Beweis des Satzes

Zuerst prüfen wir, dass jeder Graph der einen Eulerkreis besitzt, zwingend gerade Knotengrade bei jedem Knoten haben muss: Beim Durchlaufen des Kreises wird jeder Knoten genauso oft angesteuert wie er verlassen wird. Jedesmal werden also zwei Kanten gebraucht. Jede Kante muss genau einmal durchlaufen werden. Also ist eine gerade Anzahl Kanten inzident zum Knoten.

Nun sei umgekehrt $G = (V, E)$ ein Graph, bei dem jeder Knoten geraden Grad hat. Wir müssen zeigen, dass ein Eulerkreis existiert.

Dazu wählen wir einen Weg mit maximaler Länge, der jede Kante höchstens einmal durchläuft. Der Weg sei $(v_0, \ldots, v_n)$.

Wir behaupten, dass $v_0 = v_n$ gilt.

Denn sonst gäbe es bei v_n noch eine ungenutzte Kante, durch die der Pfad verlängert werden könnte, im Widerspruch zur Maximalität!

Beweis (Fortsetzung)

Nun haben wir also einen Kreis, der jede Kante höchstens einmal durchläuft. Durchläuft er alle Kanten, sind wir fertig.

Sei nun $\{u, u'\}$ eine nicht durchlaufene Kante.

1. Fall: $u = v_i$ und $u' = v_j$ für zwei Knoten aus dem Kreis.
   Das kann nicht sein, weil dann leicht ein längerer Pfad konstruiert werden kann.

2. Fall: $u = x$ und $u' = v_i$, wobei v_i aus dem Kreis ist, x aber nicht.
   Das kann auch nicht sein – aus dem selben Grund wie im 1. Fall.

3. Fall: $u = x$ und $u' = y$, und x, y gehören beide nicht zum Kreis.
   Weil G zusammenhängend ist, können wir aber einen Weg von x zu einem v_i finden, dessen letzte Kante uns wieder zum 2. Fall führt - also auch unmöglich.

Also ist der gefundene Kreis schon ein Eulerkreis.

Die notwendige Modifikation für den Eulerweg, wenn zwei Knoten ungeraden Grades existieren, ist leicht und wird den Hörern und Hörerinnen zur Übung überlassen.

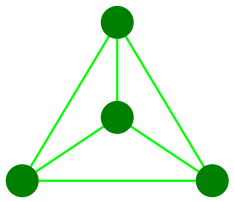
Planare Graphen

Bei der Betrachtung des $K_{3,3}$ ergab sich die Frage, ob man diesen Graph so in die Ebene einzeichnen kann, dass sich die Kanten nicht schneiden. Das motiviert folgende Definition:

Ein Graph heißt *planar*, wenn er sich so in die Ebene einzeichnen lässt, dass sich die Kanten nicht schneiden.

Zum Beispiel alle P_n und alle C_n sind planar. (Das sollte klar sein.)

Wie sieht es mit den vollständigen Graphen K_n aus?
Der K_2 ist der P_2, der K_3 ist der C_3, also sind beide planar!
Der K_4 ist auch planar:



Auch die Graphen $K_{2,n}$ sind für alle n planar.

Dagegen sind weder der K_5 noch der $K_{3,3}$ planar!
Beweis folgt gleich...

Eulerformel

Satz: In endlichen zusammenhängenden planaren Graphen mit $n \geq 1$ Knoten, m Kanten und f Facetten gilt

$$n - m + f = 2$$

(Als Facette bezeichnen wir hier eine zusammenhängende Fläche, die von Kanten berandet wird. Insbesondere ist *das Äußere* immer eine Facette!)

Beweis: Wir führen eine Induktion über die Anzahl der Knoten und der Kanten durch. Bei einem Knoten haben wir $n = 1$, $m = 0$ und $f = 1$.

Sei nun G ein Graph mit $n \geq 2$ Knoten, m Kanten und f Facetten. Die Induktionsvoraussetzung besagt, dass für alle zusammenhängenden planaren Graphen mit n Knoten und weniger als m Kanten oder mit weniger als n Knoten die Eulerformel erfüllt ist.

Induktionsschritt

1. Fall: Der Graph habe Kreise, dann hat er auch einen einfachen Kreis. Wir entfernen aus einem beliebigen einfachen Kreis eine beliebige Kante. Dann erhalten wir einen Graph mit n Knoten, $m-1$ Kanten und $f-1$ Facetten. Nach Ind.vorauss. gilt $n-(m-1)+(f-1)=2$. Aber dann folgt

$$n-m+f=n-(m-1)+(f-1)=2.$$

2. Fall: Nun habe G keine Kreise. Dann muss ein Knoten mit Grad 1 existieren. Wir entfernen diesen und seine einzige Kante. Dann bleibt der Graph zusammenhängend und planar, er hat nur noch $n-1$ Knoten und $m-1$ Kanten, aber die Anzahl der Facetten ändert sich nicht. Nach Ind.vorauss. gilt

$$(n-1)-(m-1)+f=2,$$

woraus wieder direkt die Behauptung folgt.

Folgerungen

Die Eulerformel zieht einige wichtige Folgerungen nach sich:

1. Ein planarer Graph mit $n \geq 3$ Knoten hat höchstens $3n - 6$ Kanten.

2. Ein planarer bipartiter Graph mit $n \geq 4$ Knoten hat höchstens $2n - 4$ Kanten.

3. In jedem planaren Graph gibt es mindestens einen Knoten mit Grad kleiner oder gleich 5.

4. Der K_5 und der $K_{3,3}$ sind nicht planar.

Beweise

Der 1. Punkt ist einzusehen, wenn man bemerkt, dass jede Facette durch mindestens 3 Kanten umrandet wird, aber jede Kante an höchstens 2 Facetten anliegt. Also ist $3f \leq 2m$, und nach Eulerformel $6 = 3n - 3m + 3f \leq 3n - 3m + 2m = 3n - m$.

Bei bipartiten Graphen wird jede Facette von mindestens vier Kanten umrandet, also gilt $4f \leq 2m$ bzw. $2f \leq m$, und daher $4 = 2n - 2m + 2f \leq 2n - 2m + m = 2n - m$.

Für die dritte Behauptung bemerken wir, dass der durchschnittliche Grad der Knoten $\frac{2m}{n}$ ist, aber nach der 1. Folgerung gilt $\frac{2m}{n} \leq \frac{6n-12}{n} < 6$. Also muss es einen Knoten mit Grad kleiner als 6 geben.

K_5 kann nicht planar sein, da hier $n = 5$ und $m = 10$ gilt. Wäre der Graph planar, müsste gelten: $10 \leq 3 \cdot 5 - 6$ (Folgerung 1).

$K_{3,3}$ bipartit, $n = 6$ und $m = 9$. Es müsste $9 \leq 2 \cdot 6 - 4$ gelten.

Satz von Kuratowski

Eine Anmerkung zur Folgerung 3: Die Zahl 5 ist hier optimal gewählt. wie man am Beispiel des *Ikosaeders* sehen kann – das ist ein Graph mit 12 Knoten, die alle den Grad 5 haben!

Wir beenden den Graphen-Abschnitt mit dem folgenden Satz:

Satz: Ein Graph ist genau dann planar, wenn er keine *Unterteilung* des K_5 oder des $K_{3,3}$ enthält.

(Eine Unterteilung ist anschaulich das, was aus einem gegebenen Graph wird, wenn man beliebig oft zusätzliche Knoten auf Kanten legt, wobei die betroffene Kante in zwei Kanten zerteilt wird.)

Dies ist der *Satz von Kuratowski.*
Sein Beweis ist recht aufwändig und wird hier weggelassen.

RSA: Das Verfahren

Das nach seinen Autoren Rivest, Shamir und Adleman benannte *RSA-Verfahren* ist ein asymmetrisches Verschlüsselungsverfahren, das in sehr vielen weit verbreiteten Systemen angewendet wird.

Bob (B) soll eine Nachricht an *Alice* (A) schicken.

Vorbereitungen durch Alice:

Wähle große Primzahlen p und q mit $p < q$.
(Das ist möglich, wie wir später sehen werden.)

Berechne $n = p \cdot q$.

Setze $\varphi(n) = (p-1)(q-1)$, wähle $e > 1$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$.

Berechne Zahl $s < n$ mit $e \cdot s \equiv 1 \bmod \varphi(n)$. (Benutze hierbei den Euklidischen) Algorithmus!)

Alice veröffentlicht das Paar (n, e).

RSA: Bob sendet Nachricht

Die Zahlen n und e sind also nun öffentlich bekannt.
Dagegen müssen p, q und s absolut geheim bleiben!

Bobs Nachricht an Alice muss als eine Zahl im Bereich $\{0, \ldots, n-1\}$ gewählt werden. Die Nachricht sei x.

Bob macht nun Folgendes:

Berechne $y = x^e \bmod n$. (Mit schneller Exponentiation – Folie 28.6)

Sende y über einen beliebigen Kanal zu Alice.

Alice berechnet schließlich den Wert $x' = y^s \bmod n$ und geht davon aus, dass $x = x'$ gilt, d.h. dass sie Bobs Nachricht korrekt entschlüsselt hat.

Es muss also gelten: $(x^e)^s \bmod n = x$. Das zeigen wir gleich!