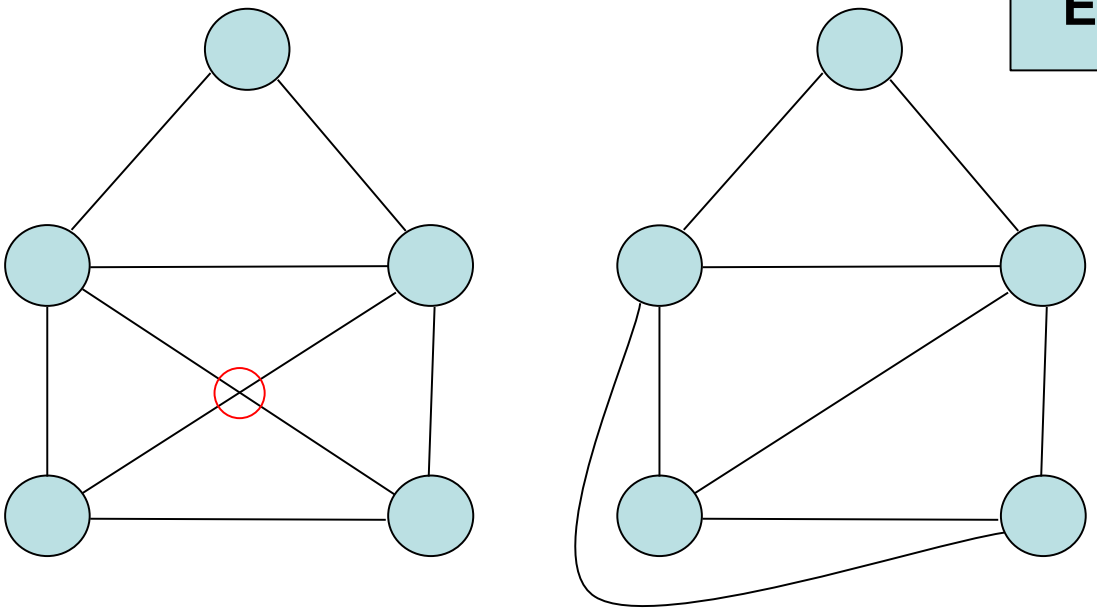
Beweis ?

5. Planar und plättbar

- **Planar**: Kanten berühren sich höchstens in den Ecken
- Ist das HvN plättbar?

Aufgabe:

Ecken - Kanten + Gebiete = ?

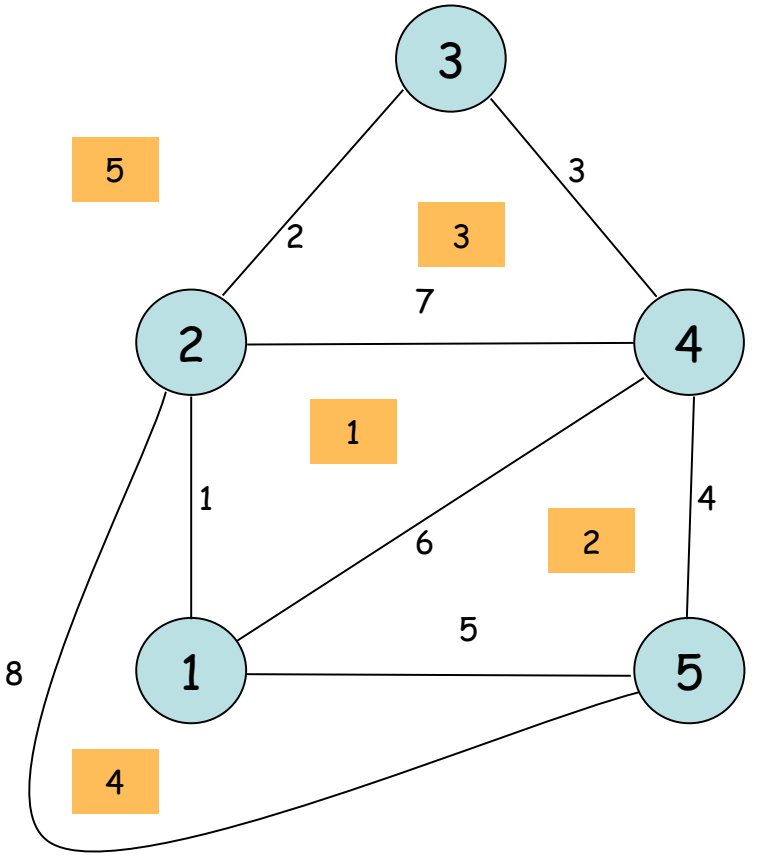


- Planare Graphen zerlegen die Ebene in Gebiete (Länder)

- HvN$_{(planar)}$:
  - n = 5 Ecken
  - m = 8 Kanten
  - g = 5 Länder

- Wir sehen:

$$5 - 8 + 5 = 2$$



Aufgabe: entferne das Dach und die nach außen verlegte Diagonale

Ecken - Kanten + Gebiete = ?

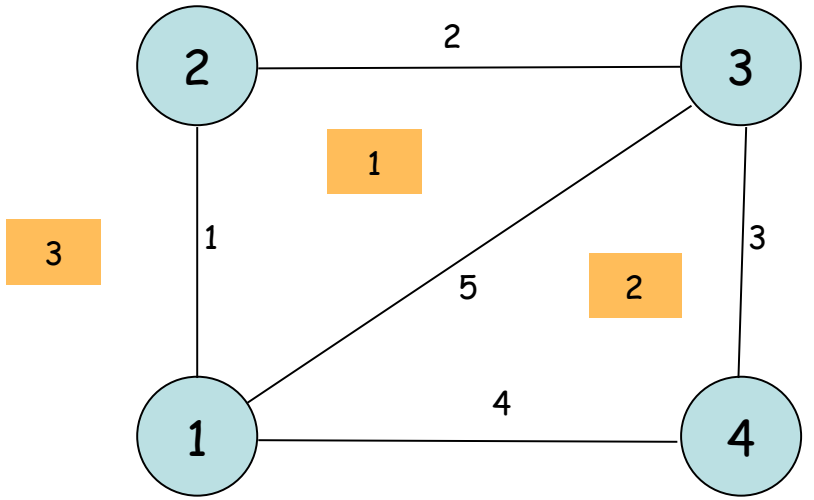
6. Eulerscher Polyedersatz

- Für einen zusammenhängenden, planaren Graphen mit
  n Ecken,
  m Kanten und
  g Gebieten gilt:

$$n - m + g = 2$$

n = 4 Ecken
m = 5 Kanten
g = 3 Länder

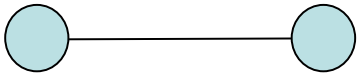
$\rightarrow \quad 4 - 5 + 3 = 2$



Beweis:

- Vollständige Induktion
- Beweis über die Kantenzahl m

$m = 1$



$\Rightarrow \quad g = 1, n = 2$

$n - m + g =$

$2 - 1 + 1 = 2$

- Induktionsvorrausetzung:

  die Aussage

  $n - m + g = 2$

  stimme für die Kantenzahl m

- (wir setzen außerdem voraus: $n \geq 2$)

- Betrachten Graphen mit m + 1 Kanten (n Ecken, g Gebieten)
- zu zeigen:

$$n - (m + 1) + g = 2$$

- **Fall 1**: $\exists e,\ grad(e) = 1$
- wir entfernen diese Ecke mit dieser Kante

  $n' = n - 1,\ m' = m + 1 - 1,\ g' = g$
- dieser Graph erfüllt nach Induktionsvorrausetzung

$$n' - m' + g' = 2 = n - 1 - m + g$$

$$\Leftrightarrow\ n - (m + 1) + g = 2$$

- **Fall 2**: $\forall e,\ grad(e) \geq 2$
- es existiert ein Kreis
- entfernen einer Kante dieses Kreises:

  $n' = n,\ m' = m + 1 - 1,\ g' = g - 1$
- nach Induktionsvorrausetzung

$$n' - m' + g' = 2 = n - m + g - 1$$

$$\Leftrightarrow\ n - (m + 1) + g = 2$$

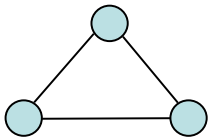
7. Wenig Kanten…

- …hat ein **planarer zusammenhängender** Graph! Nämlich:

$$m \leq 3n - 6$$

- Zum Beweis betrachten wir für jedes Gebiet eines Graphen die Zahl der g_i umschließenden Kanten:

$$m(g_i)$$

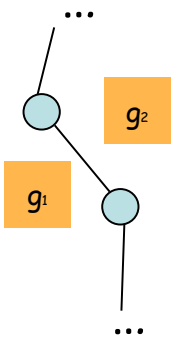


- Jedes Land hat mindestens 3 Kanten:

$$\sum m(g_i) \geq 3g$$

- Jetzt haben wir aber jede Kanten doppelt gezählt

$$\sum m(g_i) = 2m$$



$$\sum m(g_i) = 2m \qquad \sum m(g_i) \geq 3g$$

$$\Rightarrow \quad g \leq \frac{2}{3} m$$

- in die Euler-Formel:

$$2 = n - m + g \leq n - m + \frac{2}{3} m$$

$$= n - \frac{1}{3} m$$

Multiplikation mit 3

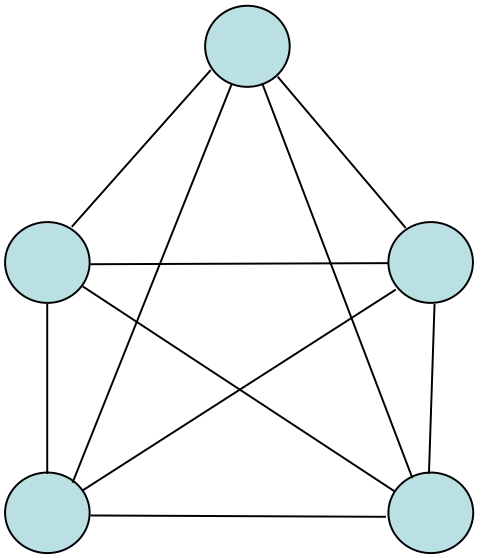
$$\Rightarrow \quad 6 \leq 3n - m$$

$$\Rightarrow \quad m \leq 3n - 6$$

qed

8. Plättbarkeit

- Dank des Zusammenhangs $m \leq 3n - 6$ zwischen Ecken und Kanten in einem planaren Graphen können wir jetzt Aussagen über die Plättbarkeit machen
- z.B. K_5



n=5
m=10

Wäre K_5 planar, würde ja oben genannte Bedingung gelten:

$$10 \leq 3 \cdot 5 - 6 = 9$$

offensichtlich falsch… daraus folgt, daß **K_5 nicht plättbar** ist

- Bei den 'Jeder mit Jedem' - Netzwerken K_n gilt:

$$m(n) = \frac{1}{2} n(n-1)$$

- In Plättbarkeits-bedingung:

$$\frac{n(n-1)}{2} \leq 3n - 6$$

$$\Leftrightarrow \quad n^2 - 7n + 12 \leq 0$$

$$\Rightarrow \quad n_1 = 3 \quad n_2 = 4$$

- K_4 ist der größte **vollständige** plättbare Graph

9. Außerdem

- In jedem planaren Graphen existiert eine Ecke *e* mit *grad(e)* < 6
- Beweis: $\sum grad(e_i) = 2m$

$$\leq 6n - 12$$

  - Angenommen, jede Ecke habe mehr als 5 Kanten:
  - Widerspruch $\sum grad(e_i) \geq 6n$

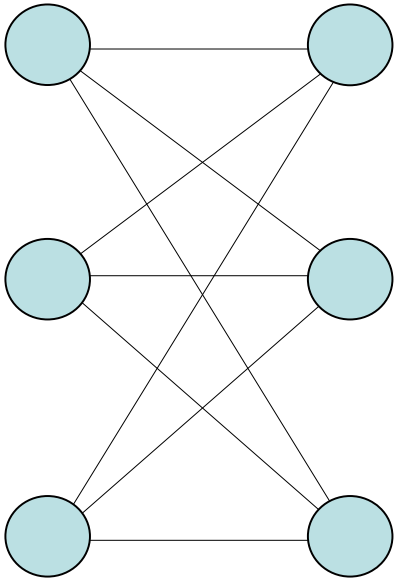
Übung

- Gibt es eine Lösung, jeden linken Knoten mit allen rechten Knoten zu verbinden?
- Lösung: Wäre der Graph plättbar
  - $n - m + g = 2$

    $\Rightarrow g = 5$
  - Jedes Gebiet enthält mindestens 4 Kanten

    $\Rightarrow 2m \geq 4g = 20$

    $\Rightarrow m \geq 10 \neq 9$



10. Zusammenfassung

- G ist **eulersch** $\Leftrightarrow \quad grad(e_i) = 2n_i$
- G ist **planar** bzw. **plättbar**
  $\Leftrightarrow \quad n - m + g = 2$
  $\Leftrightarrow \quad m \leq 3n - 6$