Hoofdstuk 3

Gehele Getallen

Public key cryptography

Als je geheime berichten wil versturen moet je een techniek afspreken om te *coderen*. Deze techniek noemen we een **cryptosysteem**.
Een bekend eenvoudig cryptosysteem bestaat erin om de letters te "verschuiven" in het alfabet. Als je bijvoorbeeld het bericht "`IK HEB EEN KOEKJE`" wil versturen, kan je elke letter drie plaatsen opschuiven in het alfabet. Je stuurt dus "`LN KHE HHQ NRHNMH`". Indien je als antwoord "`LN ZLO HHQ VWXN`" krijgt, kan je door de inverse operatie het bericht ontcijferen. Je krijgt "`IK WIL EEN STUK`".

Zulk eenvoudig systeem is doeltreffend indien men er zeker van is dat het bericht nooit zal onderschept worden door iemand die iets weet over de frequentie waarmee letters voorkomen in de Nederlandse taal. In onze berichten zie je bijvoorbeeld twee keer "HHQ". Er is veel kans dat dit "EEN" voorstelt.
Een ander nadeel van dit systeem is dat de twee personen die willen communiceren, op voorhand moeten afspreken hoeveel plaatsen zij elke letter opschuiven. Dit is wat men de *sleutel* van het cryptosysteem noemt. Deze sleutel moet geheim blijven. De sleutel uitwisselen tussen de twee personen die willen communiceren is dus een probleem bij dit soort cryptosysteem. Voor betalingen over internet moeten vele gebruikers communiceren met één bedrijf. Het is onbegonnen werk om voor elke gebruiker een sleutel mee te delen zonder dat hij kan onderschept worden. Gelukkig werd er in de jaren '70 door Rivest, Shamir en Adleman een systeem bedacht waarbij de sleutels niet meer geheim hoeven te zijn. Men spreekt van *Public Key Cryptography*.

Het systeem is gebaseerd op priemgetallen en modulair rekenen. Persoon A wil een geheim bericht naar persoon B sturen. Hiervoor gaat hij eerst zijn bericht (dat in letters geschreven is) vertalen naar getallen zodat er kan gerekend worden. Dit gebeurt via een standaard tabel die niet geheim hoeft te zijn. We kunnen bijvoorbeeld afspreken dat "A" wordt voorgesteld door het getal 1, "B" door 2, enz. De spatie is 0. Het bericht "`LUISTER GOED`" wordt dan bijvoorbeeld "`12 21 09 19 20 05 18 00 07 15 05 04`".
We gaan nu elke letter coderen door het te verheffen tot een vaste macht en dan het resultaat te reduceren modulo 33 (omdat er bijvoorbeeld 33 tekens zijn in ons eenvoudig systeem: letters plus wat leestekens). Laat ons bijvoorbeeld telkens de derde macht nemen. Dan is het gecodeerd bericht "`12 21 3 28 14 26 24 0 13 9 26 31`".

Dit was een voorbeeld met kleine getallen om te illustreren wat er gebeurt. In de praktijk gaan we te werk met veel grotere getallen. We moeten ook nog zien hoe deze machtsverheffing kan geïnverteerd worden om te decoderen.
Eén van de voornaamste eigenschappen waarop de veiligheid van het RSA cryptosysteem steunt, is de moeilijkheid om een willekeurig getal te ontbinden in priemfactoren. Het is bijvoorbeeld zeer gemakkelijk om de twee priemgetallen 71 en 59 met elkaar te vermenigvuldigen. We krijgen 4189. Probeer nu het omgekeerde: neem een vergelijkbaar getal, 4161, en probeer dat eens te ontbinden in priemfactoren.

Laat ons de methode van de machtsverheffing nu eens proberen met grotere getallen: we verheffen tot de macht 101 en reduceren modulo 1189. Vermits resten modulo 1189 groter kunnen worden dan 27 hebben we de mogelijkheid om meer symbolen te gebruiken of meerdere letters ineens te coderen. In ons bericht "12 21 09 19 20 05 18 00 07 15 05 04" van hoger kunnen we de cijfers per drie groeperen zodat we "122 109 192 005 180 007 150 504" verkrijgen. Indien het aantal cijfers geen veelvoud is van drie, voegen we op het einde nullen toe om overal groepjes van drie cijfers te hebben.
We moeten nu dus 122^{101} berekenen. Dat is een ander paar mouwen... Zelfs met een rekenmachine zal dat niet lukken, tenzij we het slim aanpakken. We hebben hier immers te maken met een getal van 211 cijfers. Een eerste idee zou zijn om die macht stap voor stap te berekenen en steeds te reduceren modulo 1189. Op die manier krijgen we geen al te grote getallen.

Hier gaan we dan:

$$
\begin{aligned}
122^2 &= 122 \cdot 122 = 14884 \equiv 616 \pmod{1189} \\
122^3 &= 122^2 \cdot 122 \equiv 616 \cdot 122 = 75152 \equiv 245 \pmod{1189} \\
122^4 &= 122^3 \cdot 122 \equiv 245 \cdot 122 = 29890 \equiv 165 \pmod{1189} \\
&\vdots
\end{aligned}
$$

Maar dat is ook nogal veel werk. Veel slimmer is om steeds te kwadrateren.

$$
\begin{aligned}
122^2 &= \qquad = 14884 \equiv 616 \pmod{1189} \\
122^4 &\equiv 616^2 = 379456 \equiv 165 \pmod{1189} \\
122^8 &\equiv 165^2 = 27225 \equiv 1067 \pmod{1189} \\
122^{16} &\equiv 1067^2 = 1138489 \equiv 616 \pmod{1189} \\
122^{32} &\equiv 616^2 = 379456 \equiv 165 \pmod{1189} \\
122^{64} &\equiv 165^2 = 27225 \equiv 1067 \pmod{1189}
\end{aligned}
$$

Nu geldt $101 = 1 + 4 + 32 + 64$ zodat
$122^{101} = 122^1 \cdot 122^4 \cdot 122^{32} \cdot 122^{64} \equiv 122 \cdot 165 \cdot 165 \cdot 1067 =$
$3543987150 \equiv 245 \pmod{1189}$.
Dus met vijf kwadrateringen, een paar vermenigvuldigingen en reducties modulo 1189 hebben we het resultaat. Dit is veel efficiënter dan de honderd vermenigvuldigingen en reducties die we eerst gingen uitvoeren! Deze methode werkt steeds omdat we elke mogelijke exponent steeds kunnen schrijven als som van machten van 2. Dit komt er immers op neer dat we de exponent uitschrijven in basis 2.

We beschrijven nu het RSA algoritme in het algemeen. Persoon B die berichten wil ontvangen kiest twee (grote) priemgetallen p en q en berekent hun product $n := pq$. Hij bepaalt ook $b := (p-1)(q-1)$ en zoekt e met $\text{ggd}(e, b) = 1$. De informatie die publiek wordt gemaakt is n en e.
Indien persoon A een gecodeerd bericht wil sturen naar B zal hij eerst zijn bericht omzetten in getallen. Elk van die getallen m gaat hij dan coderen als volgt

$$c := m^e \pmod{n}$$

Het symbool c wordt dan verstuurd.

Wanneer B het bericht c ontvangt, moet hij dat decoderen. Hij maakt hiervoor gebruik van het feit dat $\text{ggd}(e, b) = 1$. Er is dus een invers d van e modulo b. Er bestaat dus een k met $ed = 1 + k(p-1)(q-1)$ zodat

$$c^d \equiv (m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} \pmod{n}$$

We veronderstellen nu even dat $\text{ggd}(m, p) = \text{ggd}(m, q) = 1$, wat geen grote beperking is. Dan kunnen we de uit de Stelling van Euler halen dat $m^{p-1} \equiv 1 \pmod{p}$ en $m^{q-1} \equiv 1 \pmod{q}$. Bijgevolg geldt

$$c^d \equiv m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1 \equiv m \pmod{p}$$

alsook

$$c^d \equiv m \cdot (m^{q-1})^{k(p-1)} \equiv m \cdot 1 \equiv m \pmod{q}.$$

Merk op dat indien m een veelvoud is van p of q, bovenstaande equivalenties geldig blijven. De onderstelling $\text{ggd}(m, p) = \text{ggd}(m, q) = 1$ was dus slechts tijdelijk nodig.
Uit de Chinese reststelling volgt nu dat

$$c^d \equiv m \pmod{pq}$$

Dus kan B decoderen door gewoon c^d te reduceren modulo n.

In de praktijk worden priemgetallen van ongeveer tweehonderd cijfers gebruikt. Dan heeft n ongeveer vierhonderd cijfers en duurt de ontbinding in priemfactoren, met de beste algoritmen die tot nu toe bekend zijn, nog duizenden jaren. Men mag dus zeggen dat RSA cryptosystemen voorlopig veilig zijn. Bovendien bieden zij het grote voordeel dat de sleutel die dient voor het coderen publiek mag gemaakt worden zonder het systeem in gevaar te brengen.

Hoofdstuk 4

Inleiding tot de Graffentheorie

Graf

Definitie.
Een **graf** *bestaat uit een verzameling V wiens elementen we* **toppen** *en een relatie $\to$ op V die we* **adjacentierelatie** *noemen. Een koppel (u, v) dat behoort tot de relatie $\to$ (d.w.z. $u \to v$) heet een* **pijl**. *De verzameling van pijlen noteren we met E.*

Meestal noteren we graffen met calligrafische letters $\mathcal{G}$, $\mathcal{H}$, ...

Bij ons zal de toppenverzameling van een ongerichte simpele graf $\mathcal{G}$ meestal eindig zijn. De **orde** van $\mathcal{G}$ is dan $|V(\mathcal{G})|$, het aantal toppen in $\mathcal{G}$.

Nu kunnen we naargelang de eigenschappen van de adjacentierelatie verschillende soorten graffen onderscheiden.

Definitie.
Zij $(V, \to)$ *een graf.*

Indien de relatie $\to$ *symmetrisch is, zegt men dat de graf* **ongericht** *is. In dat geval schrijven we dikwijls* $\sim$ *in plaats van* $\to$*. Indien we willen benadrukken dat de graf niet ongericht is, spreken we van een* **gerichte graf***.*

Indien $v \to v$ *zeggen we dat de graf een* **lus** *heeft in* v*. Een graf zonder lussen noemen we* **simpel***.*

Als er meerdere zulke graffen in het spel zijn, noteren we $V(\mathcal{G})$ om de toppenverzameling van $\mathcal{G}$ aan te duiden en $E(\mathcal{G})$ voor de pijlen. De letters V en E komen van het Engels : een top is een "vertex" (meervoud "vertices") en een pijl is een "edge".

Een ongerichte simpele graf kunnen we ook zien als een koppel verzamelingen (V, E) waarbij V gestructureerd wordt door een verzameling E van 2-verzamelingen van V. We hebben dus $E \subset \binom{V}{2}$ en de elementen van E noemen we dan **bogen**.

Twee toppen u, v van zulk een graf (V, E) zijn dus adjacent indien $\{u, v\} \in E$. We zeggen dan ook dat u en v **buren** zijn.

De **buurt** van een top v van een graf $\mathcal{G}$ is de verzameling $\mathcal{G}_v$ van alle buren van v. We hebben dus

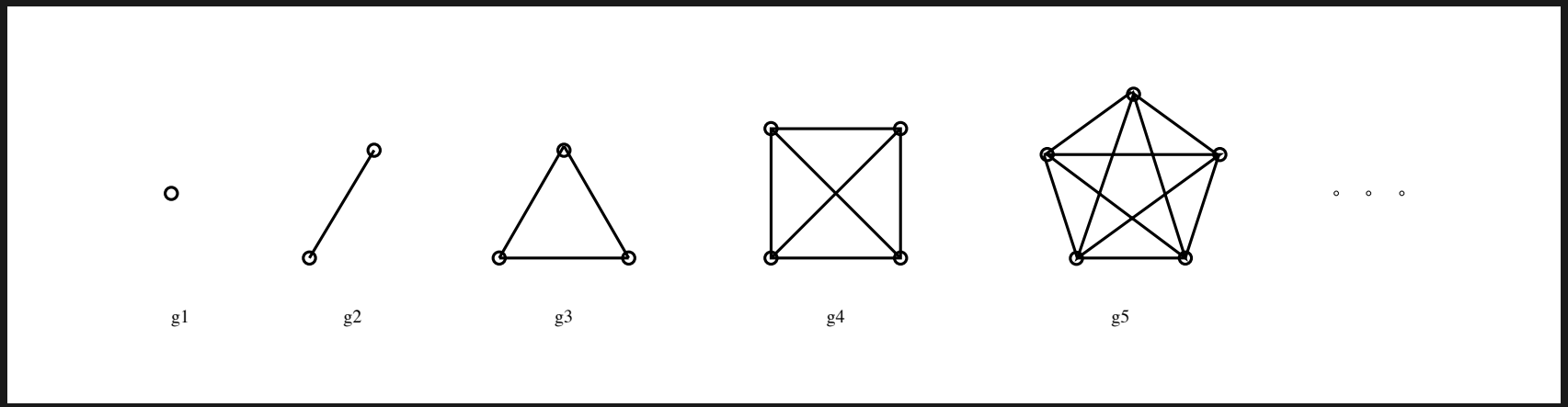
$$\mathcal{G}_v = \{x \in V(\mathcal{G}) \mid x \sim v\}$$

Een top zonder buren heet **geïsoleerd**.

In de literatuur gebruikt men het woord "graf" vaak voor deze specifieke soort van ongerichte simpele graffen.

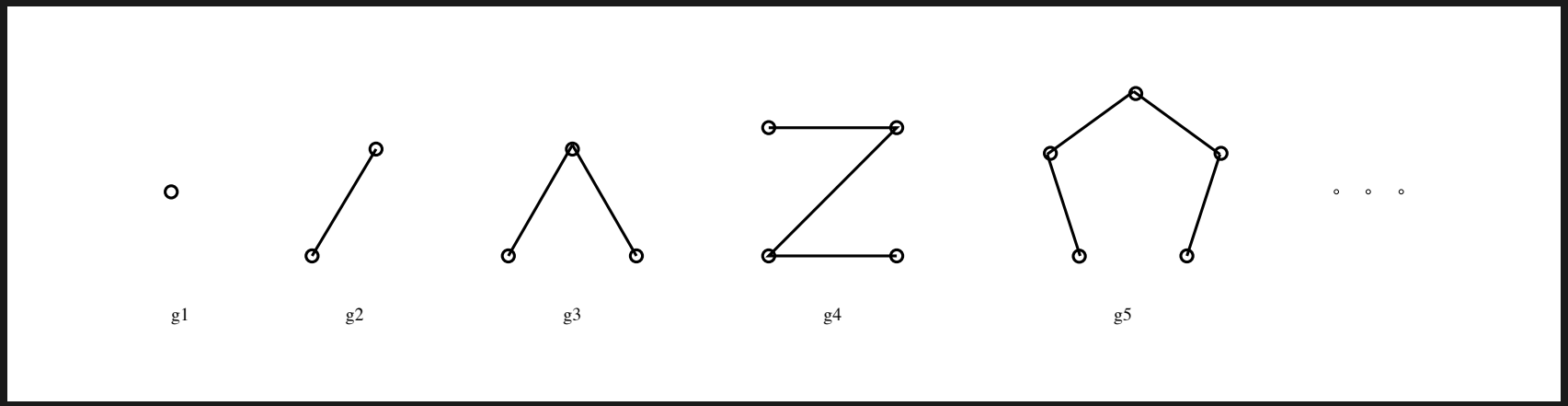
Belangrijke voorbeelden van ongerichte simpele graffen: Complete graffen

De complete graf K_n heeft n toppen. Alle toppen zijn verbonden met alle overige toppen.



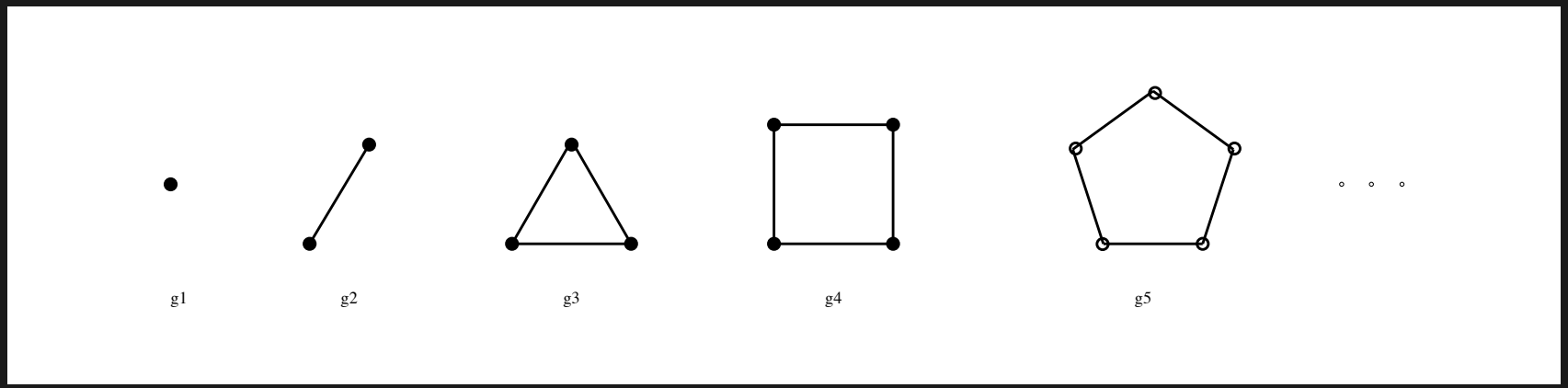
Belangrijke voorbeelden van ongerichte simpele graffen: Paden

Het pad P_n heeft n toppen $t_1, t_2, \ldots, t_n$ die zó verbonden zijn dat $t_i \sim t_{i+1}$ voor $i \in [n-1]$.



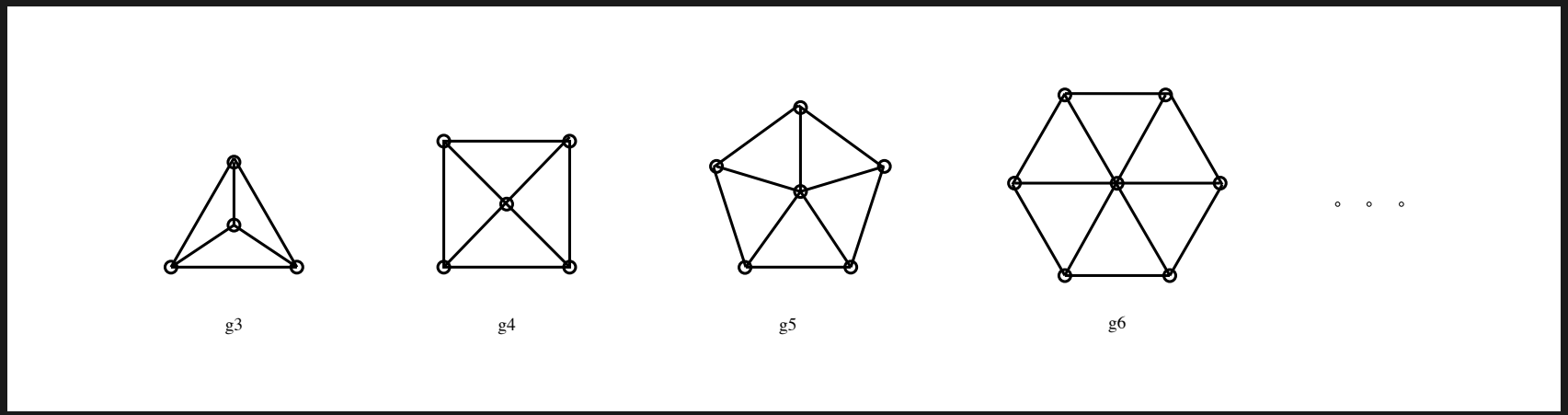
Belangrijke voorbeelden van ongerichte simpele graffen: Cycli

Een cyclus (of cykel) van lengte n is een graf C_n met n toppen $t_0, t_1, \ldots, t_{n-1}$ die zó verbonden zijn dat $t_i \sim t_{i+1}$ voor $i \in \mathbb{Z}_n$, waarbij we de indices modulo n nemen.



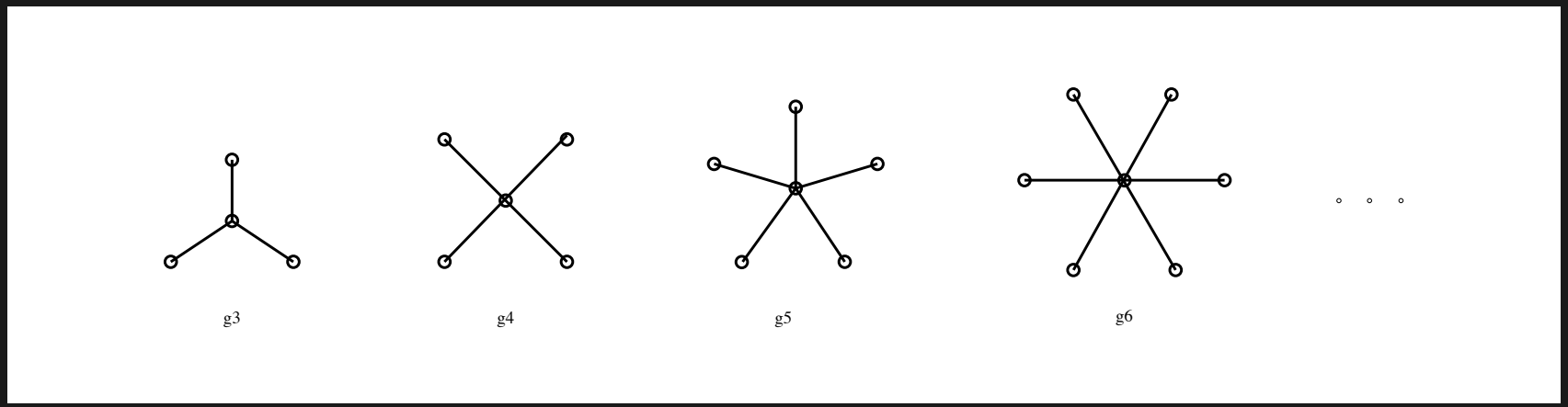
Belangrijke voorbeelden van ongerichte simpele graffen: Wielen

Het wiel W_n van orde n is een cyclus C_n met in het midden een top toegevoegd die verbonden is met alle toppen van de cyclus.



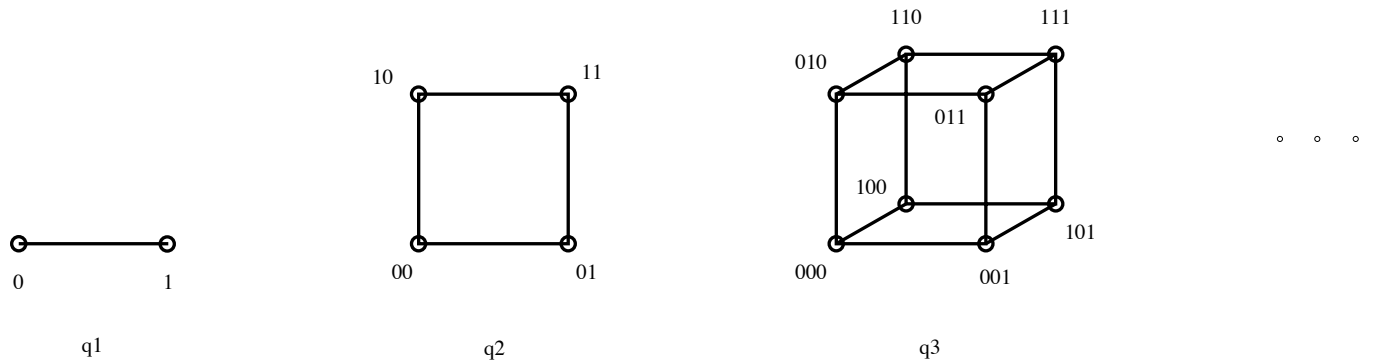
Belangrijke voorbeelden van ongerichte simpele graffen: Sterren

De ster S_n van orde n bekom je door in het wiel W_n de bogen van de cyclus weg te laten.



Belangrijke voorbeelden van ongerichte simpele graffen: Kubussen

Neem $\{0,1\}^n$ als toppenverzameling en maak twee toppen adjacent als ze verschillen in juist één coördinaat. We noteren de kubus in dimensie n met Q_n.



De **graad** van een top v in een ongerichte graf $\mathcal{G}$ is het aantal bogen die v bevatten. We noteren dit met $\deg(v)$ zodat geldt

$$\deg(v) = |\mathcal{G}_v|.$$

Eigenschap.

(Handshake). In een eindige ongerichte graf $\mathcal{G}$ geldt steeds

$$\sum_{v \in V(\mathcal{G})} \deg(v) = 2|E(\mathcal{G})|$$

Bewijs. Dubbeltelling : $\deg(v)$ is het aantal bogen die v bevatten en elke boog bevat juist twee toppen. □

Gevolg.

Een eindige ongerichte graf heeft steeds een even aantal toppen van oneven graad.

Bewijs. Omdat, wegens de vorige eigenschap, de som van alle graden even moet zijn. □

Een ander woord voor graad is **valentie**. Indien alle toppen van een ongerichte graf dezelfde graad hebben, zeggen we dat de graf **regulier** is. Een k-**reguliere** graf is een ongerichte graf waarin elke top graad k heeft.

Definitie.
In een gerichte graf $\mathcal{G}$ definiëren we voor elke top v de **ingraad** *en de* **uitgraad** *als het aantal pijlen dat in v respectievelijk aankomt en vertrekt. We noteren deze graden respectievelijk* $\deg^+(v)$ *en* $\deg^-(v)$.
Een gerichte graf heet **gebalanceerd** *indien voor elke top v geldt dat* $\deg^+(v) = \deg^-(v)$.

Een **deelgraf** van een graf $\mathcal{G}$ is een graf $\mathcal{H}$ met $V(\mathcal{H}) \subset V(\mathcal{G})$ en $E(\mathcal{H}) \subset E(\mathcal{G})$.

We spreken van een **opspannende deelgraf** indien $V(\mathcal{H}) = V(\mathcal{G})$.

Zij $S \subset V(\mathcal{G})$. De **deelgraf door $\mathcal{G}$ geïnduceerd op S** is de graf met toppenverzameling S en de hierbij horende pijlen (voor een ongerichte graf hebben we dus de bogenverzameling $E(\mathcal{G}) \cap \binom{S}{2}$).

Een **wandeling** in een ongerichte graf $\mathcal{G}$ is een rij van toppen

$$t_0, t_1, \ldots, t_k$$

zodanig dat $t_{i-1} \sim t_i$ voor elke $i \in [k]$.
We spreken van een **gerichte wandeling** als $t_{i-1} \to t_i$.

De **lengte** van de wandeling is k, één minder dan het aantal toppen.

De top t_0 heet **beginpunt** (of vertrekpunt) van de wandeling en t_k heet het **eindpunt** (of aankomstpunt). In een wandeling $t_0 \sim t_1 \sim \cdots \sim t_k$ zijn er dus k bogen van de vorm $\{t_{i-1}, t_i\}$ met $i \in [k]$.

Als al die bogen verschillend zijn, wordt de wandeling een **pad** genoemd.
Als $t_0 = t_k$ heet het pad **gesloten**. Een **enkelvoudig pad** is een pad waarin geen twee toppen gelijk zijn. Een gesloten pad dat na verwijderen van de top $t_0 = t_k$ een enkelvoudig pad wordt, heet een **cyclus**.

Een ongerichte graf heet **samenhangend** indien er voor elk paar toppen $u, v \in V(\mathcal{G})$ een pad van u naar v bestaat. Een graf die niet samenhangend is bestaat uit verschillende **samenhangscomponenten** waartussen geen bogen bestaan.

Je kan dit ook als volgt bekijken : de relatie "... is verbonden met ... via een pad" is een equivalentierelatie op $V(\mathcal{G})$. De equivalentieklassen van die relatie zijn de samenhangscomponenten.

Een gerichte graf $\mathcal{G}$ heet **samenhangend** indien de onderliggende graf (verwijder alle pijlen op de bogen) samenhangend is. We zeggen dat $\mathcal{G}$ **sterk samenhangend** is indien er tussen elke twee toppen u en v een **gericht pad** bestaat. Dit wil natuurlijk zeggen dat er een opeenvolging van toppen en bogen $u = t_0, b_1, t_1, b_2, t_2, \ldots, b_k, t_k = v$ bestaat zodanig dat de boog b_i gericht is van t_{i-1} naar t_i en al zulke pijlen verschillend zijn.

Op een ongerichte graf kunnen we ook een **afstand** definiëren.

Voor $u, v \in V(\mathcal{G})$ stellen we $d(u, v)$ gelijk aan de lengte van de kortste wandeling van u naar v. Als er tussen u en v geen wandeling bestaat, schrijven we $d(u, v) = \infty$. We stellen ook voor elke top v dat $d(v, v) = 0$.

Eigenschap.
Voor een ongerichte graf $\mathcal{G}$ geldt dat

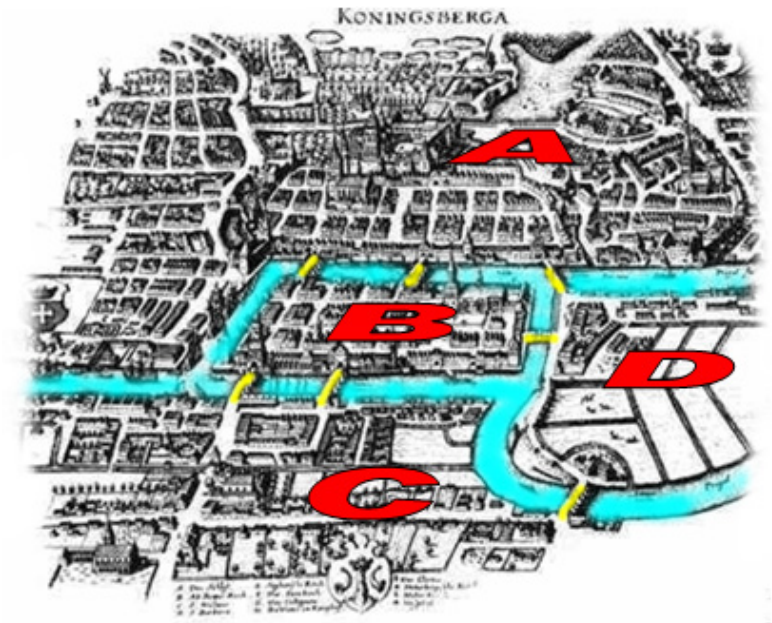
$$d\colon V(\mathcal{G}) \times V(\mathcal{G}) \longrightarrow \mathbb{N} \cup \{\infty\}\colon (u, v) \longmapsto d(u, v)$$

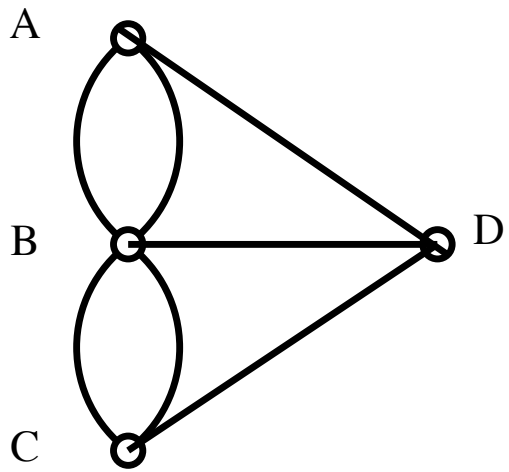
een metriek is.

Bewijs. Het is duidelijk dat $d(u, v) = 0 \Leftrightarrow u = v$ en dat $d(u, v) = d(v, u)$ voor elk paar toppen $u, v \in V(\mathcal{G})$.
Zij nu $u, v, w \in V(\mathcal{G})$ drie toppen met $d(u, v) = k$ en $d(v, w) = l$. Dit geeft een wandeling van u naar v en één van v naar w. Door deze na elkaar te volgen, krijgen we een wandeling van v naar w die lengte $k + l$ heeft. De afstand $d(u, w)$ zal dus ten hoogste $k + l$ bedragen. □

Eulerpaden

Graffen werden uitgevonden door Leonhard Euler (1707–1783). Hij leefde op dat moment in Königsberg (nu Kaliningrad, Rusland) in Pruisen. De stad wordt in vier stukken verdeeld door de Pregel-rivier. Er zijn ook zeven bruggen over de rivier om de verschillende stadsgedeelten te verbinden. Op een dag was er een stoet die door de hele stad ging en Euler vroeg zich af of er een wandeling bestond voor de stoet zodanig dat elke brug juist één maal overgestoken werd en bovendien de wandeling terug zou komen naar het startpunt.
Euler stelde het probleem grafisch voor met zeven bogen en vier toppen, welke overeenkomen met de zeven bruggen en de vier stadsgedeelten. Het resultaat is geen graf aangezien er “dubbele” bogen zijn en in een relatie komen de koppels immers hoogstens één keer voor.





Een plattegrond van Königsberg ten tijde van Euler en daarnaast zijn grafische voorstelling.

Definitie.
Een **multigraf** *is een graf* $\mathcal{G} = (V, \to)$ *uitgebreid door middel van een functie* $\mu\colon V \times V \longrightarrow \mathbb{N}$ *die een* **multipliciteit** *toekent aan elke pijl. We interpreteren de functie* μ *als volgt:*

- $\mu(u, v) = 0$ *betekent* u *en* v *niet adjacent zijn;*
- $\mu(u, v) = k > 0$ *betekent dat er* k *pijlen zijn van* u *naar* v*.*

Pijlen die hetzelfde begin- en eindpunt hebben worden **parallel** *genoemd.*

Een multigraf zonder parallelle pijlen is een graf.